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

H. R. 4350

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

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT INTENDED TO BE PROPOSED BY MR. PETERS (for himself, Mr. PORTMAN, Mr. WARNER, and Ms. COLLINS and Ms. SINEMA) to the amendment (No. 3867) proposed by Mr. REED

Viz:

At the end, add the following:

DIVISION E—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2021

SEC. 5101. SHORT TITLE.

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

SEC. 5102. 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 for threats to systems that evade detection by automated threat detection systems.

TITLE LI—UPDATES TO FISMA

SEC. 5121. TITLE 44 AMENDMENTS.

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

(1) in section 3504—

(A) in subsection (a)(1)(B)—

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

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

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

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

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

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

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

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

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

(C) in subsection (h)(1)—

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

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

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

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

(2) in section 3505—

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

(i) in subparagraph (B)—

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

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

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

(iii) by adding at the end the following:

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

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

(3) in section 3506—

(A) in subsection (b)(1)(C), by inserting ", availability" after "integrity"; and

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

(4) in section 3513—

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

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

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

(b) Subchapter II Definitions.—

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

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

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

"(1) The term 'additional cybersecurity procedure' means a process, procedure, or other activity that is established in excess of the information security standards promulgated

under section 11331(b) of title 40 to increase the security and reduce the cybersecurity risk of agency systems.";

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

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

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

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

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

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

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

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

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

(2) CONFORMING AMENDMENTS.—

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

(B) TITLE 10.—

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

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

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

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

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

(D) INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 3(5) of the Internet of Things Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a)

is amended by striking "section 3552(b)(6)" and inserting "section 3552(b)".

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

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

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

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

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

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

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

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

(ii) in subsection (f)—

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

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

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

(1) in section 3551—

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

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

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

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

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

(E) in paragraph (7), as so redesignated, by striking the period at the end and

inserting a semi colon; and

(F) by adding at the end the following:

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

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

"(10) recognize that—

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

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

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

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

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

(2) in section 3553—

(A) by striking the section heading and inserting "Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency".

(B) in subsection (a)—

(i) in paragraph (1), by inserting "in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director," before "developing and overseeing";

(ii) in paragraph (5)—

(I) by inserting ", in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director," before "agency compliance"; and

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

(iii) by adding at the end the following:

"(8) promoting, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Institute of Standards and Technology—

"(A) the use of automation to improve Federal cybersecurity and visibility with respect to the implementation of Federal cybersecurity; and

"(B) the use of presumption of compromise and least privilege principles to improve resiliency and timely response actions to incidents on Federal systems.";

(C) in subsection (b)—

(i) by striking the subsection heading and inserting "Cybersecurity and Infrastructure Security Agency";

(ii) in the matter preceding paragraph (1), by striking "The Secretary, in consultation with the Director" and inserting "The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and the National Cyber Director";

(iii) in paragraph (2)—

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

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

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

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

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

(D) in subsection (c)—

(i) in the matter preceding paragraph (1), by striking "each year" and inserting "each year during which agencies are required to submit reports under section 3554(c)";

(ii) by striking paragraph (1);

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

(iv) in paragraph (3), as so redesignated, by striking "and" at the end;

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

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

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

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

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

"(i) Federal Risk Assessments.—On an ongoing and continuous basis, the Director of the Cybersecurity and Infrastructure Security Agency shall perform assessments of Federal risk

posture using any available information on the cybersecurity posture of agencies, and brief the Director and National Cyber Director on the findings of those assessments including—

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

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

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

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

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

"(6) evaluation of agency threat hunting results;

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

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

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

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

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

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

"(1) the specific";

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

(iii) by adding at the end the following:

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

(H) by adding at the end the following:

"(n) Binding Operational Directives.—If the Director of the Cybersecurity and Infrastructure Security Agency issues a binding operational directive or an emergency directive under this section, not later than 2 days after the date on which the binding operational directive requires an agency to take an action, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate reporting entities the status of the implementation of the binding operational directive at the agency.";

(3) in section 3554—

(A) in subsection (a)—

(i) in paragraph (1)—

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

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

following:

"(A) on an ongoing and continuous basis, performing agency system risk assessments that—

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

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

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

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

"(v) evaluate the vulnerability of agency systems and data, including high value assets, including by analyzing—

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

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

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

"(IV) incidents; and

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

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

"(vii) assess the consequences of potential incidents occurring on agency systems that would impact systems at other agencies, including due to interconnectivity between different agency systems or 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 conducted under subparagraph (A), providing, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, information";

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

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

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

(V) by adding at the end the following:

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

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

"(ii) on a periodic basis, as determined by guidance issued by the Director but not less frequently than annually, to—

"(I) the Director;

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

"(III) the National Cyber Director;

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

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

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

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

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

"(ii) the Director; and

"(iii) the National Cyber Director; and

"(H) if the head of the agency determines there is need for additional cybersecurity procedures, ensuring that those additional cybersecurity procedures are reflected in the budget request of the agency in accordance with the risk-based cyber budget model developed pursuant to section 3553(a)(7);";

(ii) in paragraph (2)—

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

(II) in subparagraph (B)—

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

"(i) standards"; and

(bb) by adding at the end the following:

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

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

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

(iii) in paragraph (3)—

(I) in subparagraph (A)—

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

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

(cc) by adding at the end the following:

"(v) ensure that—

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

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

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

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

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

(B) in subsection (b)—

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

"(1) pursuant to subsection (a)(1)(A), performing ongoing and continuous agency system risk assessments, which may include using guidelines and automated tools consistent with standards and guidelines promulgated under section 11331 of title 40, as applicable;";

(ii) in paragraph (2)—

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

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

(II) in subparagraph (D)—

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

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

"(iii) binding operational directives and emergency directives promulgated by the Director of the Cybersecurity and Infrastructure Security Agency under

section 3553;"; and

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

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

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

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

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

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

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

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

(vii) in paragraph (8)(C), as so redesignated—

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

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

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

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

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

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

(aa) in subclause (I), by striking "and relevant offices of inspectors general";

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

(cc) by striking subclause (III); and

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

(C) in subsection (c)—

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

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

"(1) BIANNUAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment under subsection (a)(1)(A), the head of each agency shall submit to the Director, the Director of the Cybersecurity and Infrastructure Security Agency, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

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

"(B) evaluates the adequacy and effectiveness of information security policies, procedures, and practices of the agency to address the risks identified in the agency system risk assessment performed under subsection (a)(1)(A), including an analysis of the agency's cybersecurity and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c));

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

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

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

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

"(B) may include a classified annex.

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

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

(iii) in paragraph (5), as so redesignated, by inserting "including the reporting procedures established under section 11315(d) of title 40 and subsection (a)(3)(A)(v) of this section"; and

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

Director"; and

(4) in section 3555—

(A) in the section heading, by striking "annual independent" and inserting "independent";

(B) in subsection (a)—

(i) in paragraph (1), by inserting "during which a report is required to be submitted under section 3553(c)," after "Each year";

(ii) in paragraph (2)(A), by inserting ", including by penetration testing and analyzing the vulnerability disclosure program of the agency" after "information systems"; and

(iii) by adding at the end the following:

"(3) An evaluation under this section may include recommendations for improving the cybersecurity posture of the agency.";

(C) in subsection (b)(1), by striking "annual";

(D) in subsection (e)(1), by inserting "during which a report is required to be submitted under section 3553(c)" after "Each year";

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

"(f) Protection of Information.—(1) Agencies, evaluators, and other recipients of information that, if disclosed, may cause grave harm to the efforts of Federal information security officers shall take appropriate steps to ensure the protection of that information, including safeguarding the information from public disclosure.

