and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4813. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4814. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4815. Mr. SANDERS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4816. Mr. COONS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4817. Ms. SINEMA submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4818. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4819. Mr. SULLIVAN (for himself and Mr. WHITEHOUSE) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4820. Mr. COTTON (for himself, Mr. MANCHIN, Mr. TUBERVILLE, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4821. Mr. BROWN (for himself and Mr. WARNER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4822. Mrs. BLACKBURN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4823. Mr. MARKEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4824. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4825. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4826. Mr. TOOMEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4827. Mr. ROUNDS (for himself and Mr. VAN HOLLEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4828. Mr. BLUMENTHAL submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4829. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4830. Mr. MANCHIN (for himself, Mrs. CAPITO, Mrs. HYDE-SMITH, Mr. ROMNEY, Mr. COTTON, Mrs. BLACKBURN, and Mr. TESTER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4831. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4832. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4833. Mr. BARRASSO (for himself, Mr. CRUZ, and Mr. JOHNSON) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 4783. Mr. HAGERTY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. 1283. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES AGAINST ISIS AND ASSOCIATED FORCES IN IRAQ.

The President is authorized to use the Armed Forces of the United States as the President determines to be necessary and appropriate in order to defend the national security of the United States against the threat posed by the Islamic State of Iraq and Syria (ISIS) and associated forces in Iraq.

SEC. 1284. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES TO PROTECT UNITED STATES DIPLOMATS AND UNITED STATES DIPLOMATIC FACILITIES IN IRAQ AGAINST TERRORIST ATTACKS.

The President is authorized to use the Armed Forces of the United States as the President determines to be necessary and appropriate in order to protect United States diplomats and United States diplomatic facilities in Iraq against terrorist attacks.

SEC. 1285. RULE OF CONSTRUCTION REGARDING THE CONSTITUTIONAL POWERS OF THE PRESIDENT AS COMMANDER-IN-CHIEF.

Nothing in this Act shall be construed to infringe upon the constitutional powers of the President as Commander-in-Chief under Article II of the Constitution of the United States.

SA 4784. Mr. KING (for himself, Mr. ROUNDS, Mr. SASSE, Ms. ROSEN, Ms. HASSAN, and Mr. OSSOFF) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—DEFENSE OF UNITED STATES INFRASTRUCTURE

SEC. 5001. SHORT TITLE.

This division may be cited as the ''Defense of United States Infrastructure Act of 2021''.

SEC. 5002. DEFINITIONS.

In this division:

(1) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(2) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given such term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(3) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

TITLE LI—INVESTING IN CYBER RESILIENCY IN CRITICAL INFRASTRUCTURE

SEC. 5101. NATIONAL RISK MANAGEMENT CYCLE.

(a) AMENDMENTS.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2202(c) (6 U.S.C. 652(c))—

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

(B) in the first paragraph designated as paragraph (12), relating to the Cybersecurity State Coordinator—

(i) by striking ''section 2215'' and inserting ''section 2217''; and

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

(C) by redesignating the second and third paragraphs designated as paragraph (12) as paragraphs (13) and (14), respectively;

(2) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(3) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(4) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(5) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217;

(6) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216; and

(7) by adding at the end the following:

''SEC. 2220A. NATIONAL RISK MANAGEMENT CYCLE.

''(a) NATIONAL CRITICAL FUNCTIONS DEFINED.—In this section, the term 'national critical functions' means the functions of

government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

''(b) NATIONAL RISK MANAGEMENT CYCLE.—

''(1) RISK IDENTIFICATION AND ASSESSMENT.—

''(A) IN GENERAL.—The Secretary, acting through the Director, shall establish a recurring process by which to identify, assess, and prioritize risks to critical infrastructure, considering both cyber and physical threats, the associated likelihoods, vulnerabilities, and consequences, and the resources necessary to address them.

''(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult with, and request and collect information to support analysis from, Sector Risk Management Agencies, critical infrastructure owners and operators, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the National Cyber Director.

''(C) PUBLICATION.—Not later than 180 days after the date of enactment of this section, the Secretary shall publish in the Federal Register procedures for the process established under subparagraph (A), subject to any redactions the Secretary determines are necessary to protect classified or other sensitive information.

''(D) REPORT.—The Secretary shall submit to the President, 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 risks identified by the process established under subparagraph (A)—

''(i) not later than 1 year after the date of enactment of this section; and

''(ii) not later than 1 year after the date on which the Secretary submits a periodic evaluation described in section 9002(b)(2) of title XC of division H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283).

''(2) NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

''(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers each report required under paragraph (1), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

''(B) ELEMENTS.—Each strategy delivered under subparagraph (A) shall—

''(i) identify, assess, and prioritize areas of risk to critical infrastructure that would compromise or disrupt national critical functions impacting national security, economic security, or public health and safety;

''(ii) assess the implementation of the previous national critical infrastructure resilience strategy, as applicable;

''(iii) identify and outline current and proposed national-level actions, programs, and efforts to be taken to address the risks identified;

''(iv) identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each; and

''(v) request any additional authorities necessary to successfully execute the strategy.

''(C) FORM.—Each strategy delivered under subparagraph (A) shall be unclassified, but may contain a classified annex.

''(3) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date on which the President delivers a strategy under this section, and every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate committees of Congress on—

''(A) the national risk management cycle activities undertaken pursuant to the strategy; and

''(B) the amounts and timeline for funding that the Secretary has determined would be necessary to address risks and successfully execute the full range of activities proposed by the strategy.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF CONTENTS.—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 striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity education and training programs.
''Sec. 2220A. National risk management cycle.''.

(2) ADDITIONAL TECHNICAL AMENDMENT.—

(A) 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''.

(B) EFFECTIVE DATE.—The amendment made by subparagraph (A) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

TITLE LII—IMPROVING THE ABILITY OF THE FEDERAL GOVERNMENT TO ASSIST IN ENHANCING CRITICAL INFRASTRUCTURE CYBER RESILIENCE

SEC. 5201. INSTITUTE A 5-YEAR TERM FOR THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) IN GENERAL.—Subsection (b)(1) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), is amended by inserting ''The term of office of an individual serving as Director shall be 5 years.'' after ''who shall report to the Secretary.''.

(b) TRANSITION RULES.—The amendment made by subsection (a) shall take effect on the first appointment of an individual to the position of Director of the Cybersecurity and Infrastructure Security Agency, by and with the advice and consent of the Senate, that is made on or after the date of enactment of this Act.

SEC. 5202. CYBER THREAT INFORMATION COLLABORATION ENVIRONMENT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term ''critical infrastructure information'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(2) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(3) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(4) ENVIRONMENT.—The term ''environment'' means the information collaboration environment established under subsection (b).

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''information sharing and analysis organization'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(6) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(b) PROGRAM.—The Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall carry out a program under which the Secretary shall develop an information collaboration environment consisting of a digital environment containing technical tools for information analytics and a portal through which relevant parties may submit and automate information inputs and access the environment in order to enable interoperable data flow that enable Federal and non-Federal entities to identify, mitigate, and prevent malicious cyber activity to—

(1) provide limited access to appropriate and operationally relevant data from unclassified and classified intelligence about cybersecurity risks and cybersecurity threats, as well as malware forensics and data from network sensor programs, on a platform that enables query and analysis;

(2) enable cross-correlation of data on cybersecurity risks and cybersecurity threats at the speed and scale necessary for rapid detection and identification;

(3) facilitate a comprehensive understanding of cybersecurity risks and cybersecurity threats; and

(4) facilitate collaborative analysis between the Federal Government and public and private sector critical infrastructure entities and information and analysis organizations.

(c) IMPLEMENTATION OF INFORMATION COLLABORATION ENVIRONMENT.—

(1) EVALUATION.—Not later than 180 days after the date of enactment of this Act, the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall—

(A) identify, inventory, and evaluate existing Federal sources of classified and unclassified information on cybersecurity threats;

(B) evaluate current programs, applications, or platforms intended to detect, identify, analyze, and monitor cybersecurity risks and cybersecurity threats;

(C) consult with public and private sector critical infrastructure entities to identify public and private critical infrastructure cyber threat capabilities, needs, and gaps; and

(D) identify existing tools, capabilities, and systems that may be adapted to achieve the purposes of the environment in order to maximize return on investment and minimize cost.

(2) IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 1 year after completing the evaluation required under paragraph (1)(B), the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in consultation with the Secretary of Defense, the Director of National Intelligence, and

the Attorney General, shall begin implementation of the environment to enable participants in the environment to develop and run analytic tools referred to in subsection (b) on specified data sets for the purpose of identifying, mitigating, and preventing malicious cyber activity that is a threat to public and private critical infrastructure.

(B) REQUIREMENTS.—The environment and the use of analytic tools referred to in subsection (b) shall—

(i) operate in a manner consistent with relevant privacy, civil rights, and civil liberties policies and protections, including such policies and protections established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(ii) account for appropriate data interoperability requirements;

(iii) enable integration of current applications, platforms, data, and information, including classified information, in a manner that supports the voluntary integration of unclassified and classified information on cybersecurity risks and cybersecurity threats;

(iv) incorporate tools to manage access to classified and unclassified data, as appropriate;

(v) ensure accessibility by entities the Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, determines appropriate;

(vi) allow for access by critical infrastructure stakeholders and other private sector partners, at the discretion of the Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General;

(vii) deploy analytic tools across classification levels to leverage all relevant data sets, as appropriate;

(viii) identify tools and analytical software that can be applied and shared to manipulate, transform, and display data and other identified needs; and

(ix) anticipate the integration of new technologies and data streams, including data from government-sponsored network sensors or network-monitoring programs deployed in support of non-Federal entities.

(3) ANNUAL REPORT REQUIREMENT ON THE IMPLEMENTATION, EXECUTION, AND EFFECTIVENESS OF THE PROGRAM.—Not later than 1 year after the date of enactment of this Act, and every year thereafter until the date that is 1 year after the program under this section terminates under subsection (g), the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, the Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives a report that details—

(A) Federal Government participation in the environment, including the Federal entities participating in the environment and the volume of information shared by Federal entities into the environment;

(B) non-Federal entities' participation in the environment, including the non-Federal entities participating in the environment and the volume of information shared by non-Federal entities into the environment;

(C) the impact of the environment on positive security outcomes for the Federal Government and non-Federal entities;

(D) barriers identified to fully realizing the benefit of the environment both for the Federal Government and non-Federal entities;

(E) additional authorities or resources necessary to successfully execute the environment; and

(F) identified shortcomings or risks to data security and privacy, and the steps necessary to improve the mitigation of the shortcomings or risks.

(d) CYBER THREAT DATA INTEROPERABILITY REQUIREMENTS.—

(1) ESTABLISHMENT.—The Secretary, in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall identify or establish data interoperability requirements for non-Federal entities to participate in the environment.

(2) DATA STREAMS.—The Secretary, in coordination with the heads of appropriate departments and agencies, shall identify, designate, and periodically update programs that shall participate in or be interoperable with the environment, in a manner consistent with data security standards under Federal law, which may include—

(A) network-monitoring and intrusion detection programs;

(B) cyber threat indicator sharing programs;

(C) certain government-sponsored network sensors or network-monitoring programs;

(D) incident response and cybersecurity technical assistance programs; or

(E) malware forensics and reverse-engineering programs.

(3) DATA GOVERNANCE.—The Secretary, in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall establish procedures and data governance structures, as necessary, to protect data shared in the environment, comply with Federal regulations and statutes, and respect existing consent agreements with private sector critical infrastructure entities that apply to critical infrastructure information.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall change existing ownership or protection of, or policies and processes for access to, agency data.

(e) NATIONAL SECURITY SYSTEMS.—Nothing in this section shall apply to national security systems, as defined in section 3552 of title 44, United States Code, or to cybersecurity threat intelligence related to such systems, without the consent of the relevant element of the intelligence community, as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(f) PROTECTION OF INTELLIGENCE SOURCES AND METHODS.—The Director of National Intelligence shall ensure that any information sharing conducted under this section shall protect intelligence sources and methods from unauthorized disclosure in accordance with section 102A(i) of the National Security Act (50 U.S.C. 3024(i)).

(g) DURATION.—The program under this section shall terminate on the date that is 5 years after the date of enactment of this Act.

TITLE LIII—ENABLING THE NATIONAL CYBER DIRECTOR

SEC. 5401. ESTABLISHMENT OF HIRING AUTHORITIES FOR THE OFFICE OF THE NATIONAL CYBER DIRECTOR.

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the National Cyber Director.

(2) EXCEPTED SERVICE.—The term ''excepted service'' has the meaning given such term in section 2103 of title 5, United States Code.

(3) OFFICE.—The term ''Office'' means the Office of the National Cyber Director.

(4) QUALIFIED POSITION.—The term ''qualified position'' means a position identified by the Director under subsection (b)(1)(A), in which the individual occupying such position performs, manages, or supervises functions that execute the responsibilities of the Office.

(b) HIRING PLAN.—The Director shall, for purposes of carrying out the functions of the Office—

(1) craft an implementation plan for positions in the excepted service in the Office, which shall propose—

(A) qualified positions in the Office, as the Director determines necessary to carry out the responsibilities of the Office; and

(B) subject to the requirements of paragraph (2), rates of compensation for an individual serving in a qualified position;

(2) propose rates of basic pay for qualified positions, which shall—

(A) be determined in relation to the rates of pay provided for employees in comparable positions in the Office, in which the employee occupying the comparable position performs, manages, or supervises functions that execute the mission of the Office; and

(B) subject to the same limitations on maximum rates of pay and consistent with section 5341 of title 5, United States Code, adopt such provisions of that title to provide for prevailing rate systems of basic pay and apply those provisions to qualified positions for employees in or under which the Office may employ individuals described by section 5342(a)(2)(A) of such title; and

(3) craft proposals to provide—

(A) employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5, United States Code; and

(B) employees in a qualified position for which the Director proposes a rate of basic pay under paragraph (2) an allowance under section 5941 of title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such section, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

SA 4785. Mr. OSSOFF (for himself, Mr. KING, Ms. CORTEZ MASTO, Mr. ROUNDS, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. DR. DAVID SATCHER CYBERSECURITY EDUCATION GRANT PROGRAM.

(a) SHORT TITLE.—This section may be cited as the ''Cybersecurity Opportunity Act''.

(b) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) ENROLLMENT OF NEEDY STUDENTS.—The term ''enrollment of needy students'' has the meaning given the term in section 312(d) of the Higher Education Act of 1965 (20 U.S.C. 1058(d)).

(3) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ''historically Black college or university'' has the meaning given the term ''part B institution'' as defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(4) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(5) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means an institution listed in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(c) AUTHORIZATION OF GRANTS.—

(1) IN GENERAL.—Subject to the availability of appropriations, the Director shall carry out the Dr. David Satcher Cybersecurity Education Grant Program by—

(A) awarding grants to assist institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to establish or expand cybersecurity programs, to build and upgrade institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities, and to support such institutions on the path to producing qualified entrants in the cybersecurity workforce or becoming a National Center of Academic Excellence in Cybersecurity; and

(B) awarding grants to build capacity at institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to expand cybersecurity education opportunities, cybersecurity programs, cybersecurity research, and cybersecurity partnerships with public and private entities.

(2) RESERVATION.—The Director shall award not less than 50 percent of the amount available for grants under this section to historically Black colleges and universities and minority-serving institutions.

(3) COORDINATION.—The Director shall carry out this section in consultation with appropriate Federal agencies.

(4) SUNSET.—The Director's authority to award grants under paragraph (1) shall terminate on the date that is 5 years after the date the Director first awards a grant under paragraph (1).

(d) APPLICATIONS.—An eligible institution seeking a grant under subsection (a) shall submit an application to the Director at such time, in such manner, and containing such information as the Director may reasonably require, including a statement of how the institution will use the funds awarded through the grant to expand cybersecurity education opportunities at the eligible institution.

(e) ACTIVITIES.—An eligible institution that receives a grant under this section may use the funds awarded through such grant for increasing research, education, technical, partnership, and innovation capacity, including for—

(1) building and upgrading institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities;

(2) building and upgrading institutional capacity to provide hands-on research and training experiences for undergraduate and graduate students; and

(3) outreach and recruitment to ensure students are aware of such new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities.

(f) REPORTING REQUIREMENTS.—Not later than—

(1) 1 year after the effective date of this section, as provided in subsection (h), and annually thereafter until the Director submits the report under paragraph (2), the Director shall prepare and submit to Congress a report on the status and progress of implementation of the grant program under this section, including on the number and nature of institutions participating, the number and nature of students served by institutions receiving grants, the level of funding provided to grant recipients, the types of activities being funded by the grants program, and plans for future implementation and development; and

(2) 5 years after the effective date of this section, as provided in subsection (h), the Director shall prepare and submit to Congress a report on the status of cybersecurity education programming and capacity-building at institutions receiving grants under this section, including changes in the scale and scope of these programs, associated facilities, or in accreditation status, and on the educational and employment outcomes of students participating in cybersecurity programs that have received support under this section.

(g) PERFORMANCE METRICS.—The Director shall establish performance metrics for grants awarded under this section.

(h) EFFECTIVE DATE.—This section shall take effect 1 year after the date of enactment of this Act.

SA 4786. Mr. MENENDEZ (for himself, Mr. SCHUMER, Mr. BOOKER, Mrs. GILLIBRAND, Mr. BLUMENTHAL, and Mr. MURPHY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. APPROPRIATIONS FOR CATCH-UP PAYMENTS.

Section 404(d)(4)(C) of the Justice for United States Victims of State Sponsored Terrorism Act (34 U.S.C. 20144(d)(4)(C)) is amended by adding at the end the following:

''(iv) FUNDING.—

''(I) APPROPRIATIONS.—

''(aa) IN GENERAL.—There are authorized to be appropriated and there are appropriated to the Fund such sums as may be necessary to carry out this subparagraph, to remain available until expended.

''(bb) EMERGENCY DESIGNATION.—The amounts provided under this subclause are designated as an emergency requirement pursuant to section 4(g) of the Statutory Pay-As-You-Go Act of 2010 (2 U.S.C. 933(g)).

''(cc) DESIGNATION IN THE HOUSE AND SENATE.—This subclause is designated by the Congress as being for an emergency requirement pursuant to section 4001(a)(1) and section 4001(b) of S. Con. Res. 14 (117th Congress), the concurrent resolution on the budget for fiscal year 2022.

''(II) LIMITATION.—Amounts appropriated pursuant to subclause (I) may not be used for a purpose other than to make lump sum catch-up payments under this subparagraph.''.

SA 4787. Mrs. SHAHEEN (for herself and Ms. COLLINS) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of title VII, add the following:

Subtitle D—Access to Contraception

SEC. 761. SHORT TITLE.

This subtitle may be cited as the ''Access to Contraception for Servicemembers and Dependents Act of 2021''.

SEC. 762. FINDINGS.

Congress finds the following:

(1) Women are serving in the Armed Forces at increasing rates, playing a critical role in the national security of the United States. Women comprise more than 18 percent of members of the Armed Forces, and as of fiscal year 2019, more than 390,000 women serve on active duty in the Armed Forces or in the reserve components. An estimated several thousand transgender men also serve on active duty in the Armed Forces and in the reserve components, in addition to non-binary members and those who identify with a different gender.

(2) Ninety-five percent of women serving in the Armed Forces are of reproductive age and as of 2019, more than 700,000 female spouses and dependents of members of the Armed Forces on active duty are of reproductive age.

(3) The TRICARE program covered more than 1,570,000 women of reproductive age in 2019, including spouses and dependents of members of the Armed Forces on active duty. Additionally, thousands of transgender dependents of members of the Armed Forces are covered by the TRICARE program.

(4) The right to access contraception is grounded in the principle that contraception and the ability to determine if and when to have children are inextricably tied to one's wellbeing, equality, and ability to determine the course of one's life. These protections have helped access to contraception become a driving force in improving the health and financial security of individuals and their families.

(5) Access to contraception is critical to the health of every individual capable of becoming pregnant. This subtitle is intended to apply to all individuals with the capacity for pregnancy, including cisgender women, transgender men, non-binary individuals, those who identify with a different gender, and others.

(6) Studies have shown that when cost barriers to the full range of methods of contraception are eliminated, patients are more likely to use the contraceptive method that meets their needs, and therefore use contraception correctly and more consistently, reducing the risk of unintended pregnancy.

(7) Under the TRICARE program, members of the Armed Forces on active duty have full coverage of all prescription drugs, including contraception, without cost-sharing requirements, in line with the Patient Protection and Affordable Care Act (Public Law 111–148), which requires coverage of all contraceptive methods approved by the Food and Drug Administration for women and related services and education and counseling. However, members not on active duty and dependents of members do not have similar coverage of all methods of contraception approved by the Food and Drug Administration without cost-sharing when they obtain the contraceptive outside of a military medical treatment facility.

(8) In order to fill gaps in coverage and access to preventive care critical for women's

health, the Patient Protection and Affordable Care Act (Public Law 111–148) requires all non-grandfathered individual and group health plans to cover without cost-sharing preventive services, including a set of evidence-based preventive services for women supported by the Health Resources and Services Administration of the Department of Health and Human Services. These women's preventive services include the full range of female-controlled contraceptive methods, effective family planning practices, and sterilization procedures, approved by the Food and Drug Administration. The Health Resources and Services Administration has affirmed that contraceptive care includes contraceptive counseling, initiation of contraceptive use, and follow-up care (such as management, evaluation, and changes to and removal or discontinuation of the contraceptive method).

(9) The Defense Advisory Committee on Women in the Services has recommended that all the Armed Forces, to the extent that they have not already, implement initiatives that inform members of the Armed Forces of the importance of family planning, educate them on methods of contraception, and make various methods of contraception available, based on the finding that family planning can increase the overall readiness and quality of life of all members of the Armed Forces.

(10) The military departments received more than 7,800 reports of sexual assaults involving members of the Armed Forces as victims or subjects during fiscal year 2019. Through regulations, the Department of Defense already supports a policy of ensuring that members of the Armed Forces who are sexually assaulted have access to emergency contraception, and the initiation of contraception if desired and medically appropriate.

SEC. 763. CONTRACEPTION COVERAGE PARITY UNDER THE TRICARE PROGRAM.

(a) PHARMACY BENEFITS PROGRAM.—Section 1074g(a)(6) of title 10, United States Code, is amended by adding at the end the following new subparagraph:

''(D) Notwithstanding subparagraphs (A), (B), and (C), cost-sharing requirements may not be imposed and cost-sharing amounts may not be collected with respect to any eligible covered beneficiary for any prescription contraceptive on the uniform formulary provided through a retail pharmacy described in paragraph (2)(E)(ii) or through the national mail-order pharmacy program.''.

(b) TRICARE SELECT.—Section 1075 of such title is amended—

(1) in subsection (c), by adding at the end the following new paragraph:

''(4)(A) Notwithstanding any other provision of this section, cost-sharing requirements may not be imposed and cost-sharing amounts may not be collected with respect to any beneficiary under this section for a service described in subparagraph (B) that is provided by a network provider.

''(B) A service described in this subparagraph is any method of contraception approved by the Food and Drug Administration, any contraceptive care (including with respect to insertion, removal, and follow up), any sterilization procedure, or any patient education or counseling service provided in connection with any such method, care, or procedure.''; and

(2) in subsection (f), by striking ''calculated as'' and inserting ''calculated (except as provided in subsection (c)(4)) as''.

(c) TRICARE PRIME.—Section 1075a of such title is amended by adding at the end the following new subsection:

''(d) PROHIBITION ON COST-SHARING FOR CERTAIN SERVICES.—(1) Notwithstanding subsections (a), (b), and (c), cost-sharing requirements may not be imposed and cost-sharing amounts may not be collected with respect to any beneficiary enrolled in TRICARE Prime for a service described in paragraph (2) that is provided under TRICARE Prime.

''(2) A service described in this paragraph is any method of contraception approved by the Food and Drug Administration, any contraceptive care (including with respect to insertion, removal, and follow up), any sterilization procedure, or any patient education or counseling service provided in connection with any such method, care, or procedure.''.

SEC. 764. PREGNANCY PREVENTION ASSISTANCE AT MILITARY MEDICAL TREATMENT FACILITIES FOR SEXUAL ASSAULT SURVIVORS.

(a) IN GENERAL.—Chapter 55 of title 10, United States Code, is amended by inserting after section 1074o the following new section:

''§ 1074p. Provision of pregnancy prevention assistance at military medical treatment facilities

''(a) INFORMATION AND ASSISTANCE.—The Secretary of Defense shall promptly furnish to sexual assault survivors at each military medical treatment facility the following:

''(1) Comprehensive, medically and factually accurate, and unbiased written and oral information about all methods of emergency contraception approved by the Food and Drug Administration.

''(2) Upon request by the sexual assault survivor, emergency contraception or, if applicable, a prescription for emergency contraception.

''(3) Notification of the right of the sexual assault survivor to confidentiality with respect to the information and care and services furnished under this section.

''(b) INFORMATION.—The Secretary shall ensure that information provided pursuant to subsection (a) is provided in language that—

''(1) is clear and concise;

''(2) is readily comprehensible; and

''(3) meets such conditions (including conditions regarding the provision of information in languages other than English) as the Secretary may prescribe in regulations to carry out this section.

''(c) DEFINITIONS.—In this section:

''(1) The term 'sexual assault survivor' means any individual who presents at a military medical treatment facility and—

''(A) states to personnel of the facility that the individual experienced a sexual assault;

''(B) is accompanied by another person who states that the individual experienced a sexual assault; or

''(C) whom the personnel of the facility reasonably believes to be a survivor of sexual assault.

''(2) The term 'sexual assault' means the conduct described in section 1565b(c) of this title that may result in pregnancy.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by inserting after the item relating to section 1074o the following new item:

''1074p. Provision of pregnancy prevention assistance at military medical treatment facilities.''.

SEC. 765. EDUCATION ON FAMILY PLANNING FOR MEMBERS OF THE ARMED FORCES.

(a) EDUCATION PROGRAMS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall establish a uniform standard curriculum to be used in education programs on family planning for all members of the Armed Forces, including both men and women members.

(2) TIMING.—Education programs under paragraph (1) shall be provided to members of the Armed Forces as follows:

(A) During the first year of service of the member.

(B) At such other times as each Secretary of a military department determines appropriate with respect to members of the Armed Forces under the jurisdiction of such Secretary.

(3) SENSE OF CONGRESS.—It is the sense of Congress that the education programs under paragraph (1) should be evidence-informed and use the latest technology available to efficiently and effectively deliver information to members of the Armed Forces.

(b) ELEMENTS.—The uniform standard curriculum for education programs under subsection (a) shall include the following:

(1) Information for members of the Armed Forces on active duty to make informed decisions regarding family planning.

(2) Information about the prevention of unintended pregnancy and sexually transmitted infections, including human immunodeficiency virus (commonly known as ''HIV'').

(3) Information on—

(A) the importance of providing comprehensive family planning for members of the Armed Forces, including commanding officers; and

(B) the positive impact family planning can have on the health and readiness of the Armed Forces.

(4) Current, medically accurate information.

(5) Clear, user-friendly information on—

(A) the full range of methods of contraception approved by the Food and Drug Administration; and

(B) where members of the Armed Forces can access their chosen method of contraception.

(6) Information on all applicable laws and policies so that members of the Armed Forces are informed of their rights and obligations.

(7) Information on the rights of patients to confidentiality.

(8) Information on the unique circumstances encountered by members of the Armed Forces and the effects of such circumstances on the use of contraception.

SA 4788. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

On page 621, strike lines 14 through 24 and insert the following:

cross-strait relations;

(7) reinforcing the status of the Republic of Singapore as a Major Security Cooperation Partner of the United States and continuing to strengthen defense and security cooperation between the military forces of the Republic of Singapore and the Armed Forces of the United States, including through participation in combined exercises and training, including the use of the Foreign Military Sales Training Center at Ebbing Air National Guard Base in Fort Smith, Arkansas; and

(8) ensuring that the allies and partners referred to in paragraphs (1) through (7) contribute more than 50 percent of the total cost of mutual defense efforts in the Indo-Pacific region.

SA 4789. Mr. LEE submitted an amendment intended to be proposed to

amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

On page 578, strike lines 14 through 19 and insert the following:

(1) by striking ''fiscal year 2021'' and inserting ''fiscal year 2022''; and

(2) by striking '', as specified in the funding tables in division D of this Act''.

SA 4790. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

Strike section 1061.

SA 4791. Mr. MORAN (for himself and Ms. ROSEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle C of title VII, add the following:

SEC. 744. GRANT PROGRAM FOR INCREASED COOPERATION ON POST-TRAUMATIC STRESS DISORDER RESEARCH BETWEEN UNITED STATES AND ISRAEL.

(a) FINDINGS AND SENSE OF CONGRESS.—

(1) FINDINGS.—Congress makes the following findings:

(A) The Department of Veterans Affairs reports that between 11 and 20 percent of veterans who served in Operation Iraqi Freedom and Operation Enduring Freedom have post-traumatic stress disorder (in this paragraph referred to as ''PTSD'') in a given year. In addition, that figure amounts to about 12 percent of Gulf War veterans and up to 30 percent of Vietnam veterans.

(B) The Department of Veterans Affairs reports that among women veterans of the conflicts in Iraq and Afghanistan, almost 20 percent have been diagnosed with PTSD.

(C) It is thought that 70 percent of individuals in the United States have experienced at least one traumatic event in their lifetime, and approximately 20 percent of those individuals have struggled or continue to struggle with symptoms of PTSD.

(D) Studies show that PTSD has links to homelessness and substance abuse in the United States. The Department of Veterans Affairs estimates that approximately 11 percent of the homeless population are veterans and the Substance Abuse and Mental Health Services Administration estimates that about seven percent of veterans have a substance abuse disorder.

(E) Our ally Israel, under constant attack from terrorist groups, experiences similar issues with Israeli veterans facing symptoms of PTSD. The National Center for Traumatic Stress and Resilience at Tel Aviv University found that five to eight percent of combat soldiers experience some form of PTSD, and during wartime, that figure rises to 15 to 20 percent.

(F) Current treatment options in the United States focus on cognitive therapy, exposure therapy, or eye movement desensitization and reprocessing, but the United States must continue to look for more effective treatments. Several leading hospitals, academic institutions, and nonprofit organizations in Israel dedicate research and services to treating PTSD.

(2) SENSE OF CONGRESS.—It is the sense of Congress that the Secretary of Defense, acting through the Psychological Health and Traumatic Brain Injury Research Program, should seek to explore scientific collaboration between academic institutions and nonprofit research entities in the United States and institutions in Israel with expertise in researching, diagnosing, and treating post-traumatic stress disorder.

(b) GRANT PROGRAM.—

(1) IN GENERAL.—The Secretary of Defense, in coordination with the Secretary of Veterans Affairs and the Secretary of State, shall award grants to eligible entities to carry out collaborative research between the United States and Israel with respect to post-traumatic stress disorders.

(2) AGREEMENT.—The Secretary of Defense shall carry out the grant program under this section in accordance with the Agreement on the United States-Israel binational science foundation with exchange of letters, signed at New York September 27, 1972, and entered into force on September 27, 1972.

(c) ELIGIBLE ENTITIES.—To be eligible to receive a grant under this section, an entity shall be an academic institution or a nonprofit entity located in the United States.

(d) AWARD.—The Secretary shall award grants under this section to eligible entities that—

(1) carry out a research project that—

(A) addresses a requirement in the area of post-traumatic stress disorders that the Secretary determines appropriate to research using such grant; and

(B) is conducted by the eligible entity and an entity in Israel under a joint research agreement; and

(2) meet such other criteria that the Secretary may establish.

(e) APPLICATION.—To be eligible to receive a grant under this section, an eligible entity shall submit an application to the Secretary at such time, in such manner, and containing such commitments and information as the Secretary may require.

(f) REPORTS.—Not later than 180 days after the date on which an eligible entity completes a research project using a grant under this section, the Secretary shall submit to Congress a report that contains—

(1) a description of how the eligible entity used the grant; and

(2) an evaluation of the level of success of the research project.

(g) TERMINATION.—The authority to award grants under this section shall terminate on the date that is seven years after the date on which the first such grant is awarded.

SA 4792. Mrs. MURRAY (for herself and Mr. MANCHIN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of title XXXI, add the following:

Subtitle F—Toxic Exposure Safety

SEC. 3161. SHORT TITLE.

This subtitle may be cited as the ''Toxic Exposure Safety Act of 2021''.

SEC. 3162. PROVIDING INFORMATION REGARDING DEPARTMENT OF ENERGY FACILITIES.

Subtitle E of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s et seq.) is amended by inserting after section 3681 the following:

''SEC. 3681A. COMPLETION AND UPDATES OF SITE EXPOSURE MATRICES.

''(a) DEFINITION.—In this section, the term 'site exposure matrices' means an exposure assessment of a Department of Energy facility that identifies the toxic substances or processes that were used in each building or process of the facility, including the trade name (if any) of the substance.

''(b) IN GENERAL.—Not later than 180 days after the date of enactment of the Toxic Exposure Safety Act of 2021, the Secretary of Labor shall, in coordination with the Secretary of Energy, create or update site exposure matrices for each Department of Energy facility based on the records, files, and other data provided by the Secretary of Energy and such other information as is available, including information available from the former worker medical screening programs of the Department of Energy.

''(c) PERIODIC UPDATE.—Beginning 90 days after the initial creation or update described in subsection (b), and each 90 days thereafter, the Secretary shall update the site exposure matrices with all information available as of such time from the Secretary of Energy.

''(d) INFORMATION.—The Secretary of Energy shall furnish to the Secretary of Labor any information that the Secretary of Labor finds necessary or useful for the production of the site exposure matrices under this section, including records from the Department of Energy former worker medical screening program.

''(e) PUBLIC AVAILABILITY.—The Secretary of Labor shall make available to the public, on the primary website of the Department of Labor—

''(1) the site exposure matrices, as periodically updated under subsections (b) and (c);

''(2) each site profile prepared under section 3633(a);

''(3) any other database used by the Secretary of Labor to evaluate claims for compensation under this title; and

''(4) statistical data, in the aggregate and disaggregated by each Department of Energy facility, regarding—

''(A) the number of claims filed under this subtitle;

''(B) the types of illnesses claimed;

''(C) the number of claims filed for each type of illness and, for each claim, whether the claim was approved or denied;

''(D) the number of claimants receiving compensation; and

''(E) the length of time required to process each claim, as measured from the date on which the claim is filed to the final disposition of the claim.

''(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary of Energy, for fiscal year 2022 and each succeeding year, such sums as may be

necessary to support the Secretary of Labor in creating or updating the site exposure matrices.''.

SEC. 3163. ASSISTING CURRENT AND FORMER EMPLOYEES UNDER THE EEOICPA.

(a) PROVIDING INFORMATION AND OUTREACH.—Subtitle A of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384d et seq.) is amended—

(1) by redesignating section 3614 as section 3616; and

(2) by inserting after section 3613 the following:

''SEC. 3614. INFORMATION AND OUTREACH.

''(a) ESTABLISHMENT OF TOLL-FREE INFORMATION PHONE NUMBER.—By not later than January 1, 2023, the Secretary of Labor shall establish a toll-free phone number that current or former employees of the Department of Energy, or current or former Department of Energy contractor employees, may use in order to receive information regarding—

''(1) the compensation program under subtitle B or E;

''(2) information regarding the process of submitting a claim under either compensation program;

''(3) assistance in completing the occupational health questionnaire required as part of a claim under subtitle B or E;

''(4) the next steps to take if a claim under subtitle B or E is accepted or denied; and

''(5) such other information as the Secretary determines necessary to further the purposes of this title.

''(b) ESTABLISHMENT OF RESOURCE AND ADVOCACY CENTERS.—

''(1) IN GENERAL.—By not later than January 1, 2024, the Secretary of Energy, in coordination with the Secretary of Labor, shall establish a resource and advocacy center at each Department of Energy facility where cleanup operations are being carried out, or have been carried out, under the environmental management program of the Department of Energy. Each such resource and advocacy center shall assist current or former Department of Energy employees and current or former Department of Energy contractor employees, by enabling the employees and contractor employees to—

''(A) receive information regarding all related programs available to them relating to potential claims under this title, including—

''(i) programs under subtitles B and E; and

''(ii) the former worker medical screening program of the Department of Energy; and

''(B) navigate all such related programs.

''(2) COORDINATION.—The Secretary of Energy shall integrate other programs available to current and former employees, and current or former Department of Energy contractor employees, which are related to the purposes of this title, with the resource and advocacy centers established under paragraph (1), as appropriate.

''(c) INFORMATION.—The Secretary of Labor shall develop and distribute, through the resource and advocacy centers established under subsection (b) and other means, information (which may include responses to frequently asked questions) for current or former employees or current or former Department of Energy contractor employees about the programs under subtitles B and E and the claims process under such programs.

''(d) COPY OF EMPLOYEE'S CLAIMS RECORDS.—

''(1) IN GENERAL.—The Secretary of Labor shall, upon the request of a current or former employee or Department of Energy contractor employee, provide the employee with a complete copy of all records or other materials held by the Department of Labor relating to the employee's claim under subtitle B or E.

''(2) CHOICE OF FORMAT.—The Secretary of Labor shall provide the copy of records described in paragraph (1) to an employee in electronic or paper form, as selected by the employee.

''(e) CONTACT OF EMPLOYEES BY INDUSTRIAL HYGIENISTS.—The Secretary of Labor shall allow industrial hygienists to contact and interview current or former employees or Department of Energy contractor employees regarding the employee's claim under subtitle B or E.''.

(b) EXTENDING APPEAL PERIOD.—Section 3677(a) of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s–6(a)) is amended by striking ''60 days'' and inserting ''180 days''.

(c) FUNDING.—Section 3684 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s–13) is amended—

(1) by striking ''There is authorized'' and inserting the following:

''(a) IN GENERAL.—There is authorized'';

(2) by inserting before the period at the end the following: '', including the amounts necessary to carry out the requirements of section 3681A''; and

(3) by adding at the end the following:

''(b) ADMINISTRATIVE COSTS FOR DEPARTMENT OF ENERGY.—There is authorized to be appropriated to the Secretary of Energy for fiscal year 2022 and each succeeding year such sums as may be necessary to support the Secretary in carrying out the requirements of this title, including section 3681A.''.

(d) ADVISORY BOARD ON TOXIC SUBSTANCES AND WORKER HEALTH.—Section 3687 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s–16) is amended—

(1) in subsection (b)—

(A) in paragraph (1)(F), by striking ''and'' after the semicolon;

(B) in paragraph (2), by striking the period at the end and inserting a semicolon; and

(C) by adding at the end the following:

''(3) develop recommendations for the Secretary of Health and Human Services regarding whether there is a class of Department of Energy employees, Department of Energy contractor employees, or other employees at any Department of Energy facility who were at least as likely as not exposed to toxic substances at that facility but for whom it is not feasible to estimate with sufficient accuracy the dose they received; and

''(4) review all existing, as of the date of the review, rules and guidelines issued by the Secretary regarding presumption of causation and provide the Secretary with recommendations for new rules and guidelines regarding presumption of causation.'';

(2) in subsection (c)(3), by inserting ''or the Board'' after ''The Secretary'';

(3) by redesignating subsections (h), (i), and (j) as subsections (i), (j), and (k), respectively; and

(4) by inserting after subsection (g) the following:

''(h) REQUIRED RESPONSES TO BOARD RECOMMENDATIONS.—Not later than 90 days after the date on which the Secretary of Labor and the Secretary of Health and Human Services receive recommendations in accordance with paragraph (1), (3), or (4) of subsection (b), each such Secretary shall submit formal responses to each recommendation to the Board and Congress.''.

SEC. 3164. RESEARCH PROGRAM ON EPIDEMIOLOGICAL IMPACTS OF TOXIC EXPOSURES.

(a) DEFINITIONS.—In this section—

(1) the term ''Department of Energy facility'' has the meaning given the term in section 3621 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384l);

(2) the term ''institution of higher education'' has the meaning given such term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001); and

(3) the term ''Secretary'' means the Secretary of Health and Human Services.

(b) ESTABLISHMENT.—The Secretary, acting through the Director of the National Institute of Environmental Health Sciences and in collaboration with the Director of the Centers for Disease Control and Prevention, shall conduct or support research on the epidemiological impacts of exposures to toxic substances at Department of Energy facilities.

(c) USE OF FUNDS.—Research under subsection (b) may include research on the epidemiological, clinical, or health impacts on individuals who were exposed to toxic substances in or near the tank or other storage farms and other relevant Department of Energy facilities through their work at such sites.

(d) ELIGIBILITY AND APPLICATION.—Any institution of higher education or the National Academy of Sciences may apply for funding under this section by submitting to the Secretary an application at such time, in such manner, and containing or accompanied by such information as the Secretary may require.

(e) RESEARCH COORDINATION.—The Secretary shall coordinate activities under this section with similar activities conducted by the Department of Health and Human Services to the extent that other agencies have responsibilities that are related to the study of epidemiological, clinical, or health impacts of exposures to toxic substances.

(f) HEALTH STUDIES REPORT TO SECRETARY.—Not later than 1 year after the end of the funding period for research under this section, the funding recipient shall prepare and submit to the Secretary a final report that—

(1) summarizes the findings of the research;

(2) includes recommendations for any additional studies;

(3) describes any classes of employees that, based on the results of the report, could warrant the establishment of a Special Exposure Cohort under the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384 et seq.) for toxic substances exposures; and

(4) describes any illnesses to be included as covered illnesses under such Act (42 U.S.C. 7384 et seq.).

(g) REPORT TO CONGRESS.—

(1) IN GENERAL.—Not later than 120 days after the date on which the reports under subsection (f) are due, the Secretary shall—

(A) identify a list of cancers and other illnesses associated with toxic substances that pose, or posed, a hazard in the work environment at any Department of Energy facility; and

(B) prepare and submit to the relevant committees of Congress a report—

(i) summarizing the findings from the reports required under subsection (f);

(ii) identifying any new illnesses that, as a result of the study, will be included as covered illnesses, pursuant to subsection (f)(4) and section 3671(2) of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s(2)); and

(iii) including the Secretary's recommendations for additional health studies relating to toxic substances, if the Secretary determines it necessary.

(2) RELEVANT COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term ''relevant committees of Congress'' means—

(A) the Committee on Armed Services, Committee on Appropriations, Committee on

Energy and Natural Resources, and Committee on Health, Education, Labor, and Pensions of the Senate; and

(B) the Committee on Armed Services, Committee on Appropriations, Committee on Energy and Commerce, and Committee on Education and Labor of the House of Representatives.

(h) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $3,000,000 for each of fiscal years 2022 through 2026.

SEC. 3165. NATIONAL ACADEMY OF SCIENCES REVIEW.

Subtitle A of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384d et seq.), as amended by section 3163, is further amended by inserting after section 3614 the following:

''SEC. 3615. NATIONAL ACADEMY OF SCIENCES REVIEW.

''(a) PURPOSE.—The purpose of this section is to enable the National Academy of Sciences, a non-Federal entity with appropriate expertise, to review and evaluate the available scientific evidence regarding associations between diseases and exposure to toxic substances found at Department of Energy cleanup sites.

''(b) DEFINITIONS.—In this section:

''(1) DEPARTMENT OF ENERGY CLEANUP SITE.—The term 'Department of Energy cleanup site' means a Department of Energy facility where cleanup operations are being carried out, or have been carried out, under the environmental management program of the Department of Energy.

''(2) HEALTH STUDIES REPORT.—The term 'health studies report' means the report submitted under section 3164(f) of the Toxic Exposure Safety Act of 2021.

''(c) AGREEMENT.—The Secretary of Health and Human Services shall seek to enter into an agreement with the National Academy of Sciences, not later than 60 days after the issuance of the health studies report, to carry out the requirements of this section.