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

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

"(A) specific information system incidents; or

"(B) specific information system vulnerabilities.";

(F) in subsection (g)(2)—

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

"(A) shall";

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

(iii) by adding at the end the following:

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

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

"(j) Guidance.—

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

"(2) PRIORITIES.—The guidance developed under paragraph (1) shall prioritize the identification of—

"(A) the most common threat patterns experienced by each agency;

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

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

(5) in section 3556(a)—

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

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

(d) Conforming Amendments.—

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

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

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

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

"3555. Independent evaluation.".

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

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

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

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

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

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

(e) Federal System Incident Response.—

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

"SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

"3591. Definitions

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

"(b) Additional Definitions.—As used in this subchapter:

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

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

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

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

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

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

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

"(G) the Director;

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

"(I) the National Cyber Director;

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

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

"(2) AWARDEE.—The term 'awardee'—

"(A) means a person, business, or other entity that receives a grant from, or is a party to a cooperative agreement or an other transaction agreement with, an agency; and

"(B) includes any subgrantee of a person, business, or other entity described in subparagraph (A).

"(3) BREACH.—The term 'breach' means—

"(A) a compromise of the security, confidentiality, or integrity of data in electronic form that results in unauthorized access to, or an acquisition of, personal information; or

"(B) a loss of data in electronic form that results in unauthorized access to, or an acquisition of, personal information.

"(4) CONTRACTOR.—The term 'contractor' means—

"(A) a prime contractor of an agency or a subcontractor of a prime contractor of an agency; and

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

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

"(6) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an agency, a contractor, 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 a senior privacy officer of the agency, shall—

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

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

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

"(C) the type of breach; and

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

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

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

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

"(b) Contents of Notice.—Each notice of a breach provided to an individual under subsection (a)(2) shall include—

"(1) a brief description of the rationale for the determination that notice should be provided under subsection (a);

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

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

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

"(B) may include a telephone number or a website;

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

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

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

"(c) Delay of Notification.—

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

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

"(B) reveal sensitive sources and methods;

"(C) cause damage to national security; or

"(D) hamper security remediation actions.

"(2) DOCUMENTATION.—

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

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

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

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

"(d) Update Notification.—If an agency determines there is a significant change in the reasonable basis to conclude that a breach occurred, a significant change to the determination

made under subsection (a)(1), or that it is necessary to update the details of the information provided to impacted individuals as described in subsection (b), the agency shall as expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify each individual who received a notification pursuant to subsection (a) of those changes.

"(e) Exemption From Notification.—

"(1) IN GENERAL.—The head of an agency, in consultation with the inspector general of the agency, may request an exemption from the Director from complying with the notification requirements under subsection (a) if the information affected by the breach is determined by an independent evaluation to be unreadable, including, as appropriate, instances in which the information is—

"(A) encrypted; and

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

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

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

"(B) the Attorney General.

"(3) DOCUMENTATION.—Any exemption granted by the Director under paragraph (1) shall be reported in writing to the head of the agency and the inspector general of the agency that experienced the breach and the Director of the Cybersecurity and Infrastructure Security Agency.

"(f) Rule of Construction.—Nothing in this section shall be construed to limit—

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

"(2) the Director from issuing guidance relating to notifications of major incidents or the head of an agency from providing more information than described in subsection (b) when notifying individuals potentially affected by breaches.

"3593. Congressional and Executive Branch reports

"(a) Initial Report.—

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

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

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

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

"(2) CONTENTS.—A report required under paragraph (1) shall include, in a manner that excludes or otherwise reasonably protects personally identifiable information and to the extent permitted by applicable law, including privacy and statistical laws—

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

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

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

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

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

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

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

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

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

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

"(7) the detection, response, and remediation actions of the agency, including any support

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

"(c) Update Report.—If the agency determines that there is any significant change in the understanding of the agency of the scope, scale, or consequence of a major incident for which an agency submitted a written report under subsection (a), the agency shall provide an updated report to the appropriate reporting entities that includes information relating to the change in understanding.

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

"(e) Delay and Exemption Report.—

"(1) IN GENERAL.—The Director shall submit to the appropriate notification entities an annual report on all notification delays and exemptions granted pursuant to subsections (c) and (d) of section 3592.

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

"(f) Report Delivery.—Any written report required to be submitted under this section may be submitted in a paper or electronic format.

"(g) Threat Briefing.—

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

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

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

"(B) may include a classified component.

"(h) Rule of Construction.—Nothing in this section shall be construed to limit—

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

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

"3594. Government information sharing and incident response

"(a) In General.—

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

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

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

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

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

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

"(ii) additional necessary safeguards; and

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

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

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

"(iii) information that could reasonably help identify the party that conducted the incident.

"(3) INFORMATION SHARING.—To the greatest extent practicable, the Director of the Cybersecurity and Infrastructure Security Agency shall share information relating to an incident with any agencies that may be impacted by the incident.

"(4) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about incidents that occur on national security systems with the Director of the Cybersecurity and Infrastructure Security Agency to the extent consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President.

"(b) Compliance.—The information provided under subsection (a) shall take into account the level of classification of the information and any information sharing limitations and protections, such as limitations and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director

"(c) Incident Response.—Each agency that has a reasonable basis to conclude that a major incident occurred involving Federal information in electronic medium or form, as defined by the Director and not involving a national security system, regardless of delays from notification granted for a major incident, shall coordinate with the Cybersecurity and Infrastructure Security Agency regarding—

"(1) incident response and recovery; and

"(2) recommendations for mitigating future incidents.

"3595. Responsibilities of contractors and awardees

"(a) Notification.—

"(1) IN GENERAL.—Unless otherwise specified in a contract, grant, cooperative agreement, or an other transaction agreement, any contractor or awardee of an agency shall

report to the agency within the same amount of time such agency is required to report an incident to the Cybersecurity and Infrastructure Security Agency, if the contractor or awardee has a reasonable basis to conclude that—

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

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

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

"(2) PROCEDURES.—

"(A) MAJOR INCIDENT.—Following a report of a breach or major incident by a contractor or awardee under paragraph (1), the agency, in consultation with the contractor or awardee, shall carry out the requirements under sections 3592, 3593, and 3594 with respect to the major incident.

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

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

"3596. Training

"(a) Covered Individual Defined.—In this section, the term 'covered individual' means an individual who obtains access to Federal information or Federal information systems because of the status of the individual as an employee, contractor, awardee, volunteer, or intern of an agency.

"(b) Requirement.—The head of each agency shall develop training for covered individuals on how to identify and respond to an incident, including—

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

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

"(c) Inclusion in Annual Training.—The training developed under subsection (b) may be included as part of an annual privacy or security awareness training of an agency.

"3597. Analysis and report on Federal incidents

"(a) Analysis of Federal Incidents.—

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

"(A) the causes of incidents, including—

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

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

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

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

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

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

"(F) trends in cross-Federal Government 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)).

"(2) AUTOMATED ANALYSIS.—The analyses developed under paragraph (1) shall, to the greatest extent practicable, use machine readable data, automation, and machine learning processes.

"(3) SHARING OF DATA AND ANALYSIS.—

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

"(i) improve the understanding of cybersecurity risk of agencies; and

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

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

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

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

"(b) Annual Report on Federal Incidents.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and other Federal agencies as appropriate, shall submit to the appropriate notification entities a report that includes—

"(1) a summary of causes of incidents from across the Federal Government that categorizes those incidents as incidents or major incidents;

"(2) the quantitative and qualitative analyses of incidents developed under subsection (a)(1) 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 compromises 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.—A version of each report submitted under subsection (b) shall be made publicly available on the website of the Cybersecurity and Infrastructure Security Agency during the year in which the report is submitted.