''(d) REVIEW OF SCIENTIFIC AND MEDICAL EVIDENCE.—

''(1) IN GENERAL.—Under the agreement described in subsection (c), the National Academy of Sciences shall, for the period of the agreement—

''(A) for each area recommended for additional study under the health studies report under section 3164(f)(2) of the Toxic Exposure Safety Act of 2021, review and summarize the scientific evidence relating to the area, including—

''(i) studies by the Department of Energy and Department of Labor; and

''(ii) any other available and relevant scientific studies, to the extent that such studies are relevant to the occupational exposures that have occurred at Department of Energy cleanup sites; and

''(B) review and summarize the scientific and medical evidence concerning the association between exposure to toxic substances found at Department of Energy cleanup sites and resultant diseases.

''(2) SCIENTIFIC DETERMINATIONS CONCERNING DISEASES.—In conducting each review of scientific evidence under subparagraphs (A) and (B) of paragraph (1), the National Academy of Sciences shall—

''(A) assess the strength of such evidence;

''(B) assess whether a statistical association between exposure to a toxic substance and a disease exists, taking into account the strength of the scientific evidence and the appropriateness of the statistical and epidemiological methods used to detect an association;

''(C) assess the increased risk of disease among those exposed to the toxic substance during service during the production and cleanup eras of the Department of Energy cleanup sites;

''(D) survey the impact to health of the toxic substance, focusing on hematologic, renal, urologic, hepatic, gastrointestinal, neurologic, dermatologic, respiratory, endocrine, ocular, ear, nasal, and oropharyngeal diseases, including dementia, leukemia, chemical sensitivities, and chronic obstructive pulmonary disease; and

''(E) determine whether a plausible biological mechanism or other evidence of a causal relationship exists between exposure to the toxic substance and disease.

''(e) ADDITIONAL SCIENTIFIC STUDIES.—If the National Academy of Sciences determines, in the course of conducting the studies under subsection (d), that additional studies are needed to resolve areas of continuing scientific uncertainty relating to toxic exposure at Department of Energy cleanup sites, the National Academy of Sciences shall include, in the next report submitted under subsection (f), recommendations for areas of additional study, consisting of—

''(1) a list of diseases and toxins that require further evaluation and study;

''(2) a review the current information available, as of the date of the report, relating to such diseases and toxins;

''(3) the value of the information that would result from the additional studies; and

''(4) the cost and feasibility of carrying out additional studies.

''(f) REPORTS.—

''(1) IN GENERAL.—By not later than 18 months after the date of the agreement under subsection (c), and every 2 years thereafter, the National Academy of Sciences shall under such agreement prepare and submit a report to—

''(A) the Secretary;

''(B) the Committee on Health, Education, Labor, and Pensions and the Committee on Energy and Natural Resources of the Senate; and

''(C) the Committee on Natural Resources, the Committee on Education and Labor, and the Committee on Energy and Commerce of the House of Representatives.

''(2) CONTENTS.—Each report submitted under paragraph (1) shall include, for the 18-month or 2-year period covered by the report—

''(A) a description of—

''(i) the reviews and studies conducted under this section;

''(ii) the determinations and conclusions of the National Academy of Sciences with respect to such reviews and studies; and

''(iii) the scientific evidence and reasoning that led to such conclusions;

''(B) the recommendations for further areas of study made under subsection (e) for the reporting period;

''(C) a description of any classes of employees that, based on the results of the reviews and studies, could qualify as a Special Exposure Cohort; and

''(D) the identification of any illness that the National Academy of Sciences has determined, as a result of the reviews and studies, should be a covered illness.

''(g) LIMITATION ON AUTHORITY.—The authority to enter into agreements under this section shall be effective for a fiscal year to the extent that appropriations are available.

''(h) SUNSET.—This section shall cease to be effective 10 years after the last day of the fiscal year in which the National Academy of Sciences transmits to the Secretary the first report under subsection (f).''.

SEC. 3166. CONFORMING AMENDMENTS.

The Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384 et seq.) is amended—

(1) in the table of contents—

(A) by redesignating the item relating to section 3614 as the item relating to section 3616;

(B) by inserting after the item relating to section 3613 the following:

''Sec. 3614. Information and outreach.
''Sec. 3615. National Academy of Sciences review.'';

and

(C) by inserting after the item relating to section 3681 the following:

''Sec. 3681A. Completion and updates of site exposure matrices.'';

and

(2) in each of subsections (b)(1) and (c) of section 3612, by striking ''3614(b)'' and inserting ''3616(b)''.

SA 4793. Mr. LEE (for himself and Mr. DAINES) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

In section 511, beginning in subsection (d)(4), strike the period at the end of subparagraph (B)(ii) and all that follows through subsection (g) and insert the following: ''; and

(C) by adding at the end the following new subsection:

''(p) No person may be inducted for training and service under this title if such person—

''(1) has a dependent child and the other parent of the dependent child has been inducted for training or service under this title unless the person volunteers for such induction; or

''(2) has a dependent child who has no other living parent.''.

(5) Section 10(b)(3) (50 U.S.C. 3809(b)(3)) is amended by striking ''the President is requested'' and all that follows through ''race or national origin'' and inserting ''the President is requested to appoint the membership of each local board so that each board has both male and female members and, to the maximum extent practicable, it is proportionately representative of those registrants within its jurisdiction in each applicable basis set forth in section 703(a) of the Civil Rights Act of 1964 (42 U.S.C. 2002e–2(a)), but no action by any board shall be declared invalid on the ground that such board failed to conform to such representation quota''.

(6) Section 16(a) (50 U.S.C. 3814(a)) is amended by striking ''men'' and inserting ''persons''.

(e) MAINTAINING THE HEALTH OF THE SELECTIVE SERVICE SYSTEM.—Section 10(a) (50 U.S.C. 3809(a)) is amended by adding at the end the following new paragraph:

''(5) The Selective Service System shall conduct exercises periodically of all mobilization plans, systems, and processes to evaluate and test the effectiveness of such plans, systems, and processes. Once every 4 years, the exercise shall include the full range of internal and interagency procedures to ensure functionality and interoperability and may take place as part of the Department of Defense mobilization exercise under section 10208 of title 10, United States Code. The Selective Service System shall conduct a public awareness campaign in conjunction

with each exercise to communicate the purpose of the exercise to the public.''.

(f) TECHNICAL AND CONFORMING AMENDMENTS.—The Military Selective Service Act is amended—

(1) in section 4 (50 U.S.C. 3803)—

(A) in subsection (a) in the third undesignated paragraph—

(i) by striking ''his acceptability in all respects, including his'' and inserting ''such person's acceptability in all respects, including such person's''; and

(ii) by striking ''he may prescribe'' and inserting ''the President may prescribe'';

(B) in subsection (c)—

(i) in paragraph (2), by striking ''any enlisted member'' and inserting ''any person who is an enlisted member''; and

(ii) in paragraphs (3), (4), and (5), by striking ''in which he resides'' and inserting ''in which such person resides'';

(C) in subsection (g), by striking ''coordinate with him'' and inserting ''coordinate with the Director''; and

(D) in subsection (k)(1), by striking ''finding by him'' and inserting ''finding by the President'';

(2) in section 5(d) (50 U.S.C. 3805(d)), by striking ''he may prescribe'' and inserting ''the President may prescribe'';

(3) in section 6 (50 U.S.C. 3806)—

(A) in subsection (c)(2)(D), by striking ''he may prescribe'' and inserting ''the President may prescribe'';

(B) in subsection (d)(3), by striking ''he may deem appropriate'' and inserting ''the President considers appropriate''; and

(C) in subsection (h), by striking ''he may prescribe'' each place it appears and inserting ''the President may prescribe'';

(4) in section 10 (50 U.S.C. 3809)—

(A) in subsection (b)—

(i) in paragraph (3)—

(I) by striking ''He shall create'' and inserting ''The President shall create''; and

(II) by striking ''upon his own motion'' and inserting ''upon the President's own motion'';

(ii) in paragraph (4), by striking ''his status'' and inserting ''such individual's status''; and

(iii) in paragraphs (4), (6), (8), and (9), by striking ''he may deem'' each place it appears and inserting ''the President considers''; and

(B) in subsection (c), by striking ''vested in him'' and inserting ''vested in the President'';

(5) in section 13(b) (50 U.S.C. 3812(b)), by striking ''regulation if he'' and inserting ''regulation if the President'';

(6) in section 15 (50 U.S.C. 3813)—

(A) in subsection (b), by striking ''his'' each place it appears and inserting ''the registrant's''; and

(B) in subsection (d), by striking ''he may deem'' and inserting ''the President considers'';

(7) in section 16(g) (50 U.S.C. 3814(g))—

(A) in paragraph (1), by striking ''who as his regular and customary vocation'' and inserting ''who, as such person's regular and customary vocation,''; and

(B) in paragraph (2)—

(i) by striking ''one who as his customary vocation'' and inserting ''a person who, as such person's customary vocation,''; and

(ii) by striking ''he is a member'' and inserting ''such person is a member'';

(8) in section 18(a) (50 U.S.C. 3816(a)), by striking ''he is authorized'' and inserting ''the President is authorized'';

(9) in section 21 (50 U.S.C. 3819)—

(A) by striking ''he is sooner'' and inserting ''sooner'';

(B) by striking ''he'' each subsequent place it appears and inserting ''such member''; and

(C) by striking ''his consent'' and inserting ''such member's consent'';

(10) in section 22(b) (50 U.S.C. 3820(b)), in paragraphs (1) and (2), by striking ''his'' each place it appears and inserting ''the registrant's''; and

(11) except as otherwise provided in this section—

(A) by striking ''he'' each place it appears and inserting ''such person'';

(B) by striking ''his'' each place it appears and inserting ''such person's'';

(C) by striking ''him'' each place it appears and inserting ''such person''; and

(D) by striking ''present himself'' each place it appears in section 12 (50 U.S.C. 3811) and inserting ''appear''.

(g) ENACTMENT OF AUTHORIZATION REQUIRED FOR DRAFT.—

(1) FINDINGS.—Congress makes the following findings:

(A) Clause 12 of section 8 of article I of the Constitution of the United States empowers Congress with the responsibility to ''raise and support Armies''.

(B) The United States first required military conscription in the American Civil War under the Civil War Military Draft Act of 1863.

(C) The Selective Services Act of 1917 authorized the President to draft additional forces beyond the volunteer force to support exceedingly high demand for additional forces when the U.S. entered the first World War.

(D) The Selective Training and Service Act of 1940 was the first authorization by Congress for conscription in peacetime but limited the President's induction authority to ''no greater number of men than the Congress shall hereafter make specific appropriation for from time to time''.

(E) Congress allowed induction authority to lapse in 1947.

(F) Congress reinstated the President's induction authority under the Selective Service Act of 1948 to raise troops for United States participation in the Korean War.

(G) Congress maintained the President's induction authority under the Selective Service Act of 1948 through the beginning of the Vietnam War.

(H) Congress passed additional reforms to the draft under the Military Selective Service Act of 1967 in response to issues arising from United States engagement in the Vietnam War.

(I) Congress prohibited any further use of the draft after July 1, 1973.

(J) If a president seeks to reactivate the use of the draft, Congress would have to enact a law providing authorization for this purpose

(2) AMENDMENT.—Section 17 of the Military Selective Service Act (50 U.S.C. 3815) is amended by adding at the end the following new subsection:

''(d) No person shall be inducted for training and service in the Armed Forces unless Congress first passes and there is enacted a law expressly authorizing such induction into service.''.

(h) EFFECTIVE DATE.—The amendments made by this section shall take effect on the date of the enactment of this Act, except that the amendments made by subsections (d) and (g) shall take effect 1 year after such date of enactment.

SA 4794. Mr. RISCH (for himself, Mr. PORTMAN, Mr. CRUZ, Mr. BARRASSO, Mr. JOHNSON, Mr. COTTON, and Mr. DAINES) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle D of title XII, add the following:

SEC. 1237. IMPOSITION OF SANCTIONS WITH RESPECT TO NORD STREAM 2.

(a) IN GENERAL.—Not later than 15 days after the date of the enactment of this Act, the President shall—

(1) impose sanctions under subsection (b) with respect to any corporate officer of an entity established for or responsible for the planning, construction, or operation of the Nord Stream 2 pipeline or a successor entity; and

(2) impose sanctions under subsection (c) with respect to any entity described in paragraph (1).

(b) INELIGIBILITY FOR VISAS, ADMISSION, OR PAROLE OF IDENTIFIED PERSONS AND CORPORATE OFFICERS.—

(1) IN GENERAL.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (a)(1) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien described in subsection (a)(1) shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

(c) BLOCKING OF PROPERTY OF IDENTIFIED PERSONS.—The President shall exercise all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of an entity described in subsection (a)(1) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(d) EXCEPTIONS.—

(1) EXCEPTION FOR INTELLIGENCE, LAW ENFORCEMENT, AND NATIONAL SECURITY ACTIVITIES.—Sanctions under this section shall not apply to any authorized intelligence, law enforcement, or national security activities of the United States.

(2) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under this section shall not apply with respect to the admission of an alien to the United States if the admission of the alien is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, the Convention on Consular Relations, done at Vienna April 24, 1963, and entered into force March 19, 1967, or other applicable international obligations.

(3) EXCEPTION RELATING TO IMPORTATION OF GOODS.—

(A) IN GENERAL.—Notwithstanding any other provision of this section, the authorities and requirements to impose sanctions under this section shall not include the authority or a requirement to impose sanctions on the importation of goods.

(B) GOOD DEFINED.—In this paragraph, the term ''good'' means any article, natural or man-made substance, material, supply or manufactured product, including inspection and test equipment, and excluding technical data.

(e) CONDITIONS FOR REMOVAL OF SANCTIONS.—Subject to review by Congress under section 216 of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9511), the President may waive the application of sanctions under this section if the President—

(1) determines that the waiver is in the national security interest of the United States; and

(2) submits to the appropriate congressional committees a report on the waiver and the reason for the waiver.

(f) IMPLEMENTATION; PENALTIES.—

(1) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this section.

(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of this section or any regulation, license, or order issued to carry out this section shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(g) SUNSET.—The authority to impose sanctions under this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(h) DEFINITIONS.—In this section:

(1) ADMISSION; ADMITTED; ALIEN.—The terms ''admission'' , ''admitted'' , and ''alien'' have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

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

(A) the Committee on Foreign Relations and the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives.

(3) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity; or

(C) any person within the United States.

SEC. 1238. CONGRESSIONAL REVIEW OF WAIVER UNDER PROTECTING EUROPE'S ENERGY SECURITY ACT OF 2019.

Section 7503(f) of the Protecting Europe's Energy Security Act of 2019 (title LXXV of Public Law 116–92; 22 U.S.C. 9526 note) is amended, in the matter preceding paragraph (1), by striking ''The President'' and inserting ''Subject to review by Congress under section 216 of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9511), the President''.

SEC. 1239. APPLICATION OF CONGRESSIONAL REVIEW UNDER COUNTERING AMERICA'S ADVERSARIES THROUGH SANCTIONS ACT.

Section 216(a)(2) of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9511(a)(2)) is amended—

(1) in subparagraph (A)—

(A) in clause (i), by inserting ''(other than sanctions described in clause (i)(IV) of that subparagraph)'' after ''subparagraph (B)''; and

(B) in clause (ii), by inserting ''or otherwise remove'' after ''waive''; and

(2) in subparagraph (B)(i)—

(A) in subclause (II), by striking ''; or'' and inserting a semicolon;

(B) in subclause (III), by striking ''; and'' and inserting a semicolon; and

(C) by adding at the end the following:

''(IV) section 7503 of the Protecting Europe's Energy Security Act of 2019 (title LXXV of Public Law 116–92; 22 U.S.C. 9526 note); or

''(V) section 1237 of the National Defense Authorization Act for Fiscal Year 2022; and''.

SEC. 1240. INCLUSION OF MATTER RELATING TO NORD STREAM 2 IN REPORT UNDER COUNTERING AMERICA'S ADVERSARIES THROUGH SANCTIONS ACT.

Each report submitted under section 216(a)(1) of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9511(a)(1)) relating to sanctions under section 1237 of this Act or section 7503 of the Protecting Europe's Energy Security Act of 2019 (title LXXV of Public Law 116–92; 22 U.S.C. 9526 note) shall include—

(1) an assessment of the security risks posed by Nord Stream 2, including—

(A) the presence along Nord Stream 2 or Nord Stream 1 infrastructure or pipeline corridors of undersea surveillance systems and sensors, fiber optic terminals, or other systems that are capable of conducting military or intelligence activities unrelated to civilian energy transmission, including those designed to enhance Russian Federation antisubmarine warfare, surveillance, espionage, or sabotage capabilities;

(B) the use of Nord Stream-affiliated infrastructure, equipment, personnel, vessels, financing, or other assets—

(i) to facilitate, carry out, or conceal Russian Federation maritime surveillance, espionage, or sabotage activities;

(ii) to justify the presence of Russian Federation naval vessels or military personnel or equipment in international waters or near North Atlantic Treaty Organization or partner countries;

(iii) to disrupt freedom of navigation; or

(iv) to pressure or intimidate countries in the Baltic Sea;

(C) the involvement in the Nord Stream 2 pipeline or its affiliated entities of current or former Russian, Soviet, or Warsaw Pact intelligence and military personnel and any business dealings between Nord Stream 2 and entities affiliated with the intelligence or defense sector of the Russian Federation; and

(D) malign influence activities of the Government of the Russian Federation, including strategic corruption and efforts to influence European decision-makers, supported or financed through the Nord Stream 2 pipeline;

(2) an assessment of whether the Russian Federation maintains gas transit through Ukraine at levels consistent with the volumes set forth in the Ukraine-Russian Federation gas transit agreement of December 2019 and continues to pay the transit fees specified in that agreement;

(3) an assessment of the status of negotiations between the Russian Federation and Ukraine to secure an agreement to extend gas transit through Ukraine beyond the expiration of the agreement described in paragraph (2); and

(4) an assessment of whether the United States and Germany have agreed on a common definition for energy ''weaponization'' and the associated triggers for sanctions and other enforcement actions, pursuant to the Joint Statement of the United States and Germany on support for Ukraine, European energy security, and our climate goals, dated July 21, 2021; and

(5) a description of the consultations with United States allies and partners in Europe, including Ukraine, Poland, and the countries in Central and Eastern Europe most impacted by the Nord Stream 2 pipeline concerning the matters agreed to as described in paragraph (4).

SA 4795. Mr. SHELBY (for himself, Mr. INHOFE, Mr. WICKER, Mr. BLUNT, Mrs. CAPITO, Mrs. HYDE-SMITH, Mr. COTTON, Mr. BOOZMAN, Ms. COLLINS, Mr. KENNEDY, Ms. MURKOWSKI, Mr. CRAMER, Mr. TILLIS, and Mr. HOEVEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—AUTHORIZATION OF AMOUNTS FOR DEPARTMENT OF DEFENSE INFRASTRUCTURE

SEC. ____1. ESTABLISHMENT OF DEFENSE INFRASTRUCTURE FUND.

There is established in the general fund of the Treasury an account to be known as the ''Defense Infrastructure Fund'' for the deposit of amounts to be used for improvement of the infrastructure of the Department of Defense.

SEC. ____2. AUTHORIZATION OF AMOUNTS FOR REDUCTION OF BACKLOG FOR FACILITY INFRASTRUCTURE PROJECTS.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $4,000,000,000 for the Defense Infrastructure Fund, of which $1,300,000,000 shall be available for each of the Departments of the Army, the Navy, and the Air Force, and $100,000,000 shall be for the Defense Health Agency, to reduce the backlog of facility infrastructure maintenance projects of the Department of Defense.

(b) COMPLIANCE WITH REPAIR REQUIREMENTS.—Any project carried out with amounts authorized under subsection (a) shall comply with the requirements under section 2811 of title 10, United States Code.

(c) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2026.

SEC. ____3. AUTHORIZATION OF AMOUNTS FOR MODERNIZATION OF TEST AND TRAINING RANGES OF DEPARTMENT OF DEFENSE.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $2,800,000,000 for the Defense Infrastructure Fund to modernize the test and training ranges of the Department of Defense, including projects included in the report required under section 2806 of the Military Construction Authorization Act for Fiscal Year 2018

(Division B of Public Law 115–91; 10 U.S.C. 222a note) for test and evaluation activities.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2032.

SEC. _____4. AUTHORIZATION OF AMOUNTS FOR REMEDIATION OF PERFLUORALKYL SUBSTANCES AND POLYFLUOROALKYL SUBSTANCES.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $700,000,000 for the Defense Infrastructure Fund to remediate perfluoralkyl substances and polyfluoroalkyl substances at installations owned by the Department of Defense.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2026.

SEC. _____5. AUTHORIZATION OF AMOUNTS FOR DEPOT MODERNIZATION.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $4,325,000,000 for the Defense Infrastructure Fund for depot modernization.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2032.

SEC. _____6. AUTHORIZATION OF AMOUNTS FOR AMMUNITION PLANT MODERNIZATION.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $2,350,000,000 for the Defense Infrastructure Fund to modernize ammunition plants.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2026.

SEC. _____7. AUTHORIZATION OF AMOUNTS FOR FIFTH-GENERATION WIRELESS NETWORKING TECHNOLOGIES.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $2,500,000,000 for the Defense Infrastructure Fund to provide fifth-generation wireless networking technologies to installations owned by the Department of Defense.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2026.

SEC. _____8. AUTHORIZATION OF AMOUNTS FOR NAVY SHIPYARD AND INFRASTRUCTURE IMPROVEMENT.

(a) AUTHORIZATION.—

(1) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $10,325,000,000 for the Defense Infrastructure Fund to improve, in accordance with subsection (b), the Navy shipyard infrastructure of the United States.

(2) AVAILABILITY OF AMOUNTS.—Amounts authorized under paragraph (1) shall be available until expended.

(3) SUPPLEMENT NOT SUPPLANT.—Amounts authorized under paragraph (1) shall supplement and not supplant other amounts appropriated or otherwise made available for the purpose described in paragraph (1).

(b) USE OF FUNDS.—

(1) IN GENERAL.—As soon as practicable after the date of the enactment of this Act, the Secretary of Defense shall make amounts appropriated pursuant to the authorization under subsection (a)(1) directly available to the Secretary of the Navy for obligation and expenditure for Navy public shipyard facilities, dock, dry dock, capital equipment improvements, and dredging efforts needed by such shipyards.

(2) PROJECTS IN ADDITION TO OTHER CONSTRUCTION PROJECTS.—Construction projects undertaken using amounts appropriated pursuant to the authorization under subsection (a)(1) shall be in addition to and separate from any military construction program authorized by any Act to authorize appropriations for a fiscal year for military activities of the Department of Defense and for military construction.

(c) NAVY PUBLIC SHIPYARD DEFINED.—In this section, the term ''Navy public shipyard'' means the following:

(1) The Norfolk Naval Shipyard, Virginia.

(2) The Pearl Harbor Naval Shipyard, Hawaii.

(3) The Portsmouth Naval Shipyard, Maine.

(4) The Puget Sound Naval Shipyard, Washington.

SA 4796. Mr. PAUL submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle C of title VII, add the following:

SEC. 744. PROHIBITION ON DISHONORABLE DISCHARGE OF MEMBERS OF THE ARMED FORCES FOR REFUSING TO COMPLY WITH COVID–19 VACCINE MANDATE.

The Secretary of Defense may not give a dishonorable discharge to a member of the Armed Forces solely on the basis of the refusal of the member, for religious, medical, or personal reasons, to comply with any requirement that the member receive a vaccination for coronavirus disease 2019 (commonly known as ''COVID–19'').

SA 4797. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle D of title XXVIII, add the following:

SEC. 2836. PAYMENT TO ENVIRONMENTAL PROTECTION AGENCY FOR CERTAIN COSTS IN CONNECTION WITH FORMER ROCKY MOUNTAIN ARSENAL, COLORADO.

(a) AUTHORITY FOR PAYMENT.—

(1) TRANSFER AMOUNT.—

(A) IN GENERAL.—Notwithstanding section 2215 of title 10, United States Code, chapter 160 of such title, section 1367 of the National Defense Authorization Act for Fiscal Year 1987 (Public Law 99–661; 100 Stat. 4003), or any other provision of law, using funds described in subsection (b), the Secretary of Defense may transfer to the Administrator of the Environmental Protection Agency for use at the former Rocky Mountain Arsenal, Colorado—

(i) in fiscal year 2022, $4,805,000 for costs associated with the involvement of the Environmental Protection Agency with the cleanup by the Department of the Army of the former Rocky Mountain Arsenal from fiscal years 2015 through 2020, after a specific accounting is provided in accordance with subparagraph (B); and

(ii) in each of fiscal years 2022, 2023, and 2024, to account for costs incurred by the Environmental Protection Agency for such cleanup in fiscal years 2021, 2022, and 2023, an amount not to exceed $600,000, after a specific accounting is provided in accordance with subparagraph (B).

(B) ACCOUNTING.—Prior to the payment of amounts under subparagraph (A), the Administrator of the Environmental Protection Agency shall furnish to the Secretary of Defense a specific accounting of costs for which payment is requested.

(C) AUTHORIZED COSTS.—Payment of amounts under subparagraph (A) may be made only for those costs incurred by the Environmental Protection Agency for fiscal years 2015 through 2023—

(i) for providing technical assistance in accordance with the document entitled ''Settlement Agreement Between the United States and Shell Oil Company Concerning the Rocky Mountain Arsenal'', effective February 17, 1989, as incorporated into the consent decree entered by the United States District Court for the District of Colorado in United States v. Shell Oil Co., Civil Action No. 83-C-2379, dated February 12, 1992 (referred to in this section as the ''Settlement Agreement''); and

(ii) that are not inconsistent with the National Oil and Hazardous Substances Pollution Contingency Plan described in part 300 of title 40, Code of Federal Regulations (or successor regulations).

(2) PURPOSE OF PAYMENT.—The amounts authorized to be transferred under paragraph (1)(A) are—

(A) for payment to the Environmental Protection Agency for all costs that may be owed by the Department of the Army to the Environmental Protection Agency pursuant to the Settlement Agreement; and

(B) for use at the former Rocky Mountain Arsenal to allow the Environmental Protection Agency to proceed with review of cleanup documents that the Agency had suspended.

(b) SOURCE OF FUNDS.—The transfer authorized under subsection (a)(1)(A) shall be made using funds authorized to be appropriated for fiscal years 2022, 2023, and 2024 for Operation and Maintenance, Army for Environmental Restoration.

(c) FINALITY OF PAYMENTS.—The transfer authorized under subsection (a)(1)(A) constitutes final and complete payment for all costs borne by the Environmental Protection Agency arising from the Settlement Agreement for fiscal years 2015 through 2023.

SA 4798. Mr. CASSIDY (for himself, Mr. WHITEHOUSE, and Ms. WARREN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. _____. POSTSECONDARY STUDENT DATA SYSTEM.

(a) SHORT TITLE.—This section may be cited as the ''College Transparency Act''.

(b) POSTSECONDARY STUDENT DATA SYSTEM.—Section 132 of the Higher Education Act of 1965 (20 U.S.C. 1015a) is amended—

(1) by redesignating subsection (l) as subsection (m); and

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

''(l) POSTSECONDARY STUDENT DATA SYSTEM.—

''(1) IN GENERAL.—

''(A) ESTABLISHMENT OF SYSTEM.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner of the National Center for Education Statistics (referred to in this subsection as the 'Commissioner') shall develop and maintain a secure, privacy-protected postsecondary student-level data system in order to—

''(i) accurately evaluate student enrollment patterns, progression, completion, and postcollegiate outcomes, and higher education costs and financial aid;

''(ii) assist with transparency, institutional improvement, and analysis of Federal aid programs;

''(iii) provide accurate, complete, and customizable information for students and families making decisions about postsecondary education; and

''(iv) reduce the reporting burden on institutions of higher education, in accordance with section 5(b) of the College Transparency Act.

''(B) AVOIDING DUPLICATED REPORTING.—Notwithstanding any other provision of this section, to the extent that another provision of this section requires the same reporting or collection of data that is required under this subsection, an institution of higher education, or the Secretary or Commissioner, may use the reporting or data required for the postsecondary student data system under this subsection to satisfy both requirements.

''(C) DEVELOPMENT PROCESS.—In developing the postsecondary student data system described in this subsection, the Commissioner shall—

''(i) focus on the needs of—

''(I) users of the data system; and

''(II) entities, including institutions of higher education, reporting to the data system;

''(ii) take into consideration, to the extent practicable—

''(I) the guidelines outlined in the U.S. Web Design Standards maintained by the General Services Administration and the Digital Services Playbook and TechFAR Handbook for Procuring Digital Services Using Agile Processes of the U.S. Digital Service; and

''(II) the relevant successor documents or recommendations of such guidelines;

''(iii) use modern, relevant privacy- and security-enhancing technology, and enhance and update the data system as necessary to carry out the purpose of this subsection;

''(iv) ensure data privacy and security is consistent with any Federal law relating to privacy or data security, including—

''(I) the requirements of subchapter II of chapter 35 of title 44, United States Code, specifying security categorization under the Federal Information Processing Standards or any relevant successor of such standards;

''(II) security requirements that are consistent with the Federal agency responsibilities in section 3554 of title 44, United States Code, or any relevant successor of such responsibilities; and

''(III) security requirements, guidelines, and controls consistent with cybersecurity standards and best practices developed by the National Institute of Standards and Technology, including frameworks, consistent with section 2(c) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)), or any relevant successor of such frameworks;

''(v) follow Federal data minimization practices to ensure only the minimum amount of data is collected to meet the system's goals, in accordance with Federal data minimization standards and guidelines developed by the National Institute of Standards and Technology; and

''(vi) provide notice to students outlining the data included in the system and how the data are used.

''(2) DATA ELEMENTS.—

''(A) IN GENERAL.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner, in consultation with the Postsecondary Student Data System Advisory Committee established under subparagraph (B), shall determine—

''(i) the data elements to be included in the postsecondary student data system, in accordance with subparagraphs (C) and (D); and

''(ii) how to include the data elements required under subparagraph (C), and any additional data elements selected under subparagraph (D), in the postsecondary student data system.

''(B) POSTSECONDARY STUDENT DATA SYSTEM ADVISORY COMMITTEE.—

''(i) ESTABLISHMENT.—Not later than 2 years after the date of enactment of the College Transparency Act, the Commissioner shall establish a Postsecondary Student Data System Advisory Committee (referred to in this subsection as the 'Advisory Committee'), whose members shall include—

''(I) the Chief Privacy Officer of the Department or an official of the Department delegated the duties of overseeing data privacy at the Department;

''(II) the Chief Security Officer of the Department or an official of the Department delegated the duties of overseeing data security at the Department;

''(III) representatives of diverse institutions of higher education, which shall include equal representation between 2-year and 4-year institutions of higher education, and from public, nonprofit, and proprietary institutions of higher education, including minority-serving institutions;

''(IV) representatives from State higher education agencies, entities, bodies, or boards;

''(V) representatives of postsecondary students;

''(VI) representatives from relevant Federal agencies; and

''(VII) other stakeholders (including individuals with expertise in data privacy and security, consumer protection, and postsecondary education research).

''(ii) REQUIREMENTS.—The Commissioner shall ensure that the Advisory Committee—

''(I) adheres to all requirements under the Federal Advisory Committee Act (5 U.S.C. App.);

''(II) establishes operating and meeting procedures and guidelines necessary to execute its advisory duties; and

''(III) is provided with appropriate staffing and resources to execute its advisory duties.

''(C) REQUIRED DATA ELEMENTS.—The data elements in the postsecondary student data system shall include, at a minimum, the following:

''(i) Student-level data elements necessary to calculate the information within the surveys designated by the Commissioner as 'student-related surveys' in the Integrated Postsecondary Education Data System (IPEDS), as such surveys are in effect on the day before the date of enactment of the College Transparency Act, except that in the case that collection of such elements would conflict with subparagraph (F), such elements in conflict with subparagraph (F) shall be included in the aggregate instead of at the student level.

''(ii) Student-level data elements necessary to allow for reporting student enrollment, persistence, retention, transfer, and completion measures for all credential levels separately (including certificate, associate, baccalaureate, and advanced degree levels), within and across institutions of higher education (including across all categories of institution level, control, and predominant degree awarded). The data elements shall allow for reporting about all such data disaggregated by the following categories:

''(I) Enrollment status as a first-time student, recent transfer student, or other non-first-time student.

''(II) Attendance intensity, whether full-time or part-time.

''(III) Credential-seeking status, by credential level.

''(IV) Race or ethnicity, in a manner that captures all the racial groups specified in the most recent American Community Survey of the Bureau of the Census.

''(V) Age intervals.

''(VI) Gender.

''(VII) Program of study (as applicable).

''(VIII) Military or veteran benefit status (as determined based on receipt of veteran's education benefits, as defined in section 480(c)).

''(IX) Status as a distance education student, whether exclusively or partially enrolled in distance education.

''(X) Federal Pell Grant recipient status under section 401 and Federal loan recipient status under title IV, provided that the collection of such information complies with paragraph (1)(B).

''(D) OTHER DATA ELEMENTS.—

''(i) IN GENERAL.—The Commissioner may, after consultation with the Advisory Committee and provision of a public comment period, include additional data elements in the postsecondary student data system, such as those described in clause (ii), if those data elements—

''(I) are necessary to ensure that the postsecondary data system fulfills the purposes described in paragraph (1)(A); and

''(II) are consistent with data minimization principles, including the collection of only those additional elements that are necessary to ensure such purposes.

''(ii) DATA ELEMENTS.—The data elements described in clause (i) may include—

''(I) status as a first generation college student, as defined in section 402A(h);

''(II) economic status;

''(III) participation in postsecondary remedial coursework or gateway course completion; or

''(IV) other data elements that are necessary in accordance with clause (i).

''(E) REEVALUATION.—Not less than once every 3 years after the implementation of the postsecondary student data system described in this subsection, the Commissioner, in consultation with the Advisory Committee described in subparagraph (B), shall review the data elements included in the postsecondary student data system and may revise the data elements to be included in such system.

''(F) PROHIBITIONS.—The Commissioner shall not include individual health data (including data relating to physical health or mental health), student discipline records or data, elementary and secondary education data, an exact address, citizenship status, migrant status, or national origin status for students or their families, course grades, postsecondary entrance examination results, political affiliation, or religion in the postsecondary student data system under this subsection.

''(3) PERIODIC MATCHING WITH OTHER FEDERAL DATA SYSTEMS.—

''(A) DATA SHARING AGREEMENTS.—

''(i) The Commissioner shall ensure secure, periodic data matches by entering into data

sharing agreements with each of the following Federal agencies and offices:

''(I) The Secretary of the Treasury and the Commissioner of the Internal Revenue Service, in order to calculate aggregate program- and institution-level earnings of postsecondary students.

''(II) The Secretary of Defense, in order to assess the use of postsecondary educational benefits and the outcomes of servicemembers.

''(III) The Secretary of Veterans Affairs, in order to assess the use of postsecondary educational benefits and outcomes of veterans.

''(IV) The Director of the Bureau of the Census, in order to assess the earnings outcomes of former postsecondary education students.

''(V) The Chief Operating Officer of the Office of Federal Student Aid, in order to analyze the use of postsecondary educational benefits provided under this Act.

''(VI) The Commissioner of the Social Security Administration, in order to evaluate labor market outcomes of former postsecondary education students.

''(VII) The Commissioner of the Bureau of Labor Statistics, in order to assess the wages of former postsecondary education students.

''(ii) The heads of Federal agencies and offices described under clause (i) shall enter into data sharing agreements with the Commissioner to ensure secure, periodic data matches as described in this paragraph.

''(B) CATEGORIES OF DATA.—The Commissioner shall, at a minimum, seek to ensure that the secure periodic data system matches described in subparagraph (A) permit consistent reporting of the following categories of data for all postsecondary students:

''(i) Enrollment, retention, transfer, and completion outcomes for all postsecondary students.

''(ii) Financial indicators for postsecondary students receiving Federal grants and loans, including grant and loan aid by source, cumulative student debt, loan repayment status, and repayment plan.

''(iii) Post-completion outcomes for all postsecondary students, including earnings, employment, and further education, by program of study and credential level and as measured—

''(I) immediately after leaving postsecondary education; and

''(II) at time intervals appropriate to the credential sought and earned.

''(C) PERIODIC DATA MATCH STREAMLINING AND CONFIDENTIALITY.—

''(i) STREAMLINING.—In carrying out the secure periodic data system matches under this paragraph, the Commissioner shall—

''(I) ensure that such matches are not continuous, but occur only periodically at appropriate intervals, as determined by the Commissioner to meet the goals of subparagraph (A); and

''(II) seek to—

''(aa) streamline the data collection and reporting requirements for institutions of higher education;

''(bb) minimize duplicative reporting across or within Federal agencies or departments, including reporting requirements applicable to institutions of higher education under the Workforce Innovation and Opportunity Act (29 U.S.C. 3101 et seq.) and the Carl D. Perkins Career and Technical Education Act of 2006;

''(cc) protect student privacy; and

''(dd) streamline the application process for student loan benefit programs available to borrowers based on data available from different Federal data systems.

''(ii) REVIEW.—Not less often than once every 3 years after the establishment of the postsecondary student data system under this subsection, the Commissioner, in consultation with the Advisory Committee, shall review methods for streamlining data collection from institutions of higher education and minimizing duplicative reporting within the Department and across Federal agencies that provide data for the postsecondary student data system.

''(iii) CONFIDENTIALITY.—The Commissioner shall ensure that any periodic matching or sharing of data through periodic data system matches established in accordance with this paragraph—

''(I) complies with the security and privacy protections described in paragraph (1)(C)(iv) and other Federal data protection protocols;

''(II) follows industry best practices commensurate with the sensitivity of specific data elements or metrics;

''(III) does not result in the creation of a single standing, linked Federal database at the Department that maintains the information reported across other Federal agencies; and

''(IV) discloses to postsecondary students what data are included in the data system and periodically matched and how the data are used.

''(iv) CORRECTION.—The Commissioner, in consultation with the Advisory Committee, shall establish a process for students to request access to only their personal information for inspection and request corrections to inaccuracies in a manner that protects the student's personally identifiable information. The Commissioner shall respond in writing to every request for a correction from a student.

''(4) PUBLICLY AVAILABLE INFORMATION.—

''(A) IN GENERAL.—The Commissioner shall make the summary aggregate information described in subparagraph (C), at a minimum, publicly available through a user-friendly consumer information website and analytic tool that—

''(i) provides appropriate mechanisms for users to customize and filter information by institutional and student characteristics;

''(ii) allows users to build summary aggregate reports of information, including reports that allow comparisons across multiple institutions and programs, subject to subparagraph (B);

''(iii) uses appropriate statistical disclosure limitation techniques necessary to ensure that the data released to the public cannot be used to identify specific individuals; and

''(iv) provides users with appropriate contextual factors to make comparisons, which may include national median figures of the summary aggregate information described in subparagraph (C).

''(B) NO PERSONALLY IDENTIFIABLE INFORMATION AVAILABLE.—The summary aggregate information described in this paragraph shall not include personally identifiable information.

''(C) SUMMARY AGGREGATE INFORMATION AVAILABLE.—The summary aggregate information described in this paragraph shall, at a minimum, include each of the following for each institution of higher education:

''(i) Measures of student access, including—

''(I) admissions selectivity and yield; and

''(II) enrollment, disaggregated by each category described in paragraph (2)(C)(ii).

''(ii) Measures of student progression, including retention rates and persistence rates, disaggregated by each category described in paragraph (2)(C)(ii).

''(iii) Measures of student completion, including—

''(I) transfer rates and completion rates, disaggregated by each category described in paragraph (2)(C)(ii); and

''(II) number of completions, disaggregated by each category described in paragraph (2)(C)(ii).

''(iv) Measures of student costs, including—

''(I) tuition, required fees, total cost of attendance, and net price after total grant aid, disaggregated by in-State tuition or in-district tuition status (if applicable), program of study (if applicable), and credential level; and

''(II) typical grant amounts and loan amounts received by students reported separately from Federal, State, local, and institutional sources, and cumulative debt, disaggregated by each category described in paragraph (2)(C)(ii) and completion status.

''(v) Measures of postcollegiate student outcomes, including employment rates, mean and median earnings, loan repayment and default rates, and further education rates. These measures shall—

''(I) be disaggregated by each category described in paragraph (2)(C)(ii) and completion status; and

''(II) be measured immediately after leaving postsecondary education and at time intervals appropriate to the credential sought or earned.

''(D) DEVELOPMENT CRITERIA.—In developing the method and format of making the information described in this paragraph publicly available, the Commissioner shall—

''(i) focus on the needs of the users of the information, which will include students, families of students, potential students, researchers, and other consumers of education data;

''(ii) take into consideration, to the extent practicable, the guidelines described in paragraph (1)(C)(ii)(I), and relevant successor documents or recommendations of such guidelines;

''(iii) use modern, relevant technology and enhance and update the postsecondary student data system with information, as necessary to carry out the purpose of this paragraph;

''(iv) ensure data privacy and security in accordance with standards and guidelines developed by the National Institute of Standards and Technology, and in accordance with any other Federal law relating to privacy or security, including complying with the requirements of subchapter II of chapter 35 of title 44, United States Code, specifying security categorization under the Federal Information Processing Standards, and security requirements, and setting of National Institute of Standards and Technology security baseline controls at the appropriate level; and

''(v) conduct consumer testing to determine how to make the information as meaningful to users as possible.

''(5) PERMISSIBLE DISCLOSURES OF DATA.—

''(A) DATA REPORTS AND QUERIES.—

''(i) IN GENERAL.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner shall develop and implement a secure process for making student-level, non-personally identifiable information, with direct identifiers removed, from the postsecondary student data system available for vetted research and evaluation purposes approved by the Commissioner in a manner compatible with practices for disclosing National Center for Education Statistics restricted-use survey data as in effect on the day before the date of enactment of the College Transparency Act, or by applying other research and disclosure restrictions to ensure data privacy and security. Such process shall be approved by the National Center for Education Statistics' Disclosure Review Board (or successor body).

''(ii) PROVIDING DATA REPORTS AND QUERIES TO INSTITUTIONS AND STATES.—

''(I) IN GENERAL.—The Commissioner shall provide feedback reports, at least annually, to each institution of higher education, each postsecondary education system that fully participates in the postsecondary student data system, and each State higher education body as designated by the governor.

''(II) FEEDBACK REPORTS.—The feedback reports provided under this clause shall include program-level and institution-level information from the postsecondary student data system regarding students who are associated with the institution or, for State representatives, the institutions within that State, on or before the date of the report, on measures including student mobility and workforce outcomes, provided that the feedback aggregate summary reports protect the privacy of individuals.

''(III) DETERMINATION OF CONTENT.—The content of the feedback reports shall be determined by the Commissioner in consultation with the Advisory Committee.

''(iii) PERMITTING STATE DATA QUERIES.—The Commissioner shall, in consultation with the Advisory Committee and as soon as practicable, create a process through which States may submit lists of secondary school graduates within the State to receive summary aggregate outcomes for those students who enrolled at an institution of higher education, including postsecondary enrollment and college completion, provided that those data protect the privacy of individuals and that the State data submitted to the Commissioner are not stored in the postsecondary education system.

''(iv) REGULATIONS.—The Commissioner shall promulgate regulations to ensure fair, secure, and equitable access to data reports and queries under this paragraph.

''(B) DISCLOSURE LIMITATIONS.—In carrying out the public reporting and disclosure requirements of this subsection, the Commissioner shall use appropriate statistical disclosure limitation techniques necessary to ensure that the data released to the public cannot include personally identifiable information or be used to identify specific individuals.

''(C) SALE OF DATA PROHIBITED.—Data collected under this subsection, including the public-use data set and data comprising the summary aggregate information available under paragraph (4), shall not be sold to any third party by the Commissioner, including any institution of higher education or any other entity.

''(D) LIMITATION ON USE BY OTHER FEDERAL AGENCIES.—

''(i) IN GENERAL.—The Commissioner shall not allow any other Federal agency to use data collected under this subsection for any purpose except—

''(I) for vetted research and evaluation conducted by the other Federal agency, as described in subparagraph (A)(i); or

''(II) for a purpose explicitly authorized by this Act.