"(d) Information Provided by Agencies.—

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

"(2) NONCOMPLIANCE REPORTS.—

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

"(i) data for the incident; and

"(ii) the information described in subsection (b) with respect to the agency.

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

"(3) NATIONAL SECURITY SYSTEM REPORTS.—

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

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

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

"(iii) the Committee on Homeland Security and Governmental Affairs of the

Senate;

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

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

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

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

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

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

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

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

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

"(e) Requirement for Compiling Information.—In publishing the public report required under subsection (c), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information such that no specific incident of an agency can be identified, except with the concurrence of the Director of the Office of Management and Budget and in consultation with the impacted agency.

"3598. Major incident definition

"(a) In General.—Not later than 180 days after the date of enactment of the Federal Information Security Modernization Act of 2021, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, shall develop and promulgate guidance on the definition of the term 'major incident' for the purposes of subchapter II and this subchapter.

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

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

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

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

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

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

"(C) any incident that the head of an agency, in consultation with a senior privacy

officer of the agency, determines is likely to have a significant privacy impact on 1 or more individual;

"(D) any incident that the head of the agency, in consultation with a senior privacy official of the agency, determines is likely to have a substantial privacy impact on a significant number of individuals;

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

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

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

"(2) stipulate that the National Cyber Director shall declare a major incident at each agency impacted by an incident if the Director of the Cybersecurity and Infrastructure Security Agency determines that an incident—

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

"(B) is enabled by—

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

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

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

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

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

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

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

"(ii) the Chair of the Federal Trade Commission.

"(c) Significant Number of Individuals.—In determining what constitutes a significant number of individuals under subsection (b)(1)(D), the Director—

"(1) may determine a threshold for a minimum number of individuals that constitutes a significant amount; and

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

"(d) Evaluation and Updates.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021, and not less frequently than every 2 years

thereafter, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives an evaluation, which shall include—

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

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

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

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

"subchapter iv—federal system incident response

"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. 5122. AMENDMENTS TO SUBTITLE III OF TITLE 40.

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

(b) Modernizing Government Technology.—Subtitle G of title X of Division A of the National Defense Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301 note) is amended—

(1) in section 1077(b)—

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

(B) in paragraph (7)—

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

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

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

(iii) in subparagraph (A), as so designated, by striking "under section

1094(b)(1)" and inserting "by the Director"; and

(iv) by adding at the end the following:

"(B) CONSULTATION.—In using funds under paragraph (3)(A), the Chief Information Officer of the covered agency shall consult with the necessary stakeholders to ensure the project appropriately addresses cybersecurity risks, including the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate."; and

(2) in section 1078—

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

"(a) Definitions.—In this section:

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

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

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

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

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

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

(C) in subsection (c)—

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

(ii) in paragraph (5)—

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

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

(III) by adding at the end the following:

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

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

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

(1) in section 11302—

(A) in subsection (b), by striking "use, security, and disposal of" and inserting "use,

and disposal of, and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, promote and improve the security of,";

(B) in subsection (c)—

(i) in paragraph (3)—

(I) in subparagraph (A)—

(aa) by striking "including data" and inserting "which shall—

"(i) include data";

(bb) in clause (i), as so designated, by striking ", and performance" and inserting "security, and performance; and"; and

(cc) by adding at the end the following:

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

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

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

(ii) in paragraph (4)(B), in the matter preceding clause (i), by inserting "not later than 30 days after the date on which the review under subparagraph (A) is completed," before "the Administrator";

(C) in subsection (f)—

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

"(1) develop";

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

(iii) by adding at the end the following:

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

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

(2) in section 11303(b)—

(A) in paragraph (2)(B)—

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

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

(iii) by adding at the end the following:

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

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

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

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

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

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

"(d) Component Agency Chief Information Officers.—The Chief Information Officer or an equivalent official of a component agency shall report to—

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

"(2) the head of the component agency.";

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

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

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

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

(2) in subsection (b)(1)(A)—

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

(B) by striking "the Secretary of Homeland Security" and inserting "the Director of the Cybersecurity and Infrastructure Security Agency";

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

"(c) Application of More Stringent Standards.—

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

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

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

"(2) EVALUATION OF MORE STRINGENT STANDARDS.—In evaluating the need to employ

more stringent standards under paragraph (1), the head of an agency shall consider available risk information, such as—

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

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

"(C) incident information of the agency;

"(D) information from—

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

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

"(E) agency threat hunting results under section 5145 of the Federal Information Security Modernization Act of 2021;

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

"(G) data on compliance with standards issued under this section;

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

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

(4) in subsection (d)(2)—

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

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

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

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

"(B) in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency;

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

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

(5) by adding at the end the following:

"(e) Review of Office of Management and Budget Guidance and Policy.—

"(1) CONDUCT OF REVIEW.—

"(A) IN GENERAL.—Not less frequently than once every 3 years, the Director of the Office of Management and Budget, in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency shall review the efficacy of the guidance and policy promulgated by the Director in reducing cybersecurity risks, including an assessment of the requirements for agencies to report information to the Director, and determine whether any changes to that guidance or policy is appropriate.

"(B) FEDERAL RISK ASSESSMENTS.—In conducting the review described in subparagraph (A), the Director shall consider the Federal risk assessments performed under section 3553(i) of title 44.

"(2) UPDATED GUIDANCE.—Not later than 90 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall issue updated guidance or policy to agencies determined appropriate by the Director, based on the results of the review.

"(3) PUBLIC REPORT.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall make publicly available a report that includes—

"(A) an overview of the guidance and policy promulgated under this section that is currently in effect;

"(B) the cybersecurity risk mitigation, or other cybersecurity benefit, offered by each guidance or policy document described in subparagraph (A); and

"(C) a summary of the guidance or policy to which changes were determined appropriate during the review and what the changes are anticipated to include.

"(4) CONGRESSIONAL BRIEFING.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the review.

"(f) Automated Standard Implementation Verification.—When the Director of the National Institute of Standards and Technology issues a proposed standard pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Director of the National Institute of Standards and Technology shall consider developing and, if appropriate and practical, develop, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, specifications to enable the automated verification of the implementation of the controls within the standard.".

SEC. 5123. ACTIONS TO ENHANCE FEDERAL INCIDENT RESPONSE.

(a) Responsibilities of the Cybersecurity and Infrastructure Security Agency.—

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

(A) develop a plan for the development of the analysis required under section 3597(a) of title 44, United States Code, as added by this division, and the report required under subsection (b) of that section that includes—

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

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

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

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

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

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

(b) Responsibilities of the Director of the Office of Management and Budget.—

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

(A) by striking subsection (b); and

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

(2) INCIDENT DATA SHARING.—

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

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

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

(I) the causes of incidents;

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

(III) a root cause analysis of incidents that—

(aa) are common across the Federal Government; or

(bb) have a Government-wide impact;

(IV) agency response, recovery, and remediation actions and the effectiveness of those actions; and

(V) the impact of incidents;

(ii) enable the efficient development of—

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

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

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

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

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

(4) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop guidance and templates, to be reviewed and, if necessary, updated not less frequently than once every 2 years, for use by Federal agencies in the activities required under sections 3592, 3593, and 3596 of title 44, United States Code, as added by this 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 Federal agencies on how to deconflict, to the greatest extent practicable, existing regulations, policies, and procedures relating to the responsibilities of contractors and awardees established under section 3595 of title 44, United States Code, as added by this 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 Federal agencies of incidents involving information of the Federal Government.