''(ii) PROHIBITION ON LIMITATION OF SERVICES.—The Secretary, or the head of any other Federal agency, shall not use data collected under this subsection to limit services to students.

''(E) LAW ENFORCEMENT.—Personally identifiable information collected under this subsection shall not be used for any Federal, State, or local law enforcement activity or any other activity that would result in adverse action against any student or a student's family, including debt collection activity or enforcement of immigration laws.

''(F) LIMITATION OF USE FOR FEDERAL RANKINGS OR SUMMATIVE RATING SYSTEM.—The comprehensive data collection and analysis necessary for the postsecondary student data system under this subsection shall not be used by the Secretary or any Federal entity to establish any Federal ranking system of institutions of higher education or a system that results in a summative Federal rating of institutions of higher education.

''(G) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to prevent the use of individual categories of aggregate information to be used for accountability purposes.

''(H) RULE OF CONSTRUCTION REGARDING COMMERCIAL USE OF DATA.—Nothing in this paragraph shall be construed to prohibit third-party entities from using publicly available information in this data system for commercial use.

''(6) SUBMISSION OF DATA.—

''(A) REQUIRED SUBMISSION.—Each institution of higher education participating in a program under title IV, or the assigned agent of such institution, shall, for each eligible program, in accordance with section 487(a)(17), collect, and submit to the Commissioner, the data requested by the Commissioner to carry out this subsection.

''(B) VOLUNTARY SUBMISSION.—Any institution of higher education not participating in a program under title IV may voluntarily participate in the postsecondary student data system under this subsection by collecting and submitting data to the Commissioner, as the Commissioner may request to carry out this subsection.

''(C) PERSONALLY IDENTIFIABLE INFORMATION.—In accordance with paragraph (2)(C)(i), if the submission of an element of student-level data is prohibited under paragraph (2)(F) (or otherwise prohibited by law), the institution of higher education shall submit that data to the Commissioner in the aggregate.

''(7) UNLAWFUL WILLFUL DISCLOSURE.—

''(A) IN GENERAL.—It shall be unlawful for any person who obtains or has access to personally identifiable information in connection with the postsecondary student data system described in this subsection to willfully disclose to any person (except as authorized in this Act or by any Federal law) such personally identifiable information.

''(B) PENALTY.—Any person who violates subparagraph (A) shall be subject to a penalty described under section 3572(f) of title 44, United States Code, and section 183(d)(6) of the Education Sciences Reform Act of 2002 (20 U.S.C. 9573(d)(6)).

''(C) EMPLOYEE OR OFFICER OF THE UNITED STATES.—If a violation of subparagraph (A) is committed by any officer or employee of the United States, the officer or employee shall be dismissed from office or discharged from employment upon conviction for the violation.

''(8) DATA SECURITY.—The Commissioner shall produce and update as needed guidance and regulations relating to privacy, security, and access which shall govern the use and disclosure of data collected in connection with the activities authorized in this subsection. The guidance and regulations developed and reviewed shall protect data from unauthorized access, use, and disclosure, and shall include—

''(A) an audit capability, including mandatory and regularly conducted audits;

''(B) access controls;

''(C) requirements to ensure sufficient data security, quality, validity, and reliability;

''(D) confidentiality protection in accordance with the applicable provisions of subchapter III of chapter 35 of title 44, United States Code;

''(E) appropriate and applicable privacy and security protection, including data retention and destruction protocols and data minimization, in accordance with the most recent Federal standards developed by the National Institute of Standards and Technology; and

''(F) protocols for managing a breach, including breach notifications, in accordance with the standards of National Center for Education Statistics.

''(9) DATA COLLECTION.—The Commissioner shall ensure that data collection, maintenance, and use under this subsection complies with section 552a of title 5, United States Code.

''(10) DEFINITIONS.—In this subsection:

''(A) INSTITUTION OF HIGHER EDUCATION.—The term 'institution of higher education' has the meaning given the term in section 102.

''(B) MINORITY-SERVING INSTITUTION.—The term 'minority-serving institution' means an institution of higher education listed in section 371(a).

''(C) PERSONALLY IDENTIFIABLE INFORMATION.—The term 'personally identifiable information' means personally identifiable information within the meaning of section 444 of the General Education Provisions Act.''.

(c) REPEAL OF PROHIBITION ON STUDENT DATA SYSTEM.—Section 134 of the Higher Education Act of 1965 (20 U.S.C. 1015c) is repealed.

(d) INSTITUTIONAL REQUIREMENTS.—

(1) IN GENERAL.—Paragraph (17) of section 487(a) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)) is amended to read as follows:

''(17) The institution or the assigned agent of the institution will collect and submit data to the Commissioner for Education Statistics in accordance with section 132(l), the nonstudent related surveys within the Integrated Postsecondary Education Data System (IPEDS), or any other Federal institution of higher education data collection effort (as designated by the Secretary), in a timely manner and to the satisfaction of the Secretary.''.

(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect on the date that is 4 years after the date of enactment of this Act.

(e) TRANSITION PROVISIONS.—The Secretary of Education and the Commissioner for Education Statistics shall take such steps as are necessary to ensure that the development and maintenance of the postsecondary student data system required under section 132(l) of the Higher Education Act of 1965, as added by subsection (b) of this section, occurs in a manner that reduces the reporting burden for entities that reported into the Integrated Postsecondary Education Data System (IPEDS).

SA 4799. Mr. PETERS (for himself, Mr. PORTMAN, Mr. WARNER, Ms. COLLINS, Mr. KING, Mr. RUBIO, Mr. RISCH, Ms. ROSEN, Mr. CORNYN, and Mr. BURR) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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, privacy, disclosure, and sharing of information;'';

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

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

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

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

''(1) develop, and in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies; and'';

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

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

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

(D) by adding at the end the following:

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

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

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

(2) in section 3553—

(A) 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 consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director,'' before ''overseeing'';

(ii) in paragraph (5), 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 cyber threat intelligence;

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

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

''(10) any other information the Director of the Cybersecurity and Infrastructure Security Agency determines relevant.''; 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 consultation 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 majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

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

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

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

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

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

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

''(B) may include a classified annex.

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

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

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

(b) 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''.

(c) 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''.

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

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

(2) in subsection (b)(1)(A), by striking ''the Secretary of Homeland Security'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(3) by 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 cyber 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 in consultation with the National Cyber Director, shall issue guidance to agencies on sharing relevant information in a consistent, automated, and machine readable manner with the 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 cyber threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and

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

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) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 6203 of this division.

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 or subcontract at any tier, grant, cooperative agreement, or other transaction agreement, unless that entity 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 section 2232(a) and 2233 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 briefings required under subsection (c);

''(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 National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—

''(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, the Department of Justice, and 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 is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

''(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 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 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 that is a Federal contractor 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.

''(5) AUTHENTICATION.—

''(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

''(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

''(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

''(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate Federal regulatory agency 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 Federal regulatory agency 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); or

''(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

''(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b); or

''(2) issued a subpoena pursuant to subsection (c).

''(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

''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 or 2233 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 cyber incident reported pursuant to section 2232 or 2233 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 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, including any independent establishment (as defined in section 104 of title 5, United States Code), 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. The Director shall share and coordinate each report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 6103 of this title.

(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, the Attorney General, 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 Attorney General, 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, the Attorney General, 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 paragraph (11), by striking ''and'' at the end;

(2) in the first paragraph (12)—

(A) by striking ''section 2215'' and inserting ''section 2217''; and

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

(3) 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 use or threat of use of unauthorized or malicious code on an information system, or the use or 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 CONTROL.—The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

''(25) 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.

''(26) SHARING.—The term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

''(27) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber incident within the supply chain of an information system that an adversary can leverage to jeopardize 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.

''(28) 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.

''(29) 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)—

(i) in subparagraph (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))''; and

(ii) in subparagraph (B)(ii), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(D) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)''; and

(ii) in paragraph (1)(E)(ii)(II), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(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) in subsection (d)(2), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(B) 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.'';

(11) in section 2218(c)(4)(A), as so redesignated, by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; 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 item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''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 paragraphs (16) and (17) and inserting the following:

''(16) SECURITY CONTROL.—The term 'security control' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(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(b) (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 (6 U.S.C. 1524)—

(A) in subsection (a)—

(i) in paragraph (1), by striking ''section 2213'' and inserting ''section 2200'';

(ii) in paragraph (2), by striking ''section 102'' and inserting ''section 2200 of the Homeland Security Act of 2002'';

(iii) in paragraph (4), by striking ''section 2210(b)(1)'' and inserting ''section 2210(a)(1)''; and

(iv) 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(b) of the Homeland Security Act of 2002 (6 U.S.C. 660(b))''.

(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)'' and inserting ''section 2200''; 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 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)''.

(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) of the Homeland Security Act of 2002 (6 U.S.C. 659(m))'' and inserting ''section 2209(l) of the Homeland Security Act of 2002 (6 U.S.C. 659(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''.

TITLE LXIII—FEDERAL CYBERSECURITY REQUIREMENTS

SEC. 6301. EXEMPTION FROM FEDERAL CYBERSECURITY REQUIREMENTS.

(a) IN GENERAL.—Section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) is amended to read as follows:

''(2) EXCEPTION.—

''(A) IN GENERAL.—A particular requirement under paragraph (1) shall not apply to an agency information system of an agency if—

''(i) with respect to the agency information system, the head of the agency submits to the Director an application for an exemption from the particular requirement, in which the head of the agency personally certifies to the Director with particularity that—

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

''(II) the particular requirement is not necessary to secure the agency information system or agency information stored on or transiting the agency information system; and

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

''(ii) the head of the agency or the designee of the head of the agency has submitted the certification described in clause (i) to the appropriate congressional committees and any other congressional committee with jurisdiction over the agency; and

''(iii) the Director grants the exemption from the particular requirement.

''(B) DURATION OF EXEMPTION.—

''(i) IN GENERAL.—An exemption granted under subparagraph (A) shall expire on the date that is 1 year after the date on which the Director grants the exemption.

''(ii) RENEWAL.—Upon the expiration of an exemption granted to an agency under subparagraph (A), the head of the agency may apply for an additional exemption.''.

(b) REPORT ON EXEMPTIONS.—Section 3554(c)(1) of title 44, United States Code, as amended by section 5121 of this Act, is further amended—

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

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

(3) by adding at the end the following:

''(E) with respect to any exemptions the agency is granted by the Director of the Office of Management and Budget under section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) that is effective on the date of submission of the report, includes—

''(i) an identification of the particular requirements from which any agency information system (as defined in section 2210 of the Homeland Security Act of 2002 (6 U.S.C. 660)) is exempted; and

''(ii) for each requirement identified under subclause (I)—

''(I) an identification of the agency information system described in subclause (I) exempted from the requirement; and

''(II) an estimate of the date on which the agency will to be able to comply with the requirement.''.

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

SA 4800. Ms. KLOBUCHAR (for herself and Mr. BLUNT) submitted an amendment intended to be proposed by her to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. 1004. AVAILABILITY OF TRAVEL PROMOTION FUND FOR BRAND USA.

(a) SHORT TITLE.—This section may be cited as the ''Restoring Brand USA Act''.

(b) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Secretary of the Treasury, subject to subsections (c) and (d), and notwithstanding any other provision of law, shall make available, from unobligated balances remaining available from fees collected before October 1, 2020, and credited to Travel Promotion Fund established under subsection (d) of the Travel Promotion Act of 2009 (22 U.S.C. 2131(d)), $250,000,000 for the Corporation for Travel Promotion (commonly known as ''Brand USA'').

(c) INAPPLICABILITY OF CERTAIN REQUIREMENTS AND LIMITATIONS.—The limitations in subsection (d)(2)(B) of the Travel Promotion Act of 2009 shall not apply to amounts made available under subsection (b), and the requirements in subsection (d)(3) of such Act shall not apply to more than $50,000,000 of the amounts so available.

(d) USE OF FUNDS.—Brand USA may only use funds provided under subsection (b) to promote travel from countries whose citizens and nationals are permitted to enter the United States.

(e) REPORT REQUIRED.—Not later than 60 days after the date of the enactment of this Act, Brand USA shall submit to Congress a plan for obligating and expending the amounts described in subsection (b).

SA 4801. Mr. KENNEDY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. SBIR AND STTR PILOT PROGRAM FOR UNDERPERFORMING STATES.

Section 9 of the Small Business Act (15 U.S.C. 638) is amended by adding at the end the following:

''(vv) DEPARTMENT OF DEFENSE PILOT PROGRAM FOR UNDERPERFORMING STATES.—

''(1) DEFINITIONS.—In this section:

''(A) DEPARTMENT.—The term 'Department' means the Department of Defense.

''(B) UNDERPERFORMING STATE.—The term 'underperforming State' means any State participating in the SBIR or STTR program that is in the bottom 68 percent of all States historically receiving SBIR or STTR program funding.

''(2) ESTABLISHMENT.—The Secretary of Defense shall establish a pilot program to provide small business concerns located in underperforming States an increased level of assistance under the SBIR and STTR programs of the Department.

''(3) ACTIVITIES.—Under the pilot program, the Department, and any component agency thereof, may—

''(A) in any case in which the Department seeks to make a Phase II SBIR or STTR award to a small business concern based on the results of a Phase I award made to the small business concern by another agency, establish a streamlined transfer and fast track approval process for that Phase II award;

''(B) provide an additional Phase II SBIR or STTR award to a small business concern

located in an underperforming State that received a Phase I SBIR or STTR award, subject to an increase in the allocation percentage;

''(C) establish a program to make Phase 1.5 SBIR or STTR awards to small business concerns located in underperforming States in order to provide funding for 12 to 24 months to continue the development of technology; and

''(D) carry out subparagraph (C) along with other mentorship programs.

''(4) DURATION.—The pilot program established under this subsection shall terminate 5 years after the date on which the pilot program is established.

''(5) REPORT.—The Department shall submit to Congress an annual report on the status of the pilot program established under this subsection, including the improvement in funding under the SBIR and STTR programs of the Department provided to small business concerns located in underperforming States.''.

SA 4802. Mr. OSSOFF (for himself, Mr. TILLIS, Mr. KING, Ms. CORTEZ MASTO, Mr. ROUNDS, Mr. SCOTT of South Carolina, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. DR. DAVID SATCHER CYBERSECURITY EDUCATION GRANT PROGRAM.

(a) SHORT TITLE.—This section may be cited as the ''Cybersecurity Opportunity Act''.

(b) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) ENROLLMENT OF NEEDY STUDENTS.—The term ''enrollment of needy students'' has the meaning given the term in section 312(d) of the Higher Education Act of 1965 (20 U.S.C. 1058(d)).

(3) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ''historically Black college or university'' has the meaning given the term ''part B institution'' as defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(4) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(5) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means an institution listed in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(c) AUTHORIZATION OF GRANTS.—

(1) IN GENERAL.—Subject to the availability of appropriations, the Director shall carry out the Dr. David Satcher Cybersecurity Education Grant Program by—

(A) awarding grants to assist institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to establish or expand cybersecurity programs, to build and upgrade institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities, and to support such institutions on the path to producing qualified entrants in the cybersecurity workforce or becoming a National Center of Academic Excellence in Cybersecurity; and

(B) awarding grants to build capacity at institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to expand cybersecurity education opportunities, cybersecurity programs, cybersecurity research, and cybersecurity partnerships with public and private entities.

(2) RESERVATION.—The Director shall award not less than 50 percent of the amount available for grants under this section to historically Black colleges and universities and minority-serving institutions.

(3) COORDINATION.—The Director shall carry out this section in coordination with appropriate Federal agencies, including the Department of Homeland Security.

(4) SUNSET.—The Director's authority to award grants under paragraph (1) shall terminate on the date that is 5 years after the date the Director first awards a grant under paragraph (1).

(d) APPLICATIONS.—An eligible institution seeking a grant under subsection (a) shall submit an application to the Director at such time, in such manner, and containing such information as the Director may reasonably require, including a statement of how the institution will use the funds awarded through the grant to expand cybersecurity education opportunities at the eligible institution.

(e) ACTIVITIES.—An eligible institution that receives a grant under this section may use the funds awarded through such grant for increasing research, education, technical, partnership, and innovation capacity, including for—

(1) building and upgrading institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities;

(2) building and upgrading institutional capacity to provide hands-on research and training experiences for undergraduate and graduate students; and

(3) outreach and recruitment to ensure students are aware of such new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities.

(f) REPORTING REQUIREMENTS.—Not later than—

(1) 1 year after the effective date of this section, as provided in subsection (h), and annually thereafter until the Director submits the report under paragraph (2), the Director shall prepare and submit to Congress a report on the status and progress of implementation of the grant program under this section, including on the number and nature of institutions participating, the number and nature of students served by institutions receiving grants, the level of funding provided to grant recipients, the types of activities being funded by the grants program, and plans for future implementation and development; and

(2) 5 years after the effective date of this section, as provided in subsection (h), the Director shall prepare and submit to Congress a report on the status of cybersecurity education programming and capacity-building at institutions receiving grants under this section, including changes in the scale and scope of these programs, associated facilities, or in accreditation status, and on the educational and employment outcomes of students participating in cybersecurity programs that have received support under this section.

(g) PERFORMANCE METRICS.—The Director shall establish performance metrics for grants awarded under this section.

(h) EFFECTIVE DATE.—This section shall take effect 1 year after the date of enactment of this Act.

SA 4803. Ms. DUCKWORTH (for herself, Mr. KELLY, Ms. HIRONO, Ms. ROSEN, Mr. BENNET, Mr. HEINRICH, Mr. MORAN, Mr. YOUNG, Mrs. FEINSTEIN, Mrs. GILLIBRAND, Mr. KING, Mrs. SHAHEEN, Ms. KLOBUCHAR, Mr. DURBIN, Mr. PETERS, and Mr. BLUMENTHAL) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle B of title XII, add the following:

SEC. 1216. AFGHANISTAN WAR COMMISSION ACT OF 2021.

(a) SHORT TITLE.—This section may be cited as the ''Afghanistan War Commission Act of 2021''.

(b) DEFINITIONS.—In this section:

(1) APPLICABLE PERIOD.—The term ''applicable period'' means the period beginning June 1, 2001, and ending August 30, 2021.

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

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Foreign Relations of the Senate;

(C) the Select Committee on Intelligence of the Senate;

(D) the Committee on Appropriations of the Senate;

(E) the Committee on Armed Services of the House of Representatives;

(F) the Committee on Foreign Affairs of the House of Representatives;

(G) the Permanent Select Committee on Intelligence of the House of Representatives; and

(H) the Committee on Appropriations of the House of Representatives.

(3) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(c) ESTABLISHMENT OF COMMISSION.—

(1) ESTABLISHMENT.—There is established in the legislative branch an independent commission to be known as the Afghanistan War Commission (in this section referred to as the ''Commission'').

(2) MEMBERSHIP.—

(A) COMPOSITION.—The Commission shall be composed of 16 members of whom—

(i) 1 shall be appointed by the Chairman of the Committee on Armed Services of the Senate;

(ii) 1 shall be appointed by the ranking member of the Committee on Armed Services of the Senate;

(iii) 1 shall be appointed by the Chairman of the Committee on Armed Services of the House of Representatives;

(iv) 1 shall be appointed by the ranking member of the Committee on Armed Services of the House of Representatives;

(v) 1 shall be appointed by the Chairman of the Committee on Foreign Relations of the Senate;
(vi) 1 shall be appointed by the ranking member of the Committee on Foreign Relations of the Senate;
(vii) 1 shall be appointed by the Chairman of the Committee on Foreign Affairs of the House of Representatives;
(viii) 1 shall be appointed by the ranking member of the Committee on Foreign Affairs of the House of Representatives;
(ix) 1 shall be appointed by the Chairman of the Select Committee on Intelligence of the Senate;
(x) 1 shall be appointed by the ranking member of the Select Committee on Intelligence of the Senate.
(xi) 1 shall be appointed by the Chairman of the Permanent Select Committee on Intelligence of the House of Representatives;
(xii) 1 shall be appointed by the ranking member of the Permanent Select Committee on Intelligence of the House of Representatives;
(xiii) 1 shall be appointed by the majority leader of the Senate;
(xiv) 1 shall be appointed by the minority leader of the Senate;
(xv) 1 shall be appointed by the Speaker of the House of Representatives; and
(xvi) 1 shall be appointed by the Minority Leader of the House of Representatives.
(B) QUALIFICATIONS.—It is the sense of Congress that each member of the Commission appointed under subparagraph (A) should have significant professional experience in national security, such as a position in—
(i) the Department of Defense;
(ii) the Department of State;
(iii) the intelligence community;
(iv) the United States Agency for International Development; or
(v) an academic or scholarly institution.
(C) PROHIBITIONS.—A member of the Commission appointed under subparagraph (A) may not—
(i) be a current member of Congress;
(ii) be a former member of Congress who served in Congress after January 3, 2001;
(iii) be a current or former registrant under the Foreign Agents Registration Act of 1938 (22 U.S.C. 611 et seq.);
(iv) have previously investigated Afghanistan policy or the war in Afghanistan through employment in the office of a relevant inspector general;
(v) have been the sole owner or had a majority stake in a company that held any United States or coalition defense contract providing goods or services to activities by the United States Government or coalition in Afghanistan during the applicable period; or
(vi) have served, with direct involvement in actions by the United States Government in Afghanistan during the time the relevant official served, as—
(I) a cabinet secretary or national security adviser to the President; or
(II) a four-star flag officer, Under Secretary, or more senior official in the Department of Defense or the Department of State.
(D) DATE.—
(i) IN GENERAL.—The appointments of the members of the Commission shall be made not later than 60 days after the date of enactment of this Act.
(ii) FAILURE TO MAKE APPOINTMENT.—If an appointment under subparagraph (A) is not made by the appointment date specified in clause (i)—
(I) the authority to make such appointment shall expire; and
(II) the number of members of the Commission shall be reduced by the number equal to the number of appointments not made.
(3) PERIOD OF APPOINTMENT; VACANCIES.—
(A) IN GENERAL.—A member of the Commission shall be appointed for the life of the Commission.
(B) VACANCIES.—A vacancy in the Commission—
(i) shall not affect the powers of the Commission; and
(ii) shall be filled in the same manner as the original appointment.
(4) MEETINGS.—
(A) INITIAL MEETING.—Not later than 30 days after the date on which all members of the Commission have been appointed, the Commission shall hold the first meeting of the Commission.
(B) FREQUENCY.—The Commission shall meet at the call of the Co-Chairpersons.
(C) QUORUM.—A majority of the members of the Commission shall constitute a quorum, but a lesser number of members may hold hearings.
(5) CO-CHAIRPERSONS.—The Commission shall select, by a simple majority vote—
(A) 1 Co-Chairperson from the members of the Commission appointed by chairpersons of the appropriate congressional committees; and
(B) 1 Co-Chairperson from the members of the Commission appointed by the ranking members of the appropriate congressional committees.
(d) PURPOSE OF COMMISSION.— The purpose of the Commission is—
(1) to examine the key strategic, diplomatic, and operational decisions that pertain to the war in Afghanistan during the relevant period, including decisions, assessments, and events that preceded the war in Afghanistan; and
(2) to develop a series of lessons learned and recommendations for the way forward that will inform future decisions by Congress and policymakers throughout the United States Government.
(e) DUTIES OF COMMISSION.—
(1) STUDY.—
(A) IN GENERAL.—The Commission shall conduct a thorough study of all matters relating to combat operations, reconstruction and security force assistance activities, intelligence operations, and diplomatic activities of the United States pertaining to the Afghanistan during the period beginning September 1, 1996, and ending August 30, 2021.
(B) MATTERS STUDIED.—The matters studied by the Commission shall include—
(i) for the time period specified under subparagraph (A)—
(I) the policy objectives of the United States Government, including—
(aa) military objectives;
(bb) diplomatic objectives;
(cc) development objectives; and
(dd) intelligence objectives;
(II) significant decisions made by the United States, including the development of options presented to policymakers;
(III) the efficacy of efforts by the United States Government in meeting the objectives described in clause (i), including an analysis of —
(aa) military efforts;
(bb) diplomatic efforts;
(cc) development efforts; and
(dd) intelligence efforts; and
(IV) the efficacy of counterterrorism efforts against al Qaeda, the Islamic State Khorasan Province, and other foreign terrorist organizations in degrading the will and capabilities of such organizations—
(aa) to mount external attacks against the United States mainland or its allies and partners; or
(bb) to threaten regional stability in Afghanistan and neighboring countries.
(ii) the efficacy of metrics, measures of effectiveness, and milestones used to assess progress of diplomatic, military, and intelligence efforts;
(iii) the efficacy of interagency planning and execution process by the United States Government;
(iv) factors that led to the collapse of the Afghan National Defense Security Forces in 2021, including—
(I) training;
(II) assessment methodologies;
(III) building indigenous forces on western models;
(IV) reliance on technology and logistics support; and
(V) reliance on warfighting enablers provided by the United States;
(v) the efficacy of counter-corruption efforts to include linkages to diplomatic lines of effort, linkages to foreign and security assistance, and assessment methodologies;
(vi) the efficacy of counter-narcotic efforts to include alternative livelihoods, eradication, interdiction, and education efforts;
(vii) the role of countries neighboring Afghanistan in contributing to the instability of Afghanistan;
(viii) varying diplomatic approaches between Presidential administrations;
(ix) the extent to which the intelligence community did or did not fail to provide sufficient warning about the probable outcomes of a withdrawal of coalition military support from Afghanistan, including as it relates to—
(I) the capability and sustainability of the Afghanistan National Defense Security Forces;
(II) the sustainability of the Afghan central government, absent coalition support;
(III) the extent of Taliban control over Afghanistan over time with respect to geographic territory, governance, and influence; and
(IV) the likelihood of the Taliban regaining control of Afghanistan at various levels of United States and coalition support, including the withdrawal of most or all United States or coalition support;
(x) the extent to which intelligence products related to the state of the conflict in Afghanistan and the effectiveness of the Afghanistan National Defense Security Forces complied with intelligence community-wide analytic tradecraft standards and fully reflected the divergence of analytic views across the intelligence community;
(xi) an evaluation of whether any element of the United States Government inappropriately restricted access to data from elements of the intelligence community, Congress, or the Special Inspector General for Afghanistan Reconstruction (SIGAR) or any other oversight body such as other inspectors general or the Gpvernment Accountability Office, including through the use of overclassification; and
(xii) the extent to which public representations of the situation in Afghanistan before Congress by United States Government officials were not consistent with the most recent formal assessment of the intelligence community at the time those representations were made.
(2) REPORT REQUIRED.—
(A) IN GENERAL.—
(i) ANNUAL REPORT.—
(I) IN GENERAL.—Not later than 1 year after the date of the initial meeting of the Commission, and annually thereafter, the Commission shall submit to the appropriate congressional committees a report describing the progress of the activities of the Commission as of the date of such report, including any findings, recommendations, or lessons learned endorsed by the Commission.
(II) ADDENDA.—Any member of the Commission may submit an addendum to a report required under subclause (I) setting

forth the separate views of such member with respect to any matter considered by the Commission.

(III) BRIEFING.—On the date of the submission of the first annual report, the Commission shall brief Congress.

(ii) FINAL REPORT.—

(I) SUBMISSION.—Not later than 3 years after the date of the initial meeting of the Commission, the Commission shall submit to Congress a report that contains a detailed statement of the findings, recommendations, and lessons learned endorsed by the Commission.

(II) ADDENDA.—Any member of the Commission may submit an addendum to the report required under subclause (I) setting forth the separate views of such member with respect to any matter considered by the Commission.

(III) EXTENSION.—The Commission may submit the report required under subclause (I) at a date that is not more than 1 year later than the date specified in such clause if agreed to by the chairperson and ranking member of each of the appropriate congressional committees.

(B) FORM.—The report required by paragraph (1)(B) shall be submitted and publicly released on a Government website in unclassified form but may contain a classified annex.

(C) SUBSEQUENT REPORTS ON DECLASSIFICATION.—

(i) IN GENERAL.—Not later than 4 years after the date that the report required by subparagraph (A)(ii) is submitted, each relevant agency of jurisdiction shall submit to the committee of jurisdiction a report on the efforts of such agency to declassify such annex.

(ii) CONTENTS.—Each report required by clause (i) shall include—

(I) a list of the items in the classified annex that the agency is working to declassify at the time of the report and an estimate of the timeline for declassification of such items;

(II) a broad description of items in the annex that the agency is declining to declassify at the time of the report; and

(III) any justification for withholding declassification of certain items in the annex and an estimate of the timeline for declassification of such items.

(f) POWERS OF COMMISSION.—

(1) HEARINGS.—The Commission may hold such hearings, take such testimony, and receive such evidence as the Commission considers necessary to carry out its purpose and functions under this section.

(2) ASSISTANCE FROM FEDERAL AGENCIES.—

(A) INFORMATION.—

(i) IN GENERAL.—The Commission may secure directly from a Federal department or agency such information as the Commission considers necessary to carry out this section.

(ii) FURNISHING INFORMATION.—Upon receipt of a written request by the Co-Chairpersons of the Commission, the head of the department or agency shall expeditiously furnish the information to the Commission.

(B) SPACE FOR COMMISSION.—Not later than 30 days after the date of the enactment of this Act, the Administrator of General Services, in consultation with the Commission, shall identify and make available suitable excess space within the Federal space inventory to house the operations of the Commission. If the Administrator of General Services is not able to make such suitable excess space available within such 30-day period, the Commission may lease space to the extent that funds are available for such purpose.

(3) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as other departments and agencies of the Federal Government.

(4) GIFTS.—The Commission may accept, use, and dispose of gifts or donations of services, goods, and property from non-Federal entities for the purposes of aiding and facilitating the work of the Commission. The authority in this subsection does not extend to gifts of money. Gifts accepted under this authority shall be documented, and conflicts of interest or the appearance of conflicts of interest shall be avoided. Subject to the authority in this section, commissioners shall otherwise comply with rules set forth by the Select Committee on Ethics of the Senate and the Committee on Ethics of the House of Representatives governing employees of the Senate and the House of Representatives.

(5) LEGISLATIVE ADVISORY COMMITTEE.—The Commission shall operate as a legislative advisory committee and shall not be subject to the provisions of the Federal Advisory Committee Act (Public Law 92–463; 5 U.S.C. App) or section 552b, United States Code (commonly known as the Government in the Sunshine Act).

(g) COMMISSION PERSONNEL MATTERS.—

(1) COMPENSATION OF MEMBERS.—A member of the Commission who is not an officer or employee of the Federal Government shall be compensated at a rate equal to the daily equivalent of the annual rate of basic pay prescribed for level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day (including travel time) during which the member is engaged in the performance of the duties of the Commission.

(2) TRAVEL EXPENSES.—A member of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Commission.

(3) STAFF.—

(A) STATUS AS FEDERAL EMPLOYEES.—Notwithstanding the requirements of section 2105 of title 5, United States Code, including the required supervision under subsection (a)(3) of such section, the members of the commission shall be deemed to be Federal employees.

(B) EXECUTIVE DIRECTOR.—The Commission shall appoint and fix the rate of basic pay for an Executive Director in accordance with section 3161(d) of title 5, United States Code.

(C) PAY.—The Executive Director, with the approval of the Commission, may appoint and fix the rate of basic pay for additional personnel as staff of the Commission in accordance with section 3161(d) of title 5, United States Code.

(4) DETAIL OF GOVERNMENT EMPLOYEES.—A Federal Government employee may be detailed to the Commission without reimbursement, and such detail shall be without interruption or loss of civil service status or privilege.

(5) PROCUREMENT OF TEMPORARY AND INTERMITTENT SERVICES.—The Co-Chairpersons of the Commission may procure temporary and intermittent services under section 3109(b) of title 5, United States Code, at rates for individuals that do not exceed the daily equivalent of the annual rate of basic pay prescribed for level V of the Executive Schedule under section 5316 of that title.

(h) TERMINATION OF COMMISSION.—The Commission shall terminate 90 days after the date on which the Commission submits the report required under subsection (e)(2)(A)(ii).

(i) AUTHORIZATION OF APPROPRIATIONS.—

(1) INCREASE.—The amount authorized to be appropriated by section 4301 for Operation and Maintenance, Defense-wide, for the Office of the Secretary of Defense, is hereby increased by $3,000,000.

(2) OFFSET.—The amount authorized to be appropriated by section 4301 for Operation and Maintenance, Afghanistan Security Forces Fund, for Afghanistan Air Force, Line 090, is hereby reduced by $3,000,000.

SA 4804. Mr. YOUNG submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle E of title XII, add the following:

SEC. 1253. REPORT ON GEOSTRATEGIC INTERESTS AND NATIONAL SECURITY IMPLICATIONS RELATED TO TRADE IN INDO-PACIFIC REGION.

(a) IN GENERAL.—Not later than 150 days after the date of the enactment of this Act, the United States Trade Representative, in coordination with the Secretary of Defense, the Secretary of State, the Secretary of Commerce, and the Secretary of Homeland Security, shall submit to Congress and make available to the public a report on geostrategic interests and national security implications related to trade in the Indo-Pacific region.

(b) ELEMENTS.—The report required by subsection (a) shall include an assessment of the following:

(1) How reductions in tariffs, revisions in government procurement rules, and other market access commitments by countries in the Indo-Pacific region could potentially affect United States producers and supply chains deemed critical for national security purposes.

(2) How agreements by those countries, including with respect to strengthening investment and intellectual property rights, could potentially affect the development by the United States of critical new technologies.

(3) How agreements by those countries relating to digital trade could potentially affect United States cybersecurity, including potential agreements entered into with the United States to promote cybersecurity and open data flows and to combat discriminatory practices and government censorship.

(4) How tariff and nontariff barriers imposed by those countries and trade agreements by those countries could broadly affect geostrategic United States interests, partnerships, and alliances.

(5) Current and predicted foreign direct investment in the Indo-Pacific region by the People's Republic of China.

(6) How agreements by those countries could counter the semiconductor policies of the Government of the People's Republic of China, particularly those policies that could lead to the transfer of intellectual property, research and development, and manufacturing to the People's Republic of China.

(c) PUBLIC HEARING.—The Trade Representative and the officials specified in subsection (a) shall jointly conduct a public hearing and invite witnesses to testify with respect to the elements described in subsection (b).

SA 4805. Ms. CORTEZ MASTO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place in title X, insert the following:

Subtitle ____—Veterans Matters

SEC. _____. EXTENSIONS OF CERTAIN PROVISIONS OF LAW RELATING TO BENEFITS PROVIDED UNDER DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE PROGRAMS DURING COVID–19 PANDEMIC.

(a) EXTENSION OF STUDENT VETERAN CORONAVIRUS RESPONSE ACT OF 2020.—Section 2 of the Student Veteran Coronavirus Response Act of 2020 (Public Law 116–140; 38 U.S.C. 3031 note), as amended by section 5202(a) of the Department of Veterans Affairs Expiring Authorities Act of 2020 (division E of Public Law 116–159), is further amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(b) EXTENSION OF PAYMENT OF WORK-STUDY ALLOWANCES DURING EMERGENCY SITUATION.—Section 3 of the Student Veteran Coronavirus Response Act of 2020 (38 U.S.C. 3485 note) is amended by striking ''During the covered period'' and inserting ''During the period beginning on March 1, 2020, and ending on June 1, 2022''.

(c) EXTENSION OF PERIOD FOR CONTINUATION OF DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE BENEFITS FOR CERTAIN PROGRAMS OF EDUCATION CONVERTED TO DISTANCE LEARNING BY REASON OF EMERGENCIES AND HEALTH-RELATED SITUATIONS.—Section 1(b) of Public Law 116–128 (38 U.S.C. 3001 note prec.), as amended by section 5202(b) of the Department of Veterans Affairs Expiring Authorities Act of 2020 (division E of Public Law 116–159), is further amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(d) EXTENSION OF MODIFICATION OF TIME LIMITATIONS ON USE OF ENTITLEMENT TO MONTGOMERY GI BILL AND VOCATIONAL REHABILITATION AND TRAINING.—Section 1105 of the Johnny Isakson and David P. Roe, M.D. Veterans Health Care and Benefits Improvement Act of 2020 (Public Law 116–315) is amended by striking ''December 21, 2021'' each place it appears and inserting ''June 1, 2022''.

(e) EXTENSION OF CONTINUATION OF DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE BENEFITS DURING COVID–19 EMERGENCY.—Section 1102(e) of the Johnny Isakson and David P. Roe, M.D. Veterans Health Care and Benefits Improvement Act of 2020 (Public Law 116–315) is amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(f) EXTENSION OF PROVISIONS RELATING TO EFFECTS OF CLOSURE OF EDUCATIONAL INSTITUTION AND MODIFICATION OF COURSES BY REASON OF COVID–19 EMERGENCY.—Section 1103(h) of such Act is amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(g) EXTENSION OF PROVISION RELATING TO PAYMENT OF EDUCATIONAL ASSISTANCE IN CASES OF WITHDRAWAL.—Section 1104(a) of such Act is amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(h) EXTENSION OF PROVISION RELATING TO APPRENTICESHIP OR ON-JOB TRAINING REQUIREMENTS.—Section 1106(b) of such Act is amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

SEC. _____. MODIFICATIONS TO REQUIREMENTS FOR EDUCATIONAL INSTITUTIONS PARTICIPATING IN THE EDUCATIONAL ASSISTANCE PROGRAMS OF THE DEPARTMENT OF VETERANS AFFAIRS.

(a) WAIVER OF VERIFICATION OF ENROLLMENT FOR CERTAIN EDUCATIONAL INSTITUTIONS.—Section 3313(l) of title 38, United States Code, is amended by adding at the end the following new paragraph:

''(4) WAIVER.—The Secretary may waive the requirements of this subsection for an educational institution that the Secretary has determined uses a flat tuition and fee structure that would make the use of a second verification under this subsection unnecessary.''.

(b) LIMITATIONS ON AUTHORITY TO DISAPPROVE OF COURSES.—

(1) IN GENERAL.—Subsection (f) of section 3679 of title 38, United States Code, is amended—

(A) in paragraph (2)(B),

(i) by inserting '', except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance'' after ''assistance''; and

(ii) by adding at the end the following new subparagraph:

''(C) In determining whether a violation of subparagraph (B) has occurred, the State approving agency, or the Secretary when acting in the place of the State approving agency, shall construe the requirements of this paragraph in accordance with the regulations and guidance prescribed by the Secretary of Education under section 487(a)(20) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)(20)).'';

(B) by redesignating paragraph (7) as paragraph (8); and

(C) by inserting after paragraph (6) the following new paragraph (7):

''(7) This subsection shall not apply to an educational institution—

''(A) located in a foreign country; or

''(B) that provides to a covered individual consumer information regarding costs of the program of education (including financial aid available to such covered individual) using a form or template developed by the Secretary of Education.''.

(2) APPLICATION DATE.—The Secretary of Veterans Affairs may not carry out subsection (f) of section 3679 of title 38, United States Code, until August 1, 2022, except that, beginning on June 15, 2022, an educational institution may submit an application for a waiver under paragraph (5) of such subsection.

(3) CONFORMING AMENDMENTS.—Subsection (c) of section 3696 of such title is amended—

(A) by inserting ''(1)'' before ''An educational'';

(B) by inserting '', except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance'' after ''assistance''; and

(C) by adding at the end the following new paragraph:

''(2) In determining whether a violation of paragraph (1) has occurred, the Under Secretary for Benefits shall construe the requirements of this paragraph in accordance with the regulations and guidance prescribed by the Secretary of Education under section 487(a)(20) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)(20)).''.

(c) EXEMPTION OF FOREIGN SCHOOLS FROM CERTAIN REQUIREMENTS.—

(1) INFORMATION RELATING TO TESTS.—Section 3689(c) of title 38, United States Code, is amended by adding at the end the following new paragraph:

''(3) Subparagraph (G) of paragraph (1) shall not apply with respect to an educational institution located in a foreign country.''.

(2) EXAMINATION OF RECORDS.—Section 3690(c) of title 38, United States Code, is amended—

(A) by striking ''Notwithstanding'' and inserting ''(1) Except as provided in paragraph (2), notwithstanding''; and

(B) by adding at the end the following new paragraph:

''(2) Paragraph (1) does not apply to the records and accounts—

''(A) of an educational institution located in a foreign country; and

''(B) that pertain to an individual who is not receiving educational assistance under this chapter.''.

SEC. _____. CONTINUATION OF DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE BENEFITS FOR CERTAIN PROGRAMS OF EDUCATION CONVERTED TO DISTANCE LEARNING BY REASON OF EMERGENCIES AND HEALTH-RELATED SITUATIONS.

(a) IN GENERAL.—In the case of a program of education approved by a State approving agency, or the Secretary of Veterans Affairs when acting in the role of a State approving agency, that is converted from being offered on-site at an educational institution to being offered by distance learning by reason of an emergency or health-related situation, as determined by the Secretary, the Secretary may continue to provide educational assistance under the laws administered by the Secretary without regard to such conversion, including with respect to paying any—

(1) monthly housing stipends under chapter 33 of title 38, United States Code; or

(2) payments or subsistence allowances under chapters 30, 31, 32, and 35 of such title and chapters 1606 and 1607 of title 10, United States Code.

(b) APPLICABILITY PERIOD.—Subsection (a) shall apply during the period beginning on December 21, 2021, and ending on June 1, 2022.

(c) DEFINITIONS.—In this section:

(1) EDUCATIONAL INSTITUTION.—The term ''educational institution'' has the meaning given that term in section 3452 of title 38, United States Code, and includes an institution of higher learning (as defined in such section).

(2) PROGRAM OF EDUCATION.—The term ''program of education'' has the meaning given that term in section 3002 of title 38, United States Code.

(3) STATE APPROVING AGENCY.—The term ''State approving agency'' has the meaning given that term in section 3671 of title 38, United States Code.

SEC. _____. BUDGETARY EFFECTS.

(a) IN GENERAL.—Amounts provided to carry out the amendments made by this subtitle are designated as an emergency requirement pursuant to section 4(g) of the Statutory Pay-As-You-Go Act of 2010 (2 U.S.C. 933(g)).

(b) DESIGNATION IN SENATE.—In the Senate, amounts provided to carry out the amendments made by this subtitle are designated as an emergency requirement pursuant to section 4112(a) of H. Con. Res. 71 (115th Congress), the concurrent resolution on the budget for fiscal year 2018.

SA 4806. Ms. SMITH (for herself and Mr. YOUNG) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—EMERGENCY PREPAREDNESS

SEC. __01. SHORT TITLE.

This title may be cited as the ''Advancing Emergency Preparedness Through One Health Act of 2021''.

SEC. __02. FINDINGS.

Congress finds the following:

(1) The term ''One Health'' reflects the interconnectedness of human health, animal health, and the environment. As technology and population growth facilitates increased interaction of human settlements with wildlife habitats and as international travel and trade increases, the interface between these elements will also continue to rise.

(2) When zoonotic diseases spill over to humans, there are often enormous health and economic costs. The World Bank estimates that, between 1997 and 2009, the global costs from six zoonotic outbreaks exceeded $80,000,000,000 and the Centers for Disease Control and Prevention estimates that there are annually 2,500,000,000 cases of zoonotic infections globally, resulting in 2,700,000 deaths.

(3) There are also immense effects on the agriculture sector. In 2014 and 2015, a high pathogenic avian influenza (HPAI) outbreak in the United States led to the cull of nearly 50,000,000 birds, and imposed up to approximately $3,300,000,000 in losses for poultry and egg farmers, animal feed producers, baked good production, and other related industries.

(4) Public health preparedness depends on agriculture in a variety of ways. For example, a wide range of vaccines, including those for influenza, yellow fever, rabies, and measles-mumps-rubella (MMR), are primarily cultivated in poultry eggs. Egg shortages resulting from zoonotic disease outbreaks could impose serious risks to vaccine manufacturing efforts.

(5) It is estimated that approximately 80 percent of potential pathogens likely to be used in bioterrorism or biowarfare are common zoonotic pathogens.

(6) While existing Federal Government initiatives related to One Health span multiple agencies, including the Centers for Disease Control and Prevention One Health office and the Department of Agriculture Animal and Plant Health Inspection Services' One Health Coordination Center, additional interagency coordination is necessary to help better prevent, prepare for, and respond to zoonotic disease outbreaks.