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

(c) Update to the Privacy Act of 1974.—Section 552a(b) of title 5, United States Code (commonly known as the "Privacy Act of 1974") is amended—

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

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

(3) by adding at the end the following:

"(13) to another agency in furtherance of a response to an incident (as defined in section 3552 of title 44) and pursuant to the information sharing requirements in section 3594 of title 44 if the head of the requesting agency has made a written request to the agency that

maintains the record specifying the particular portion desired and the activity for which the record is sought.".

SEC. 5124. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

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

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

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

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

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

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

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

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

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

(a) Definitions.—In this section:

(1) REPORTING ENTITY.—The term "reporting entity" means private organization or governmental unit that is required by statute or regulation to submit sensitive information to an agency.

(2) SENSITIVE INFORMATION.—The term "sensitive information" has the meaning given the term by the Director in guidance issued under subsection (b).

(b) Guidance on Notification of Reporting Entities.—Not later than 180 days after the date of enactment of this Act, the Director shall issue guidance requiring the head of each agency to notify a reporting entity of an incident that is likely to substantially affect—

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

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

TITLE LII—IMPROVING FEDERAL CYBERSECURITY

SEC. 5141. MOBILE SECURITY STANDARDS.

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

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

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

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

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

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

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

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

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

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

SEC. 5142. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

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

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

(1) the types of logs to be maintained;

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

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

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

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

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

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

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

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

SEC. 5143. CISA AGENCY ADVISORS.

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

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

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

(2) performing risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

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

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

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

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

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

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

SEC. 5144. FEDERAL PENETRATION TESTING POLICY.

(a) In General.—Subchapter II of chapter 35 of title 44, United States Code, is amended by

adding at the end the following:

"3559A. Federal penetration testing

"(a) Definitions.—In this section:

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

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

"(b) Guidance.—

"(1) IN GENERAL.—The Director shall issue guidance that—

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

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

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

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

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

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

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

"(c) Agency Plans and Rules of Engagement.—The agency operational plan and rules of engagement of an agency shall—

"(1) require the agency to—

"(A) perform penetration testing on the high value assets of the agency; or

"(B) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency to ensure that penetration testing is being performed;

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

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

"(B) adverse impacts to operational environments and systems of the agency; and

"(C) inappropriate access to data;

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

"(4) include mechanisms for providing consistently formatted, and, if applicable, automated and machine-readable, data to the Director and the Director of the Cybersecurity and Infrastructure Security Agency.

"(d) Responsibilities of CISA.—The Director of the Cybersecurity and Infrastructure Security

Agency shall—

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

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

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

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

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

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

"(2) develop and maintain a standardized process for the use of penetration testing.

"(f) Prioritization of Penetration Testing Resources.—

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

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

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

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

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

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

"(g) Exception for National Security Systems.—The guidance issued under subsection (b) shall not apply to national security systems.

"(h) Delegation of Authority for Certain Systems.—The authorities of the Director described in subsection (b) shall be delegated—

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

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

(b) Deadline for Guidance.—Not later than 180 days after the date of enactment of this Act, the Director shall issue the guidance required under section 3559A(b) of title 44, United States Code, as added by subsection (a).

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

"3559A. Federal penetration testing.".

(d) Penetration Testing by the Secretary of Homeland Security.—Section 3553(b) of title 44,

United States Code, as amended by section 5121, is further amended—

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

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

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

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

SEC. 5145. ONGOING THREAT HUNTING PROGRAM.

(a) Threat Hunting Program.—

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

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

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

(B) provide on-premises support to agencies;

(C) staff threat hunting services;

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

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

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

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

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

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

(2) not less than 30 days before the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services under the program 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. 5146. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS.

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

"3559B. Federal vulnerability disclosure programs

"(a) Definitions.—In this section:

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

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

"(b) Responsibilities of OMB.—

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

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

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

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

"(A) any valid or credible reports of newly discovered or not publicly known vulnerabilities (including misconfigurations) on Federal information systems that use commercial software or services;

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

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

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

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

"(3) AGENCY VULNERABILITY DISCLOSURE POLICIES.—The Director shall issue guidance to agencies on the required minimum scope of agency systems covered by the vulnerability

disclosure policy of an agency required under subsection (d)(2).

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

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

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

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

"(d) Responsibilities of Agencies.—

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

"(A) an appropriate security contact; and

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

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

"(A) describe—

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

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

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

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

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

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

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

"(C) include any other relevant information; and

"(D) be mature in scope, to cover all Federal information systems used or operated by that agency or on behalf of that agency.

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

"(e) Paperwork Reduction Act Exemption.—The requirements of subchapter I (commonly known as the 'Paperwork Reduction Act') shall not apply to a vulnerability disclosure program

established under this section.

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

"(g) Exemptions.—The authorities and functions of the Director and Director of the Cybersecurity and 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 204, the following:

"3559B. Federal vulnerability disclosure programs.".

SEC. 5147. IMPLEMENTING PRESUMPTION OF COMPROMISE AND LEAST PRIVILEGE PRINCIPLES.

(a) Guidance.—Not later than 1 year after the date of enactment of this Act, the Director shall provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems, including—

(1) shifting away from "trusted networks" to implement security controls based on a presumption of compromise;

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

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

(4) identifying incidents quickly;

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

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

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

(b) Agency Progress Reports.—Not later than 1 year after the date of enactment of this Act, the head of each agency shall submit to the Director a progress report on implementing an information security program based on the presumption of compromise and least privilege principles, which shall include—

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

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

(3) a schedule to implement any planned activities.

SEC. 5148. AUTOMATION REPORTS.

(a) OMB Report.—Not later than 180 days after the date of enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the use of automation under paragraphs (1), (5)(C) and (8)(B) of section 3554(b) of title 44, United States Code.

(b) GAO Report.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall perform a study on the use of automation and machine readable data across the Federal Government for cybersecurity purposes, including the automated updating of cybersecurity tools, sensors, or processes by agencies.

SEC. 5149. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL.

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

SEC. 5150. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

(a) Dashboard Required.—Section 11(e)(2) of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

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

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

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

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

SEC. 5151. 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, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall—

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

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

(A) update the covered metrics; and

(B) establish new covered metrics.

(c) Implementation.—

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

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

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

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

(d) Congressional Reports.—

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

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

(e) Cybersecurity Act of 2015 Updates.—Section 224 of the Cybersecurity Act of 2015 (6 U.S.C. 1522) is amended—

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

"(c) Improved Metrics.—

"(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall establish, review, and update metrics to measure the cybersecurity and incident response capabilities of agencies in accordance with

the responsibilities of agencies under section 3554 of title 44, United States Code.

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

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

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

"(ii) the amount of time that passes between—

"(I) the detection of an incident and the remediation of the incident; and

"(II) the remediation of an incident and the recovery from the incident; and

"(B) the metrics may include other measurable outcomes.";

(2) by striking subsection (e); and

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

TITLE LIII—RISK-BASED BUDGET MODEL

SEC. 5161. DEFINITIONS.

In this title:

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

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

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

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

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

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

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

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

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

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

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

SEC. 5162. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.

(a) In General.—

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

(2) RESPONSIBILITY OF DIRECTOR.—Section 3553(a) of title 44, United States Code, as amended by section 5121 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".

(3) CONTENTS OF MODEL.—The model required to be developed under paragraph (1) shall—

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

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

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

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

(i) information technology and cybersecurity tools;

(ii) information technology and cybersecurity architectures;

(iii) information technology and cybersecurity personnel; and

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

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

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

(5) PUBLICATION.—The Director shall publish the model required to be developed under this subsection, and any updates necessary under paragraph (4), on the public website of the Office of Management and Budget.