SEC. __03. INTERAGENCY ONE HEALTH PROGRAM.

(a) IN GENERAL.—The Secretary of the Interior, the Secretary of Health and Human Services, and the Secretary of Agriculture (referred to in this title as the ''Secretaries''), in coordination with the United States Agency for International Development, the Environmental Protection Agency, the Department of Homeland Security, the Department of Defense, the Department of Commerce, and other departments and agencies as appropriate, shall develop, publish, and submit to Congress a national One Health Framework (referred to in this title as the ''framework'') for coordinated Federal Activities under the One Health Program.

(b) NATIONAL ONE HEALTH FRAMEWORK.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretaries, in cooperation with the United States Agency for International Development, the Environmental Protection Agency, the Department of Homeland Security, the Department of Defense, the Department of Commerce, and other departments and agencies as appropriate, shall develop, publish, and submit to Congress a One Health Framework (referred to in this section as the ''framework'') for coordinated Federal activities under the One Health Program.

(2) CONTENTS OF FRAMEWORK.—The framework described in paragraph (1) shall describe existing efforts and contain recommendations for building upon and complementing the activities of the Department of the Interior, the Centers for Disease Control and Prevention, the Food and Drug Administration, the Office of the Assistant Secretary for Preparedness and Response, the Department of Agriculture, the United States Agency for International Development, the Environmental Protection Agency, the National Institutes of Health, the Department of Homeland Security, and other departments and agencies, as appropriate, and shall—

(A) assess, identify, and describe, as appropriate, existing activities of Federal agencies and departments under the One Health Program and consider whether all relevant agencies are adequately represented;

(B) for the 10-year period beginning in the year the framework is submitted, establish specific Federal goals and priorities that most effectively advance—

(i) scientific understanding of the connections between human, animal, and environmental health;

(ii) coordination and collaboration between agencies involved in the framework including sharing data and information, engaging in joint fieldwork, and engaging in joint laboratory studies related to One Health;

(iii) identification of priority zoonotic diseases and priority areas of study;

(iv) surveillance of priority zoonotic diseases and their transmission between animals and humans;

(v) prevention of priority zoonotic diseases and their transmission between animals and humans;

(vi) protocol development to improve joint outbreak response to and recovery from zoonotic disease outbreaks in animals and humans; and

(vii) workforce development to prevent and respond to zoonotic disease outbreaks in animals and humans;

(C) describe specific activities required to achieve the goals and priorities described in subparagraph (B), and propose a timeline for achieving these goals;

(D) identify and expand partnerships, as appropriate, among Federal agencies, States, Indian tribes, academic institutions, nongovernmental organizations, and private entities in order to develop new approaches for reducing hazards to human and animal health and to strengthen understanding of the value of an integrated approach under the One Health Program to addressing public health threats in a manner that prevents duplication;

(E) identify best practices related to State and local-level research coordination, field activities, and disease outbreak preparedness, response, and recovery related to One Health; and

(F) provide recommendations to Congress regarding additional action or legislation that may be required to assist in establishing the One Health Program.

(3) ADDENDUM.—Not later than 3 years after the creation of the framework, the Secretaries, in coordination with the agencies described in paragraph (1), shall submit to Congress an addendum to the framework that describes the progress made in advancing the activities described in the framework.

(c) AUTHORIZATION OF APPROPRIATIONS.—To carry out this section, there is authorized to be appropriated such sums as may be necessary.

SEC. __04. GAO REPORT.

Not later than 2 years after the date of the submission of the addendum under section __03(b)(3), the Comptroller General of the United States shall submit to Congress a report that—

(1) details existing collaborative efforts between the Department of the Interior, the Centers for Disease Control and Prevention, the Food and Drug Administration, the Department of Agriculture, the United States Agency for International Development, the Environmental Protection Agency, the National Institutes of Health, the Department of Homeland Security, and other departments and agencies to prevent and respond to zoonotic disease outbreaks in animals and humans; and

(2) contains an evaluation of the framework and the specific activities requested to achieve the framework.

SA 4807. Ms. SMITH (for herself, Mr. CASSIDY, and Ms. WARREN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. 1064. STUDY AND REPORT ON THE REDISTRIBUTION OF COVID–19 VACCINE DOSES THAT WOULD OTHERWISE EXPIRE TO FOREIGN COUNTRIES AND ECONOMIES.

(a) STUDY.—

(1) IN GENERAL.—The Secretary of Health and Human Services, in consultation with the Secretary of State and the Administrator of the United States Agency for International Development, shall conduct a study to identify and analyze the logistical prerequisites for the collection of unused and unexpired doses of the COVID–19 vaccine in the United States and for the distribution of such doses to foreign countries and economies.

(2) MATTERS STUDIED.—The matters studied by the Secretary of Health and Human Services under paragraph (1) shall include—

(A) options for the collection of unused and unexpired doses of the COVID–19 vaccine from entities in the United States;

(B) methods for the collection and shipment of such doses to foreign countries and economies;

(C) methods for ensuring the appropriate storage and handling of such doses during and following the distribution and delivery of the doses to such countries and economies;

(D) the capacity and capability of foreign countries and economies receiving such doses to distribute and administer the doses while assuring their safety and quality;

(E) the minimum supply of doses of the COVID–19 vaccine necessary to be retained within the United States; and

(F) other Federal agencies with which the heads of the relevant agencies should coordinate to accomplish the tasks described in subparagraphs (A) through (E) and the degree of coordination necessary between such agencies.

(b) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Health and Human Services, in consultation with the other heads of the relevant agencies, shall submit to the appropriate congressional committees a report on the results of the study conducted under subsection (a).

(c) DEFINITIONS.—In this section:

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

(A) the Committee on Health, Education, Labor, and Pensions, and the Committee on Foreign Relations of the Senate; and

(B) the Committee on Energy and Commerce, and the Committee on Foreign Affairs of the House of Representatives.

(2) RELEVANT AGENCIES.—The term ''relevant agencies'' means—

(A) the Department of Health and Human Services;

(B) the Department of State; and

(C) the United States Agency for International Development.

SA 4808. Mrs. FEINSTEIN (for herself, Ms. ERNST, Mr. DURBIN, Ms. COLLINS, Ms. HIRONO, Ms. ROSEN, Mr. PETERS, Mr. CORNYN, and Ms. DUCKWORTH) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle B of title XII, add the following:

SEC. 1216. STATUS OF WOMEN AND GIRLS IN AFGHANISTAN.

(a) FINDINGS.—Congress finds the following:

(1) Since May 2021, the escalation of violent conflict in Afghanistan has forcibly displaced an estimated 655,000 civilians, and 80 percent of those forced to flee are women and children.

(2) Since regaining control of Afghanistan in August 2021, the Taliban have taken actions reminiscent of their brutal rule in the late 1990s, including by cracking down on protesters, detaining and beating journalists, reestablishing the Ministry for the Promotion of Virtue and Prevention of Vice, and requiring women to study at universities in gender-segregated classrooms while wearing Islamic attire.

(3) Until the Taliban assumed control of the country in August 2021, the women and girls of Afghanistan had achieved much since 2001, even as insecurity, poverty, underdevelopment, and patriarchal norms continued to limit their rights and opportunities in much of Afghanistan.

(4) Through strong support from the United States and the international community—

(A) female enrollment in public schools in Afghanistan continued to increase through 2015, with an estimated high of 50 percent of school age girls attending; and

(B) by 2019—

(i) women held political leadership positions, and women served as ambassadors; and

(ii) women served as professors, judges, prosecutors, defense attorneys, police, military members, health professionals, journalists, humanitarian and developmental aid workers, and entrepreneurs.

(5) Efforts to empower women and girls in Afghanistan continue to serve the national interests of Afghanistan and the United States because women are sources of peace and economic progress.

(6) With the return of Taliban control, the United States has little ability to preserve the human rights of women and girls in Afghanistan, and those women and girls may again face the intimidation and marginalization they faced under the last Taliban regime.

(7) Women and girls in Afghanistan are again facing gender-based violence, including—

(A) forced marriage;

(B) intimate partner and domestic violence;

(C) sexual harassment;

(D) sexual violence, including rape; and

(E) emotional and psychological violence.

(8) Gender-based violence has always been a significant problem in Afghanistan and is expected to become more widespread with the Taliban in control. In 2020, even before the Taliban assumed control of the country, some studies projected that 87 percent of Afghan women and girls will experience at least one form of gender-based violence in their lifetime, with 62 percent experiencing multiple incidents of such violence.

(9) Prior to the Taliban takeover in August 2021, approximately 7,000,000 people in Afghanistan lacked or had limited access to emergency and primary health services as a result of inadequate public health coverage, weak health systems, and conflict-related interruptions in care.

(10) Women and girls faced additional challenges, as their access to prenatal, childbirth, and postpartum care was limited due to a shortage of female medical staff, cultural barriers, stigma and fears of reprisals following sexual violence, or other barriers to mobility, including security fears.

(11) Only approximately 50 percent of pregnant women and girls in Afghanistan deliver their children in a health facility with a professional attendant, which increases the risk of complications in childbirth and preventable maternal mortality.

(12) Food insecurity in Afghanistan is also posing a variety of threats to women and girls, as malnutrition weakens their immune systems and makes them more susceptible to infections, complications during pregnancy, and risks during childbirth.

(13) With the combined impacts of ongoing conflict and COVID–19, Afghan households increasingly resort to child marriage, forced marriage, and child labor to address food insecurity and other effects of extreme poverty.

(14) In Afghanistan, the high prevalence of anemia among adolescent girls reduces their ability to survive childbirth, especially when coupled with high rates of child marriage and forced marriage and barriers to accessing prenatal and childbirth services.

(b) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) since 2001, organizations and networks promoting the empowerment of women and girls have been important engines of social, economic, and political development in Afghanistan;

(2) any future political order in Afghanistan should secure the political, economic, and social gains made by Afghan women and work to increase the equal treatment of women and girls;

(3) respecting the internationally recognized human rights of all people is essential to securing lasting peace and sustainable development in Afghanistan;

(4) in cooperation with international partners, the United States must endeavor to preserve the hard-won gains made in Afghanistan during the past two decades, particularly as related to the social, economic and political empowerment of women and girls in society;

(5) the continued provision of humanitarian assistance in Afghanistan should be targeted toward the most vulnerable, including for the protection, education, and well-being of women and girls;

(6) immediate and ongoing humanitarian needs in Afghanistan can only be met by a humanitarian response that includes formal agreements between local nongovernmental organizations and international partners that promotes the safe access and participation of female staff at all levels and across functional roles among all humanitarian actors; and

(7) a lack of aid would exacerbate the current humanitarian crisis and harm the well-being of women and girls in Afghanistan.

(c) POLICY OF THE UNITED STATES REGARDING THE RIGHTS OF WOMEN AND GIRLS OF AFGHANISTAN.—

(1) IN GENERAL.—It is the policy of the United States—

(A) to continue to support the internationally recognized human rights of women and girls in Afghanistan following the withdrawal of the United States Armed Forces from Afghanistan, including through mechanisms to hold all parties publicly accountable for violations of international humanitarian law and violations of such rights against women and girls;

(B) to strongly oppose any weakening of the political or economic rights of women and girls in Afghanistan;

(C) to use the voice and influence of the United States at the United Nations to promote, respect, and uphold the internationally recognized human rights of the women and girls of Afghanistan, including the right to safely work;

(D) to identify individuals who violate the internationally recognized human rights of women and girls in Afghanistan, such as by committing acts of murder, lynching, and grievous domestic violence against women, and to press for bringing those individuals to justice; and

(E) to systematically consult with Afghan women and girls on their needs and priorities in the development, implementation, and monitoring of humanitarian action, including women and girls who are part of the Afghan diaspora community.

(d) HUMANITARIAN ASSISTANCE AND AFGHAN WOMEN.—The Administrator of the United States Agency for International Development should work to ensure that Afghan women are employed and enabled to work in the delivery of humanitarian assistance in Afghanistan, to the extent practicable.

(e) REPORT ON WOMEN AND GIRLS IN AFGHANISTAN.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter through 2024, the Secretary of State shall submit to the appropriate committees of Congress, and make available to the public, a report that includes the following:

(A) An assessment of the status of women and girls in Afghanistan following the departure of United States and partner military forces, including with respect to access to primary and secondary education, jobs, primary and emergency health care, and legal protections and status.

(B) An assessment of the political and civic participation of women and girls in Afghanistan.

(C) An assessment of the prevalence of gender-based violence in Afghanistan.

(D) A report on funds for United States foreign assistance obligated or expended during the period covered by the report to advance

gender equality and the internationally recognized human rights of women and girls in Afghanistan, including funds directed toward local organizations promoting such rights of women and girls, that includes the following:

(i) The amounts awarded to principal recipients and sub-recipients for such purposes during the reporting period.

(ii) A description of each program for which such funds are used for such purposes.

(2) ASSESSMENT.—

(A) INPUT.—The assessment described in paragraph (1)(A) shall include the input of—

(i) Afghan women and girls;

(ii) organizations employing and working with Afghan women and girls; and

(iii) humanitarian organizations, including faith-based organizations, providing assistance in Afghanistan.

(B) SAFETY AND CONFIDENTIALITY.—In carrying out the assessment described in paragraph (1)(A), the Secretary shall, to the maximum extent practicable, ensure the safety and confidentiality of personal information of each individual who provides information from within Afghanistan.

(3) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the Committee on Foreign Relations and the Committee on Appropriations of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives.

SA 4809. Mr. WARNER submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle E of title V, add the following:

SEC. 576. COUNTERING EXTREMISM IN THE ARMED FORCES.

(a) IN GENERAL.—The Secretary of Defense shall—

(1) promulgate policy that prohibits and defines participation in extremist activities;

(2) develop and implement programs, resources, and activities to counter extremism within the Armed Forces, including screening of publicly available information and Insider Threat Programs;

(3) collect and report data on incidents, allegations, investigations, disciplinary actions, and separations related to extremism, as well as publication of reports on these data in a regular, public, and transparent manner; and

(4) designate a senior official, to be known as the ''Senior Official for Countering Extremism'', within the Department of Defense as responsible for facilitation and coordination of the activities described in this subsection with personnel and readiness officials, law enforcement organizations, security organizations, insider threat programs, and watch lists related to extremism in the Armed Forces.

(b) TRAINING AND EDUCATION.—

(1) IN GENERAL.—The Secretary of each military department, in coordination with the Senior Official for Countering Extremism, shall develop and implement training and education programs and related materials to assist members of the Armed Forces and civilian employees of the Department of Defense in identifying, preventing, responding to, reporting, and mitigating the risk of extremist activities.

(2) CONTENT.—The training and education described in paragraph (1) shall include specific material for activities determined by the Senior Official for Countering Extremism as high risk for extremist activities, including recruitment activities and separating members of the Armed Forces.

(3) REQUIREMENTS.—The Secretary of Defense, in consultation with the Secretary of Homeland Security, shall provide the training and education described paragraph (1)—

(A) to a member of the Armed Forces, civilian employee of the Department of Defense, or an individual in a pre-commissioning program no less than once a year;

(B) to a member of the Armed Forces whose discharge (regardless of character of discharge) or release from active duty is anticipated as of a specific date within the time period specified under section 1142(a)(3) of title, United States Code;

(C) to a member of the Armed Forces performing recruitment activities within the 30 days prior to commencing such activities; and

(D) additionally as determined by the Secretary of Defense.

(c) PROGRESS REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and House of Representatives a report on the status of the implementation of this section.

SA 4810. Mrs. GILLIBRAND (for herself, Mr. RUBIO, Mr. HEINRICH, Mr. BLUNT, and Mr. GRAHAM) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place in title XV, insert the following:

SEC. ____. ESTABLISHMENT OF STRUCTURE AND AUTHORITIES TO ADDRESS UNIDENTIFIED AERIAL PHENOMENA.

(a) ESTABLISHMENT OF ANOMALY SURVEILLANCE, TRACKING, AND RESOLUTION OFFICE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall, in coordination with the Director of National Intelligence, establish an office within an appropriate component of the Department of Defense, or within a joint organization of the Department of Defense and the Office of the Director of National Intelligence, to assume—

(A) the duties of the Unidentified Aerial Phenomenon Task Force, as in effect on the day before the date of the enactment of this Act; and

(B) such other duties as are required by this section.

(2) DESIGNATION.—The office established under paragraph (1) shall be known as the ''Anomaly Surveillance, Tracking, and Resolution Office'' (in this section referred to as the ''Office'').

(3) TERMINATION OR SUBORDINATION OF PRIOR TASK FORCE.—Upon the establishment of the Anomaly Surveillance, Tracking, and Resolution Office, the Secretary shall terminate the Unidentified Aerial Phenomenon Task Force or subordinate it to the Office.

(b) FACILITATION OF REPORTING AND DATA SHARING.—The Director and the Secretary shall each, in coordination with each other, require that—

(1) each element of the intelligence community and the Department, with any data that may be relevant to the investigation of unidentified aerial phenomena, make such data available immediately to the Office; and

(2) military and civilian personnel employed by or under contract to the Department or an element of the intelligence community shall have access to procedures by which they shall report incidents or information, including adverse physiological effects, involving or associated with unidentified aerial phenomena directly to the Office.

(c) DUTIES.—The duties of the Office established under subsection (a) shall include the following:

(1) Developing procedures to synchronize and standardize the collection, reporting, and analysis of incidents, including adverse physiological effects, regarding unidentified aerial phenomena across the Department and in consultation with the intelligence community.

(2) Developing processes and procedures to ensure that such incidents from each component of the Department and each element of the intelligence community are reported and incorporated in a centralized repository.

(3) Establishing procedures to require the timely and consistent reporting of such incidents.

(4) Evaluating links between unidentified aerial phenomena and adversarial foreign governments, other foreign governments, or nonstate actors.

(5) Evaluating the threat that such incidents present to the United States.

(6) Consulting with other departments and agencies of the Federal Government, as appropriate, including the Federal Aviation Administration, the National Aeronautics and Space Administration, the Department of Homeland Security, the National Oceanic and Atmospheric Administration, and the Department of Energy.

(7) Consulting with allies and partners of the United States, as appropriate, to better assess the nature and extent of unidentified aerial phenomena.

(8) Preparing reports for Congress, in both classified and unclassified form, as required by subsections (h) and (i).

(d) EMPLOYMENT OF LINE ORGANIZATIONS FOR FIELD INVESTIGATIONS OF UNIDENTIFIED AERIAL PHENOMENA.—

(1) IN GENERAL.—The Secretary shall, in coordination with the Director, designate line organizations within the Department of Defense and the intelligence community that possess appropriate expertise, authorities, accesses, data, systems, platforms, and capabilities to rapidly respond to, and conduct field investigations of, incidents involving unidentified aerial phenomena under the direction of the Office.

(2) PERSONNEL, EQUIPMENT, AND RESOURCES.—The Secretary, in coordination with the Director, shall take such actions as may be necessary to ensure that the designated organization or organizations have available adequate personnel with requisite expertise, equipment, transportation, and other resources necessary to respond rapidly to incidents or patterns of observations of unidentified aerial phenomena of which the Office becomes aware.

(e) UTILIZATION OF LINE ORGANIZATIONS FOR SCIENTIFIC, TECHNOLOGICAL, AND OPERATIONAL ANALYSES OF DATA ON UNIDENTIFIED AERIAL PHENOMENA.—

(1) IN GENERAL.—The Secretary, in coordination with the Director, shall designate one or more line organizations that will be primarily responsible for scientific, technical, and operational analysis of data gathered by field investigations conducted under subsection (d), or data from other sources, including testing of materials, medical studies, and development of theoretical models to better understand and explain unidentified aerial phenomena.

(2) AUTHORITY.—The Secretary and the Director shall promulgate such directives as necessary to ensure that the designated line organizations have authority to draw on special expertise of persons outside the Federal Government with appropriate security clearances.

(f) INTELLIGENCE COLLECTION AND ANALYSIS PLAN.—

(1) IN GENERAL.—The head of the Office shall supervise the development and execution of an intelligence collection and analysis plan on behalf of the Secretary and the Director to gain as much knowledge as possible regarding the technical and operational characteristics, origins, and intentions of unidentified aerial phenomena, including the development, acquisition, deployment, and operation of technical collection capabilities necessary to detect, identify, and scientifically characterize unidentified aerial phenomena.

(2) USE OF RESOURCES AND CAPABILITIES.—In developing the plan required by paragraph (1), the head of the Office shall consider and propose, as appropriate, the use of any resource, capability, asset, or process of the Department and the intelligence community.

(g) SCIENCE PLAN.—The head of the Office shall supervise the development and execution of a science plan on behalf of the Secretary and the Director to develop and test, as practicable, scientific theories to account for characteristics and performance of unidentified aerial phenomena that exceed the known state of the art in science or technology, including in the areas of propulsion, aerodynamic control, signatures, structures, materials, sensors, countermeasures, weapons, electronics, and power generation, and to provide the foundation for potential future investments to replicate any such advanced characteristics and performance.

(h) ASSIGNMENT OF PRIORITY.—The Director, in consultation with, and with the recommendation of the Secretary, shall assign an appropriate level of priority within the National Intelligence Priorities Framework to the requirement to understand, characterize, and respond to unidentified aerial phenomena.

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such sums as may be necessary to carry out the work of the Office, including—

(1) general intelligence gathering and intelligence analysis; and

(2) strategic defense, space defense, defense of controlled air space, defense of ground, air, or naval assets, and related purposes.

(j) ANNUAL REPORT.—

(1) REQUIREMENT.—Not later than October 31, 2022, and annually thereafter until October 31, 2026, the Secretary in consultation with the Director, shall submit to the appropriate committees of Congress a report on unidentified aerial phenomena.

(2) ELEMENTS.—Each report under paragraph (1) shall include, with respect to the year covered by the report, the following information:

(A) An analysis of data and intelligence received through reports of unidentified aerial phenomena.

(B) An analysis of data relating to unidentified aerial phenomena collected through—

(i) geospatial intelligence

(ii) signals intelligence;

(iii) human intelligence; and

(iv) measurement and signals intelligence.