(6) REPORTS.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until the date on which the model

required to be developed under this subsection is completed, whichever is sooner, the Director shall submit a report to Congress on the development of the model.

(b) Required Use of Risk-based Budget Model.—

(1) IN GENERAL.—Not later than 2 years after the date on which the model developed under subsection (a) is published, the head of each covered agency shall use the model to develop the annual cybersecurity and information technology budget requests of the agency.

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

(c) Verification.—

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

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

(B) in subclause (III), by striking "and" at the end; and

(C) by adding at the end the following:

"(V) a validation that the budgets submitted were developed using a risk-based methodology; and

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

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall take effect on the date that is 2 years after the date on which the model developed under subsection (a) is published.

(d) Reports.—

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

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

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

(C) by adding at the end the following:

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

(2) ASSESSMENT.—Section 3553(c) of title 44, United States Code, as amended by section 5121, is further amended by inserting after paragraph (5) the following:

"(6) an assessment of—

"(A) Federal agency implementation of the model required under subsection (a)(7);

"(B) how cyber vulnerabilities of Federal agencies changed from the previous year; and

"(C) whether the model mitigates the cyber vulnerabilities of the Federal Government.".

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

(1) an evaluation of the success of covered agencies in developing risk-based budgets;

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

(3) an evaluation of whether the risk-based budgets developed by covered agencies mitigate cyber vulnerability, including the extent to which the risk-based budgets inform Federal Government-wide cybersecurity programs; and

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

TITLE LIV—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

SEC. 5181. ACTIVE CYBER DEFENSIVE STUDY.

(a) Definition.—In this section, the term "active defense technique"—

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

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

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

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

(2) an evaluation of—

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

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

(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impede threat response efforts, criminal investigations, and national

security activities, including intelligence collection; and

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

SEC. 5182. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

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

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

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

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

(2) staffing and resources; and

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

(d) Pilot Program.—

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

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

(e) Briefing and Report.—

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

DIVISION F—CYBER INCIDENT REPORTING ACT OF 2021 AND CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

TITLE LXI—CYBER INCIDENT REPORTING ACT OF 2021

SEC. 6101. SHORT TITLE.

This title may be cited as the "Cyber Incident Reporting Act of 2021".

SEC. 6102. DEFINITIONS.

In this title:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms "covered cyber incident", "covered entity", and "cyber incident" have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 6103 of this title.

(2) RANSOM PAYMENT; RANSOMWARE ATTACK.—The terms "ransom payment" and "ransomware attack" have the meanings given those terms in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 651), as added by section 6203 of this division.

(3) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

(4) INFORMATION SYSTEM; SECURITY VULNERABILITY.—The terms "information system" and "security vulnerability" have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

SEC. 6103. CYBER INCIDENT REPORTING.

(a) Cyber Incident Reporting.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(b) (6 U.S.C. 659(b)), as so redesignated by section 6203(b) of this division—

(A) in paragraph (11), by striking "and" at the end;

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

(C) by adding at the end the following:

"(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 2230) submitted by covered entities (as defined in section 2230) and reports related to ransom payments submitted by entities in furtherance of the activities specified in sections 2202(e), 2203, and 2231, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors."; and

(2) by adding at the end the following:

"Subtitle C—Cyber Incident Reporting

"SEC. 2230. DEFINITIONS.

"In this subtitle:

"(1) CENTER.—The term 'Center' means the center established under section 2209.

"(2) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

"(3) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

"(4) COVERED ENTITY.—The term 'covered entity' means—

"(A) any Federal contractor; or

"(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

"(5) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2200.

"(6) CYBER THREAT.—The term 'cyber threat'—

"(A) has the meaning given the term 'cybersecurity threat' in section 2200; and

"(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

"(7) FEDERAL CONTRACTOR.—The term 'Federal contractor' means a business, nonprofit organization, or other private sector entity that holds a Federal Government contract, unless that contractor is a party only to—

"(A) a service contract to provide housekeeping or custodial services; or

"(B) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

"(8) FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL.—The terms 'Federal entity', 'information system', and 'security control' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

"(9) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cybersecurity incident, or a group of related cybersecurity incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

"(10) SMALL ORGANIZATION.—The term 'small organization'—

"(A) means—

"(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

"(ii) any nonprofit organization, including faith-based organizations and houses of worship, or other private sector entity with fewer than 200 employees (determined on a full-time equivalent basis); and

"(B) does not include—

"(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

"(ii) a Federal contractor.

"SEC. 2231. CYBER INCIDENT REVIEW.

"(a) Activities.—The Center shall—

"(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to support law enforcement investigations, to assess potential impact of incidents on public health and safety, and to have a more accurate picture of the cyber threat to critical infrastructure and the people of the United States;

"(2) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetuate cyber incidents and ransomware attacks;

"(3) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

"(4) leverage information gathered about cybersecurity incidents to—

"(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, critical infrastructure owners and operators, cybersecurity and incident response firms, and security researchers; and

"(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2235;

"(5) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

"(6) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

"(7) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

"(8) with respect to covered cyber incident reports under subsection (b) involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

"(9) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the reports required under subsection (b);

"(10) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

"(11) proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable;

"(12) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Center; and

"(13) in accordance with section 2235 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 2233, or information received pursuant to a request for information or subpoena under section 2234, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

"(b) Interagency Sharing.—The Director of the Office of Management and Budget, in consultation with the Director and the National Cyber Director—

"(1) may establish a specific time requirement for sharing information under subsection (a)(13); and

"(2) shall determine the appropriate Federal agencies under subsection (a)(13).

"(c) Periodic Briefing.—Not later than 60 days after the effective date of the final rule required under section 2232(b), and on the first day of each month thereafter, the Director, in

consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

"(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

"(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

"(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

"(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

"(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and

"(4) be unclassified, but may include a classified annex.

"SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

"(a) In General.—

"(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

"(2) RANSOM PAYMENT REPORTS.—An entity, including a covered entity and except for an individual or a small organization, that makes a ransom payment as the result of a ransomware attack against the entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

"(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

"(4) PRESERVATION OF INFORMATION.—Any entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

"(5) EXCEPTIONS.—

"(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under paragraphs (1) and (2) apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

"(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

"(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2) and (3) shall not apply to an entity or the functions of an entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

"(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

"(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

"(b) Rulemaking.—

"(1) NOTICE OF PROPOSED RULEMAKING.—Not later than 2 years after the date of enactment of this section, the Director, in consultation with Sector Risk Management Agencies and the heads of other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

"(2) FINAL RULE.—Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

"(3) SUBSEQUENT RULEMAKINGS.—

"(A) IN GENERAL.—The Director may issue regulations to implement subsection (a) after issuance of the final rule under paragraph (2), including a rule to amend or revise the final rule.

"(B) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

"(c) Elements.—The final rule issued pursuant to subsection (b) shall be composed of the following elements:

"(1) A clear description of the types of entities that constitute covered entities, based on—

"(A) the consequences that disruption to or compromise of such an entity could

cause to national security, economic security, or public health and safety;

"(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

"(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

"(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

"(A) at a minimum, require the occurrence of—

"(i) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

"(ii) a disruption of business or industrial operations due to a cyber incident; or

"(iii) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

"(B) consider—

"(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

"(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

"(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

"(C) exclude—

"(i) any event where the cyber incident is perpetuated by a United States Government entity, good faith security research, or in response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as through a vulnerability disclosure program or the use of authorized penetration testing services; and

"(ii) the threat of disruption as extortion, as described in section 2201(9)(A).

"(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

"(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

"(A) A description of the covered cyber incident, including—

"(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident;

"(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

"(iii) the estimated date range of such incident; and

"(iv) the impact to the operations of the covered entity.

"(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident.

"(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.

"(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

"(E) The name and other information that clearly identifies the entity impacted by the covered cyber incident.

"(F) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subtitle.

"(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

"(A) A description of the ransomware attack, including the estimated date range of the attack.

"(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.

"(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

"(D) The name and other information that clearly identifies the entity that made the ransom payment.

"(E) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that entity to assist with compliance with the requirements of this subtitle.

"(F) The date of the ransom payment.

"(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

"(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

"(I) The amount of the ransom payment.

"(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which the data is required to be preserved.

"(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

"(A) be established by the Director in consultation with the Council;

"(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable; and

"(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and investigations.

"(8) Procedures for—

"(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

"(B) the Agency to carry out the enforcement provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of subpoenas, appeals and due process procedures, the suspension and debarment provisions in section 2234(c), and other aspects of noncompliance;

"(C) implementing the exceptions provided in subparagraphs (A), (B), and (D) of subsection (a)(5); and

"(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 105(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)) and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

"(9) A clear description of the types of entities that constitute other private sector entities for purposes of section 2230(b)(7).

"(d) Third Party Report Submission and Ransom Payment.—

"(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law firm, to submit the required report under

subsection (a).

"(2) RANSOM PAYMENT.—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

"(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

"(4) RESPONSIBILITY TO ADVISE.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the responsibilities of the impacted entity regarding reporting ransom payments under this section.

"(e) Outreach to Covered Entities.—

"(1) IN GENERAL.—The Director shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

"(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

"(A) An overview of the final rule issued pursuant to subsection (b).

"(B) An overview of mechanisms to submit to the Center covered cyber incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

"(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

"(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

"(E) Specific outreach to cybersecurity vendors, incident response providers, cybersecurity insurance entities, and other entities that may support covered entities or ransomware attack victims.

"(F) An overview of the privacy and civil liberties requirements in this subtitle.

"(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Director may coordinate with—

"(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

"(B) information sharing and analysis organizations;

"(C) trade associations;

"(D) information sharing and analysis centers;

"(E) sector coordinating councils; and

"(F) any other entity as determined appropriate by the Director.

"(f) Organization of Reports.—Notwithstanding chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), the Director may request information within the scope of the final rule issued under subsection (b) by the alteration of existing questions or response fields and the reorganization and reformatting of the means by which covered cyber incident reports, ransom payment reports, and any voluntarily offered information is submitted to the Center.

"SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

"(a) In General.—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

"(b) Voluntary Provision of Additional Information in Required Reports.—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

"(c) Application of Protections.—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

"SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.

"(a) Purpose.—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirement to report, the Director may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

"(b) Initial Request for Information.—

"(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2231(a), that an entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment to the Center within 72 hours in accordance with section 2232(a), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

"(2) TREATMENT.—Information provided to the Center in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2232.

"(c) Authority to Issue Subpoenas and Debar.—

"(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

"(2) CIVIL ACTION.—

"(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

"(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the entity against which the action is brought resides, is found, or does business.

"(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

"(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

"(4) DEBARMENT OF FEDERAL CONTRACTORS.—If a covered entity with a Federal Government contract, grant, cooperative agreement, or other transaction agreement fails to comply with a subpoena issued under this subsection—

"(A) the Director may refer the matter to the Administrator of General Services; and

"(B) upon receiving a referral from the Director, the Administrator of General Services may impose additional available penalties, including suspension or debarment.

"(d) Actions by Attorney General and Regulators.—

"(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate regulator determines, based on information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Attorney General or the appropriate regulator may use that information for a regulatory enforcement action or criminal prosecution.

"(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

"(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise

prohibited by law.

"(e) Considerations.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

"(1) the size and complexity of the entity;

"(2) the complexity in determining if a covered cyber incident has occurred; and

"(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

"(f) Exclusions.—This section shall not apply to a State, local, Tribal, or territorial government entity.

"(g) Report to Congress.—The Director shall submit to Congress an annual report on the number of times the Director—

"(1) issued an initial request for information pursuant to subsection (b);

"(2) issued a subpoena pursuant to subsection (c);

"(3) brought a civil action pursuant to subsection (c)(2); or

"(4) conducted additional actions pursuant to subsection (d).

"SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

"(a) Disclosure, Retention, and Use.—

"(1) AUTHORIZED ACTIVITIES.—Information provided to the Center or Agency pursuant to section 2232 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

"(A) a cybersecurity purpose;

"(B) the purpose of identifying—

"(i) a cyber threat, including the source of the cyber threat; or

"(ii) a security vulnerability;

"(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

"(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

"(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a covered cyber incident or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

"(2) AGENCY ACTIONS AFTER RECEIPT.—

"(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the center shall immediately review the report to determine whether the incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

"(B) STANDARDS FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

"(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Center or the Agency pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

"(A) personal information of a specific individual; or

"(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

"(4) DIGITAL SECURITY.—The Center and the Agency shall ensure that reports submitted to the Center or the Agency pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

"(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Center or the Agency in accordance with this subtitle to regulate, including through an enforcement action, the lawful activities of the covered entity or entity that made a ransom payment.

"(b) No Waiver of Privilege or Protection.—The submission of a report to the Center or the Agency under section 2232 shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

"(c) Exemption From Disclosure.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the 'Freedom of Information Act') and any State, Tribal, or local provision of law requiring disclosure of information or records.

"(d) Ex Parte Communications.—The submission of a report to the Agency under section 2232 shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

"(e) Liability Protections.—

"(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2232(a) that is submitted in conformance with this subtitle and the rule promulgated under section 2232(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2234(c)(2).

"(2) SCOPE.—The liability protections provided in subsection (e) shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Center or the Agency.

"(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

"(f) Sharing With Non-Federal Entities.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2232 available to critical infrastructure owners and operators and the general public.

"(g) Proprietary Information.—Information contained in a report submitted to the Agency under section 2232 shall be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.

"(h) Stored Communications Act.—Nothing in this subtitle shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the 'Stored Communications Act').".

(b) Technical and Conforming Amendment.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the items relating to subtitle B of title XXII the following:

"Subtitle C—Cyber Incident Reporting

"Sec.2230.Definitions.

"Sec.2231.Cyber Incident Review.

"Sec.2232.Required reporting of certain cyber incidents.

"Sec.2233.Voluntary reporting of other cyber incidents.

"Sec.2234.Noncompliance with required reporting.

"Sec.2235.Information shared with or provided to the Federal Government.".

SEC. 6104. FEDERAL SHARING OF INCIDENT REPORTS.

(a) Cyber Incident Reporting Sharing.—

(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, any Federal agency that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Director as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cybersecurity Infrastructure Security Agency and the recipient Federal agency.

(2) RULE OF CONSTRUCTION.—The requirements described in paragraph (1) shall not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(3) PROTECTION OF INFORMATION.—The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this Act or the amendments made by this Act.

(4) FOIA EXEMPTION.—Any report received by the Director pursuant to paragraph (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the "Freedom of Information Act").

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

(1) in paragraph (1)—

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

(B) by redesignating subparagraph (H) as subparagraph (I); and

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

"(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget and the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with Sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651)); and"; and

(2) by adding at the end the following:

"(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1)(H) shall be construed to provide any additional regulatory authority to any Federal entity.".

(c) Harmonizing Reporting Requirements.—The National Cyber Director shall, in consultation with the Director, the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), and the Director of the Office of Management and Budget, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report cyber incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with the Director and regulatory authorities that receive reports relating to cyber incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of such agencies to gain timely situational awareness of a covered cyber incident or ransom payment.

SEC. 6105. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) Program.—Not later than 1 year after the date of enactment of this Act, the Director shall establish a ransomware vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

(b) Identification of Vulnerable Systems.—The pilot program established under subsection (a) shall—

(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

(2) utilize existing authorities to identify Federal and other relevant information systems that contain the security vulnerabilities identified in paragraph (1).

(c) Entity Notification.—

(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures within that section.

(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

(d) Prioritization of Notifications.—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

(e) Limitation on Procedures.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or

operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

(f) Rule of Construction.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

(g) Termination.—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act.

SEC. 6106. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) Joint Ransomware Task Force.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in consultation with the Attorney General and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the task force to mitigate the

threat of ransomware attacks against Federal and non-Federal entities.

(b) Clarifying Private Sector Lawful Defensive Measures.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on Oversight and Reform of the House of Representatives a report that describes defensive measures that private sector actors can take when countering ransomware attacks and what laws need to be clarified to enable that action.

(c) Rule of Construction.—Nothing in this section shall be construed to provide any additional authority to any Federal agency.

SEC. 6107. CONGRESSIONAL REPORTING.

(a) Report on Stakeholder Engagement.—Not later than 30 days after the date on which the Director issues the final rule under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103(b) of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that describes how the Director engaged stakeholders in the development of the final rule.

(b) Report on Opportunities to Strengthen Security Research.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report describing how the National Cybersecurity and Communications Integration Center established under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) has carried out activities under section 2231(a)(9) of the Homeland Security Act of 2002, as added by section 6103(a) of this title, by proactively identifying opportunities to use cyber incident data to inform and enable cybersecurity research within the academic and private sector.

(c) Report on Ransomware Vulnerability Warning Pilot Program.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 6105, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report, which may include a classified annex, on the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 6105(c) in mitigating security vulnerabilities and the threat of ransomware.

(2) Identification of the most common vulnerabilities utilized in ransomware.

(3) The number of notifications issued during the preceding year.

(4) To the extent practicable, the number of vulnerable devices or systems mitigated under this pilot by the Agency during the preceding year.

(d) Report on Harmonization of Reporting Regulations.—

(1) IN GENERAL.—Not later than 180 days after the date on which the National Cyber

Director convenes the Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

(B) a description of any challenges in harmonizing the duplicative reporting requirements;

(C) any actions the National Cyber Director intends to take to facilitate harmonizing the duplicative reporting requirements; and

(D) any proposed legislative changes necessary to address the duplicative reporting.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to provide any additional regulatory authority to any Federal agency.

(e) GAO Reports.—

(1) IMPLEMENTATION OF THIS ACT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this Act and the amendments made by this Act.

(2) EXEMPTIONS TO REPORTING.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103 of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the exemptions to reporting under paragraphs (2) and (5) of section 2232(a) of the Homeland Security Act of 2002, as added by section 6103 of this title, which shall include—

(A) to the extent practicable, an evaluation of the quantity of incidents not reported to the Federal Government;

(B) an evaluation of the impact on impacted entities, homeland security, and the national economy of the ransomware criminal ecosystem of incidents and ransom payments, including a discussion on the scope of impact of incidents that were not reported to the Federal Government;

(C) an evaluation of the burden, financial and otherwise, on entities required to report cyber incidents under this Act, including an analysis of entities that meet the definition of a small organization and would be exempt from ransom payment reporting but not for being a covered entity; and

(D) a description of the consequences and effects of the exemptions.

(f) Report on Effectiveness of Enforcement Mechanisms.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103 of this title, the Director shall submit to the

Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the enforcement mechanisms within section 2234 of the Homeland Security Act of 2002, as added by section 6103 of this title.

TITLE LXII—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 6201. SHORT TITLE.

This title may be cited as the "CISA Technical Corrections and Improvements Act of 2021".

SEC. 6202. REDESIGNATIONS.

(a) In General.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(2) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(3) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(4) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217; and

(5) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216.

(b) Technical and Conforming Amendments.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in the first paragraph (12), by striking "section 2215" and inserting "section 2217"; and

(2) by redesignating the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

(c) Additional Technical Amendment.—

(1) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking "Homeland Security Act" and inserting "Homeland Security Act of 2002".

(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

SEC. 6203. CONSOLIDATION OF DEFINITIONS.

(a) In General.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651) is amended by inserting before the subtitle A heading the following:

"SEC. 2200. DEFINITIONS.

"Except as otherwise specifically provided, in this title:

"(1) AGENCY.—The term 'Agency' means the Cybersecurity and Infrastructure Security Agency.

"(2) AGENCY INFORMATION.—The term 'agency information' means information collected or maintained by or on behalf of an agency.

"(3) AGENCY INFORMATION SYSTEM.—The term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency.

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

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

"(B) the Committee on Homeland Security of the House of Representatives.

"(5) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

"(6) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including—

"(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

"(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

"(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

"(7) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' means information that is necessary to describe or identify—

"(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related

to a cybersecurity threat or security vulnerability;

"(B) a method of defeating a security control or exploitation of a security vulnerability;

"(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

"(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

"(E) malicious cyber command and control;

"(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

"(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

"(H) any combination thereof.

"(8) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

"(9) CYBERSECURITY RISK.—The term 'cybersecurity risk'—

"(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

"(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

"(10) CYBERSECURITY THREAT.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'cybersecurity threat' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

"(B) EXCLUSION.—The term 'cybersecurity threat' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

"(11) DEFENSIVE MEASURE.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'defensive measure' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or

transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

"(B) EXCLUSION.—The term 'defensive measure' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

"(i) the entity operating the measure; or

"(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

"(12) HOMELAND SECURITY ENTERPRISE.—The term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

"(13) INCIDENT.—The term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

"(14) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

"(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

"(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

"(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

"(15) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

"(16) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

"(17) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

"(18) MONITOR.—The term 'monitor' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

"(19) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term 'national cybersecurity asset response activities' means—

"(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

"(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

"(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

"(D) facilitating information sharing and operational coordination with threat response; and

"(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

"(20) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

"(21) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

"(22) RANSOMWARE ATTACK.—The term 'ransomware attack'—

"(A) means a cyber incident that includes the threat of use of unauthorized or malicious code on an information system, or the threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

"(B) does not include any such event where the demand for payment is made by a Federal Government entity, good faith security research, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system.

"(23) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

"(24) SECURITY VULNERABILITY.—The term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

"(25) SHARING.—The term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

"(26) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber incident within the supply chain of an information technology system whereby an adversary jeopardizes the confidentiality, integrity, or availability of the information technology system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

"(27) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

"(28) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.".

(b) Technical and Conforming Amendments.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by amending section 2201 to read as follows:

"SEC. 2201. DEFINITION.

"In this subtitle, the term 'Cybersecurity Advisory Committee' means the advisory committee established under section 2219(a).";

(2) in section 2202—

(A) in subsection (a)(1), by striking "(in this subtitle referred to as the Agency)";

(B) in subsection (f)—

(i) in paragraph (1), by inserting "Executive" before "Assistant Director"; and

(ii) in paragraph (2), by inserting "Executive" before "Assistant Director";

(3) in section 2203(a)(2), by striking "as the 'Assistant Director'" and inserting "as the 'Executive Assistant Director'";

(4) in section 2204(a)(2), by striking "as the 'Assistant Director'" and inserting "as the 'Executive Assistant Director'";

(5) in section 2209—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (o) as subsections (a) through (n), respectively;

(C) in subsection (c)(1)(A)(iii), as so redesignated, by striking ", as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))";

(D) in subsection (d), as so redesignated, in the matter preceding paragraph (1), by striking "subsection (c)" and inserting "subsection (b)";

(E) in subsection (j), as so redesignated, by striking "subsection (c)(8)" and inserting "subsection (b)(8)"; and

(F) in subsection (n), as so redesignated—

(i) in paragraph (2)(A), by striking "subsection (c)(12)" and inserting "subsection (b)(12)"; and

(ii) in paragraph (3)(B)(i), by striking "subsection (c)(12)" and inserting "subsection (b)(12)";

(6) in section 2210—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (d) as subsections (a) through (c), respectively;

(C) in subsection (b), as so redesignated—

(i) by striking "information sharing and analysis organizations (as defined in section 2222(5))" and inserting "Information Sharing and Analysis Organizations"; and

(ii) by striking "(as defined in section 2209)"; and

(D) in subsection (c), as so redesignated, by striking "subsection (c)" and inserting "subsection (b)";

(7) in section 2211, by striking subsection (h);

(8) in section 2212, by striking "information sharing and analysis organizations (as defined in section 2222(5))" and inserting "Information Sharing and Analysis Organizations";

(9) in section 2213—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (f) as subsections (a) through (e); respectively;

(C) in subsection (b), as so redesignated, by striking "subsection (b)" each place it appears and inserting "subsection (a)";

(D) in subsection (c), as so redesignated, in the matter preceding paragraph (1), by striking "subsection (b)" and inserting "subsection (a)"; and

(E) in subsection (d), as so redesignated—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A), by striking "subsection (c)(2)" and inserting "subsection (b)(2)";

(II) in subparagraph (A), by striking "subsection (c)(1)" and inserting "subsection (b)(1)"; and

(III) in subparagraph (B), by striking "subsection (c)(2)" and inserting "subsection (b)(2)"; and

(ii) in paragraph (2), by striking "subsection (c)(2)" and inserting "subsection

(b)(2)";

(10) in section 2216, as so redesignated—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (h) as subsections (a) through (g), respectively;

(C) in subsection (a), as so redesignated—

(i) in the matter preceding paragraph (1), by striking "subsection (e)" and inserting "subsection (d)";

(ii) in paragraph (1), by striking "subsection (c)" and inserting "subsection (b)"; and

(iii) in paragraph (2), by striking "subsection (c)" and inserting "subsection (b)";

(D) in subsection (b)(4), as so redesignated—

(i) by striking "subsection (e)" and inserting "subsection (d)"; and

(ii) by striking "subsection (h)" and inserting "subsection (g)";

(E) in subsection (d), as so redesignated, by striking "subsection (b)(1)" each place it appears and inserting "subsection (a)(1)";

(F) in subsection (e), as so redesignated—

(i) by striking "subsection (b)" and inserting "subsection (a)";

(ii) by striking "subsection (e)" and inserting "subsection (d)"; and

(iii) by striking "subsection (b)(1)" and inserting "subsection (a)(1)"; and

(G) in subsection (f), as so redesignated, by striking "subsection (c)" and inserting "subsection (b)";

(11) in section 2217, as so redesignated, by striking subsection (f) and inserting the following:

"(f) Cyber Defense Operation Defined.—In this section, the term 'cyber defense operation' means the use of a defensive measure."; and

(12) in section 2222—

(A) by striking paragraphs (3), (5), and (8);

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

(C) by redesignating paragraphs (6) and (7) as paragraphs (4) and (5), respectively.

(c) Table of Contents Amendments.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by inserting before the item relating to subtitle A of title XXII the following:

"Sec.2200.Definitions.";

(2) by striking the item relating to section 2201 and inserting the following:

"Sec.2201.Definition."; and

(3) by striking the second item relating to section 2215 and all that follows through the item relating to section 2217 and inserting the following:

"Sec.2216.Cybersecurity State Coordinator.

"Sec.2217.Joint Cyber Planning Office.

"Sec.2218.Duties and authorities relating to .gov internet domain.

"Sec.2219.Cybersecurity Advisory Committee.

"Sec.2220.Cybersecurity Education and Training Programs.".

(d) Cybersecurity Act of 2015 Definitions.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(1) by striking paragraphs (4) through (7) and inserting the following:

"(4) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

"(5) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

"(6) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

"(7) DEFENSIVE MEASURE.—The term 'defensive measure' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.";

(2) by striking paragraph (13) and inserting the following:

"(13) MONITOR.— The term 'monitor' has the meaning given the term in section 2200 of the Homeland Security Act of 2002."; and

(3) by striking paragraph (17) and inserting the following:

"(17) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.".

SEC. 6204. ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.

(a) Federal Cybersecurity Enhancement Act of 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

(1) in section 222 (6 U.S.C. 1521)—

(A) in paragraph (2), by striking "section 2210" and inserting "section 2200"; and

(B) in paragraph (4), by striking "section 2209" and inserting "section 2200";

(2) in section 223 (6 U.S.C. 151 note), by striking "section 2213(b)(1)" each place it appears and inserting "section 2213(a)(1)";

(3) in section 226—

(A) in subsection (a)—

(i) in paragraph (1), by striking "section 2213" and inserting "section 2200";

(ii) in paragraph (4), by striking "section 2210(b)(1)" and inserting "section 2210(a)(1)"; and

(iii) in paragraph (5), by striking "section 2213(b)" and inserting "section 2213(a)"; and

(B) in subsection (c)(1)(A)(vi), by striking "section 2213(c)(5)" and inserting "section 2213(b)(5)"; and

(4) in section 227(b) (6 U.S.C. 1525(b)), by striking "section 2213(d)(2)" and inserting "section 2213(c)(2)".

(b) Public Health Service Act.—Section 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C. 300hh–10(b)(4)(D)) is amended by striking "section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))" and inserting "section 2210(c) of the Homeland Security Act of 2002".

(c) William M. (Mac) Thornberry National Defense Authorization Act of Fiscal Year 2021.—Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking "section 2222(5) of the Homeland Security Act of 2002 (6 U.S.C. 671(5))" and inserting "section 2200 of the Homeland Security Act of 2002"; and

(B) by amending paragraph (7) to read as follows:

"(7) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.";

(2) in subsection (c)(3)(B), by striking "section 2201(5) of the Homeland Security Act of 2002 (6 U.S.C. 651(5))" and inserting "section 2200 of the Homeland Security Act of 2002"; and

(3) in subsection (d)—

(A) by striking "section 2215" and inserting "section 2218"; and

(B) by striking ", as added by this section".

(d) National Security Act of 1947.—Section 113B of the National Security Act of 1947 (50 U.S.C. 3049a(b)(4)) is amended by striking "section 226 of the Homeland Security Act of 2002 (6 U.S.C. 147)" and inserting "section 2206 of the Homeland Security Act of 2002".

(e) IoT Cybersecurity Improvement Act of 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c) is amended by striking "section 2209(m)" and inserting "section 2209(l)".

(f) Small Business Act.—Section 21(a)(8)(B) of the Small Business Act (15 U.S.C.

648(a)(8)(B)) is amended by striking "section 2209(a)" and inserting "section 2200".

(g) Title 46.—Section 70101(2) of title 46, United States Code, is amended by striking "section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)" and inserting "section 2200 of the Homeland Security Act of 2002".