(C) The number of reported incidents of unidentified aerial phenomena over restricted air space of the United States.

(D) An analysis of such incidents identified under subparagraph (C).

(E) Identification of potential aerospace or other threats posed by unidentified aerial phenomena to the national security of the United States.

(F) An assessment of any activity regarding unidentified aerial phenomena that can be attributed to one or more adversarial foreign governments.

(G) Identification of any incidents or patterns regarding unidentified aerial phenomena that indicate a potential adversarial foreign government may have achieved a breakthrough aerospace capability.

(H) An update on the coordination by the United States with allies and partners on efforts to track, understand, and address unidentified aerial phenomena.

(I) An update on any efforts to capture or exploit discovered unidentified aerial phenomena.

(J) An assessment of any health-related effects for individuals who have encountered unidentified aerial phenomena.

(K) The number of reported incidents, and descriptions thereof, of unidentified aerial phenomena associated with military nuclear assets, including strategic nuclear weapons and nuclear-powered ships and submarines.

(L) In consultation with the Administrator of the National Nuclear Security Administration, the number of reported incidents, and descriptions thereof, of unidentified aerial phenomena associated with facilities or assets associated with the production, transportation, or storage of nuclear weapons or components thereof.

(M) In consultation with the Chairman of the Nuclear Regulatory Commission, the number of reported incidents, and descriptions thereof, of unidentified aerial phenomena or drones of unknown origin associated with nuclear power generating stations, nuclear fuel storage sites, or other sites or facilities regulated by the Nuclear Regulatory Commission.

(N) The names of the line organizations that have been designated to perform the specific functions imposed by subsections (d) and (e) of this section, and the specific functions for which each such line organization has been assigned primary responsibility.

(3) FORM.— Each report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(k) SEMIANNUAL BRIEFINGS.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act and not less frequently than semiannually thereafter until December 31, 2026, the head of the Office shall provide the classified briefings on unidentified aerial phenomena to—

(A) the Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(2) FIRST BRIEFING.—The first briefing provided under paragraph (1) shall include all incidents involving unidentified aerial phenomena that were reported to the Unidentified Aerial Phenomena Task Force or to the Office after June 24, 2021, regardless of the date of occurrence of the incident.

(3) SUBSEQUENT BRIEFINGS.—Each briefing provided subsequent to the first briefing described in paragraph (2) shall include, at a minimum, all events relating to unidentified aerial phenomena that occurred during the previous 180 days, and events relating to unidentified aerial phenomena that were not included in an earlier briefing due to delay in an incident reaching the reporting system or other such factors.

(4) INSTANCES IN WHICH DATA WAS NOT SHARED.—For each briefing period, the Chairman and Vice Chairman or Ranking Member of the Committee on Armed Services and the Select Committee on Intelligence of the Senate and the Committee on Armed Services and the Permanent Select Committee on Intelligence of the House of Representatives shall receive an enumeration of any instances in which data related to unidentified aerial phenomena was denied to the Office because of classification restrictions on that data or for any other reason.

(l) AERIAL AND TRANSMEDIUM PHENOMENA ADVISORY COMMITTEE.—

(1) ESTABLISHMENT.—(A) Not later than October 1, 2022, the Secretary and the Director shall establish an advisory committee for the purpose of—

(i) advising the Office in the execution of the duties of the Office as provided by this subsection; and

(ii) advising the Secretary and the Director regarding the gathering and analysis of data, and scientific research and development pertaining to unidentified aerial phenomena.

(B) The advisory committee established under subparagraph (A) shall be known as the ''Aerial and Transmedium Phenomena Advisory Committee'' (in this subparagraph the ''Committee'').

(2) MEMBERSHIP.—(A) Subject to subparagraph (B), the Committee shall be composed of members as follows:

(i) 20 members selected by the Secretary as follows:

(I) Three members selected from among individuals recommended by the Administrator of the National Astronautics and Space Administration.

(II) Two members selected from among individuals recommended by the Administrator of the Federal Aviation Administration.

(III) Two members selected from among individuals recommended by the President of the National Academies of Sciences.

(IV) Two members selected from among individuals recommended by the President of the National Academy of Engineering.

(V) One member selected from among individuals recommended by the President of the National Academy of Medicine.

(VI) Three members selected from among individuals recommended by the Director of the Galileo Project at Harvard University.

(VII) Two members selected from among individuals recommended by the Board of Directors of the Scientific Coalition for Unidentified Aerospace Phenomena Studies.

(VIII) Two members selected from among individuals recommended by the President of the American Institute of Astronautics and Aeronautics.

(IX) Two members selected from among individuals recommended by the Director of the Optical Technology Center at Montana State University.

(X) One member selected from among individuals recommended by the president of the American Society for Photogrammetry and Remote Sensing.

(ii) Up to five additional members, as the Secretary, in consultation with the Director, considers appropriate, selected from among individuals with requisite expertise, at least

3 of whom shall not be employees of any Federal Government agency or Federal Government contractor.

(B) No individual may be appointed to the Committee under subparagraph (A) unless the Secretary and the Directly jointly determine that the individual—

(i) qualifies for a security clearance at the secret level or higher;

(ii) possesses scientific, medical, or technical expertise pertinent to some aspect of the investigation and analysis of unidentified aerial phenomena; and

(iii) has previously conducted research or writing that demonstrates scientific, technological, or operational knowledge regarding aspects of the subject matter, including propulsion, aerodynamic control, signatures, structures, materials, sensors, countermeasures, weapons, electronics, power generation, field investigations, forensic examination of particular cases, analysis of open source and classified information regarding domestic and foreign research and commentary, and historical information pertaining to unidentified aerial phenomena.

(C) The Secretary and Director may terminate the membership of any individual on the Committee upon a finding by the Secretary and the Director jointly that the member no longer meets the criteria specified in this subsection.

(3) CHAIRPERSON.—The Secretary shall, in coordination with the Director, designate a temporary Chairperson of the Committee, but at the earliest practicable date the Committee shall elect a Chairperson from among its members, who will serve a term of 2 years, and is eligible for re-election.

(4) EXPERT ASSISTANCE, ADVICE, AND RECOMMENDATIONS.—(A) The Committee may, upon invitation of the head of the Office, provide expert assistance or advice to any line organization designated to carry out field investigations or data analysis as authorized by subsections (d) and (e).

(B) The Committee, on its own initiative, or at the request of the Director, the Secretary, or the head of the Office, may provide advice and recommendations regarding best practices with respect to the gathering and analysis of data on unidentified aerial phenomena in general, or commentary regarding specific incidents, cases, or classes of unidentified aerial phenomena.

(5) REPORT.—Not later than December 31, 2022, and not later than December 31 of each year thereafter, the Committee shall submit a report summarizing its activities and recommendations to the following:

(A) The Secretary.

(B) The Director.

(C) The head of the Office.

(D) The Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate.

(E) The Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(6) RELATION TO FACA.—For purposes of the Federal Advisory Committee Act (5 U.S.C. App.), the Committee shall be considered an advisory committee (as defined in section 3 of such Act, except as otherwise provided in the section or as jointly deemed warranted by the Secretary and the Director under section 4(b)(3) of such Act.

(7) TERMINATION OF COMMITTEE.—The Committee shall terminate on the date that is six years after the date of the establishment of the Committee.

(m) DEFINITIONS.—In this section:

(1) The term ''appropriate committees of Congress'' means—

(A) the Committee on Armed Services, the Select Committee on Intelligence, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Foreign Affairs, and the Committee on Appropriations of the House of Representatives.

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

(3) The term ''transmedium objects or devices'' means objects or devices that are observed to transition between space and the atmosphere, or between the atmosphere and bodies of water, that are not immediately identifiable.

(4) The term ''unidentified aerial phenomena'' means—

(A) airborne objects that are not immediately identifiable;

(B) transmedium objects or devices; and

(C) submerged objects or devices that are not immediately identifiable and that display behavior or performance characteristics suggesting that they may be related to the subjects described in subparagraph (A) or (B).

SA 4811. Mr. TUBERVILLE (for himself and Mr. BRAUN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. PROHIBITING THE INTERNAL REVENUE SERVICE FROM REQUIRING FINANCIAL INSTITUTIONS TO REPORT ON FINANCIAL TRANSACTIONS OF CUSTOMERS.

(a) IN GENERAL.—Subject to subsection (b), the Internal Revenue Service shall not be permitted to create or implement any new financial account information reporting program that—

(1) was not in effect as of October 1, 2021, and

(2) would require financial institutions to report data on financial accounts in an information return listing balances, transactions, transfers, or inflows or outflows of any kind.

(b) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—Nothing in this section shall preempt, limit, or supersede, or be construed to preempt, limit, or supersede, any provision of, or requirement under, the Bank Secrecy Act or any regulations promulgated under such Act.

(2) DEFINITION.—For purposes of this subsection, the term ''Bank Secrecy Act'' means—

(A) section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b),

(B) chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951 et seq.), and

(C) subchapter II of chapter 53 of title 31, United States Code.

SA 4812. Mr. TUBERVILLE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. PROHIBITING TSP INVESTMENT IN CHINA.

(a) FINDINGS.—Congress finds the following:

(1) The Thrift Savings Fund invests more than $700,000,000,000 on behalf of plan participants. As the guardian of the retirement funds of approximately 6,000,000 Federal civilian and military plan participants, it is critical that sums in the Thrift Savings Fund are not invested in securities linked to the economy of the People's Republic of China.

(2) Companies headquartered in the People's Republic of China have repeatedly committed corporate espionage, violated sanctions imposed by the United States, flouted international property laws, committed theft, and failed to comply with audit and regulatory standards designed to safeguard investors.

(3) The Thrift Savings Plan is known for its low management fees and comprehensive array of investment strategies. The provisions of this section, and the amendments made by this section, will not increase fees imposed on participants of the Thrift Savings Plan.

(4) The November 2017 selection of the MSCI ACWI Index by the Federal Retirement Thrift Investment Board, initially scheduled to be effective in 2020, would violate the terms of subsection (i) of section 8438 of title 5, United States Code, as added by subsection (b)(1) of this section.

(b) PROHIBITION ON ANY TSP FUND INVESTING IN ENTITIES BASED IN THE PEOPLE'S REPUBLIC OF CHINA.—

(1) IN GENERAL.—Section 8438 of title 5, United States Code, is amended by adding at the end the following:

''(i) Notwithstanding any other provision of this section, no fund established or overseen by the Board may include an investment in any security of—

''(1) an entity based in the People's Republic of China; or

''(2) any subsidiary that is owned or operated by an entity described in paragraph (1).''.

(2) DIVESTITURE OF ASSETS.—Not later than 30 days after the date of enactment of this Act, the Federal Retirement Thrift Investment Board established under section 8472(a) of title 5, United States Code, shall—

(A) review whether any sums in the Thrift Savings Fund are invested in violation of subsection (i) of section 8438 of that title, as added by paragraph (1) of this subsection;

(B) if any sums are invested in the manner described in subparagraph (A), divest those sums in a manner that is consistent with the legal and fiduciary duties provided under chapter 84 of that title, or any other applicable provision of law; and

(C) reinvest any sums divested under subparagraph (B) in investments that do not violate subsection (i) of section 8438 of that title, as added by paragraph (1) of this subsection.

(c) PROHIBITION ON INVESTMENT OF TSP FUNDS IN ENTITIES BASED IN THE PEOPLE'S REPUBLIC OF CHINA THROUGH THE TSP MUTUAL FUND WINDOW.—Section 8438(b)(5) of title 5, United States Code, is amended by adding at the end the following:

''(E) A mutual fund accessible through a mutual fund window authorized under this

paragraph may not include an investment in any security of—

''(i) an entity based in the People's Republic of China; or

''(ii) any subsidiary that is owned or operated by an entity described in clause (i).''.

SA 4813. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end, add the following:

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

TITLE LI—CYBER INCIDENT REPORTING ACT OF 2021

SEC. 5101. SHORT TITLE.

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

SEC. 5102. 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 5103 of this title.

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

(3) INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 5203 of this division.

SEC. 5103. 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 5203(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 or subcontract at any tier, grant, cooperative agreement, or other transaction agreement, unless that entity 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 section 2232(a) and 2233 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 briefings required under subsection (c);

''(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 National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—

''(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.—A covered entity, except for an individual or a small organization, that makes a ransom payment as the result of a ransomware attack against the covered 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 covered 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 a covered 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, the Department of Justice, and 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 is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

''(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 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 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 that is a Federal contractor 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.

''(5) AUTHENTICATION.—

''(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

''(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

''(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

''(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate Federal regulatory agency 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 Federal regulatory agency 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); or

''(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

''(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b); or

''(2) issued a subpoena pursuant to subsection (c).

''(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

''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 or 2233 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 cyber incident reported pursuant to section 2232 or 2233 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 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. 5104. FEDERAL SHARING OF INCIDENT REPORTS.

(a) CYBER INCIDENT REPORTING SHARING.—

(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5, United States Code), 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. The Director shall share and coordinate each report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 5103 of this title.

(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 title or the amendments made by this title.

(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, the Attorney General, 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 Attorney General, 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, the Attorney General, 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. 5105. 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. 5106. 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. 5107. 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 5103(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 5103(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 5105, 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 5105(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 TITLE.—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 title and the amendments made by this title.

(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 5103 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 5103 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 title, 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 5103 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 5103 of this title.

TITLE LII—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 5201. SHORT TITLE.

This title may be cited as the ''CISA Technical Corrections and Improvements Act of 2021''.

SEC. 5202. 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 paragraph (11), by striking ''and'' at the end;

(2) in the first paragraph (12)—

(A) by striking ''section 2215'' and inserting ''section 2217''; and

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

(3) 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. 5203. 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 use or threat of use of unauthorized or malicious code on an information system, or the use or 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 CONTROL.—The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

''(25) 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.

''(26) SHARING.—The term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

''(27) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber incident within the supply chain of an information system that an adversary can leverage to jeopardize 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.

''(28) 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.

''(29) 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)—

(i) in subparagraph (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))''; and

(ii) in subparagraph (B)(ii), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(D) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)''; and

(ii) in paragraph (1)(E)(ii)(II), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(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) in subsection (d)(2), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(B) 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.'';

(11) in section 2218(c)(4)(A), as so redesignated, by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; 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 item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''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 paragraphs (16) and (17) and inserting the following:

''(16) SECURITY CONTROL.—The term 'security control' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(17) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''.

SEC. 5204. 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(b) (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 (6 U.S.C. 1524)—

(A) in subsection (a)—

(i) in paragraph (1), by striking ''section 2213'' and inserting ''section 2200'';

(ii) in paragraph (2), by striking ''section 102'' and inserting ''section 2200 of the Homeland Security Act of 2002'';

(iii) in paragraph (4), by striking ''section 2210(b)(1)'' and inserting ''section 2210(a)(1)''; and

(iv) 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(b) of the Homeland Security Act of 2002 (6 U.S.C. 660(b))''.

(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)'' and inserting ''section 2200''; 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 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)''.

(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) of the Homeland Security Act of 2002 (6 U.S.C. 659(m))'' and inserting ''section 2209(l) of the Homeland Security Act of 2002 (6 U.S.C. 659(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''.

SA 4814. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. EXTENSION OF AVAILABILITY OF CORONAVIRUS RELIEF FUND PAYMENTS TO TRIBAL GOVERNMENTS.

Section 601(d)(3) of the Social Security Act (42 U.S.C. 801(d)(3)) is amended by inserting ''(or, in the case of costs incurred by a Tribal government, during the period that begins on March 1, 2020, and ends on December 31, 2022)'' before the period.

SA 4815. Mr. SANDERS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. 1064. REQUIREMENT OF DENTAL CLINIC OF DEPARTMENT OF VETERANS AFFAIRS IN EACH STATE.

The Secretary of Veterans Affairs shall ensure that each State has a dental clinic of the Department of Veterans Affairs to service the needs of the veterans within that State by not later than September 30, 2024.

SA 4816. Mr. COONS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

Subtitle ____—Sudan Democracy Act

SEC. ___1. SHORT TITLE.

This subtitle may be cited as the ''Sudan Democracy Act''.

SEC. ___2. DEFINITIONS.

In this subtitle:

(1) ADMITTED; ALIEN.—The terms ''admitted'' and ''alien'' have the meanings given such terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1001).

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

(A) the Committee on Foreign Relations of the Senate;

(B) the Committee on Appropriations of the Senate;

(C) the Committee on Foreign Affairs of the House of Representatives; and

(D) the Committee on Appropriations of the House of Representatives.

(3) FOREIGN PERSON.—The term ''foreign person'' means a person that is not a United States person.

(4) GROSS VIOLATIONS OF INTERNATIONALLY RECOGNIZED HUMAN RIGHTS.—The term ''gross violations of internationally recognized human rights'' has the meaning given such term in section 502B(d)(1) of the Foreign Assistance Act of 1961 (22 U.S.C. 2304(d)(1)).

(5) INTERNATIONAL FINANCIAL INSTITUTIONS.—The term ''international financial institutions'' means—

(A) the International Monetary Fund;

(B) the International Bank for Reconstruction and Development;

(C) the International Development Association;

(D) the International Finance Corporation;

(E) the Inter-American Development Bank;

(F) the Asian Development Bank;

(G) the Inter-American Investment Corporation;

(H) the African Development Bank;

(I) the African Development Fund;

(J) the European Bank for Reconstruction and Development; and

(K) the Multilateral Investment Guaranty Agency.

(6) KNOWINGLY.—The term ''knowingly'' means, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.

(7) SECURITY AND INTELLIGENCE SERVICES.—The term ''security and intelligence servvices'' means—

(A) the Sudan Armed Forces;

(B) the Rapid Support Forces;

(C) the Popular Defense Forces;

(D) other Sudanese paramilitary units;

(E) Sudanese police forces; and

(F) the General Intelligence Service (previously known as the National Intelligence and Security Services).

(8) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen, an alien lawfully admitted for permanent residence to the United States, or any other individual subject to the jurisdiction of the United States; or

(B) an entity organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such entity.

SEC. ___3. FINDINGS; STATEMENT OF POLICY.

(a) FINDINGS.—Congress makes the following findings:

(1) On November 17, 1958, Lieutenant General Ibrahim Abboud of Sudan led the country's first coup after independence, and the first successful coup in post-independence Africa.

(2) There have been more than 200 coup attempts across Africa since the 1958 coup in Sudan, including successful coups in Sudan in 1969, 1985, 1989, and 2019.

(3) On April 11, 2019, President Omar al Bashir of Sudan, who came to power in a military coup in 1989, was overthrown after months of popular protests by his own security chiefs, who established a Transitional Military Council, led by Lieutenant General Abdel Fattah al-Burhan, that ignored calls from the Sudanese people to transfer power to civilians.

(4) On August 17, 2019—

(A) the Transitional Military Council, under domestic and international pressure, signed a power-sharing agreement with the Forces for Freedom and Change, a broad coalition of political parties and civic groups representing the protest movement that had pushed for the end of the Bashir regime and a transition to civilian rule; and

(B) a transitional government was formed that allowed the junta leaders to remain in government in a partnership with new civilian authorities nominated by the Forces for Freedom and Change, including Prime Minister Abdallah Hamdok, for a transitional period to democracy.

(5) On October 25, 2021, Lieutenant General Burhan, with the support of Lieutenant Mohamed Hamdan Dagalo (also known as ''Hemedti'')—

(A) seized control of the Government of Sudan;

(B) deployed the military to the streets of Khartoum and Omdurman;

(C) shut down the internet in Sudan; and

(D) detained Prime Minister Hamdok and other civilian officials.

(6) The African Union Peace and Security Council has condemned the military takeover, rejected the unconstitutional change of

government, and on October 27, 2021, suspended Sudan from the Council until the civilian-led transitional government is restored.

(7) The Troika (the United States, United Kingdom, Norway), the European Union, and Switzerland ''continue to recognize the Prime Minister and his cabinet as the constitutional leaders of the transitional government''.

(8) The Sudanese people have condemned the military takeover and launched a campaign of peaceful civil disobedience, continuing the protests for democracy that began in late 2018 and reflecting a historic tradition of non-violence protests led by previous generations in Sudan against military regimes in 1964 and 1985.

(9) In response to public calls for civilian rule since October 25, 2021, Sudanese security forces have arbitrarily detained civilians and used excessive and lethal force against peaceful protesters that has resulted in civilian deaths across the country.

(10) The October 25, 2021 military takeover represents a threat to—

(A) Sudan's economic recovery and stability;

(B) the bilateral relationship between Sudan and the United States; and

(C) regional peace and security.

(b) STATEMENT OF POLICY.—It is the policy of the United States—

(1) to support the democratic aspirations of the people of Sudan and a political transition process that results in a civilian government that is democratic, accountable, respects the human rights of its citizens, and is at peace with itself and with its neighbors;

(2) to encourage the reform of the security sector of Sudan to one that is protects citizens under a democracy and respects civilian authority; and

(3) to deter military coups and efforts by external parties to support them.

SEC. ___4. IMPOSITION OF SANCTIONS.

(a) IN GENERAL.—The President shall impose the sanctions described in subsection (b) with respect to any person or entity that the President determines, on or after the date of enactment of this Act—

(1) is responsible for, complicit in, or directly or indirectly engaged or attempted to engage in—

(A) actions that undermine the transition to democracy in Sudan, or, after elections, undermine democratic processes or institutions;

(B) actions that threaten the peace, security, or stability of Sudan;

(C) actions that prohibit, limit, or penalize the exercise of freedom of expression or assembly by people in Sudan, or limit access to print, online, or broadcast media in Sudan;

(D) the arbitrary detention or torture of any person in Sudan or other gross violations of internationally recognized human rights in Sudan;

(E) significant efforts to impede investigations or prosecutions of alleged serious human rights abuses in Sudan;

(F) actions that result in the misappropriation of significant state assets of Sudan or manipulation of the currency, or that hinder government oversight of parastatal budgets and revenues;

(G) actions that violate medical neutrality, including blocking access to care and targeting first responders, medical personnel, or medical institutions; or

(H) disrupting access to communication technologies and information on the internet;

(2) is an entity owned or controlled by any person or entity described in paragraph (1);

(3) forms an entity for the purpose of evading sanctions that would otherwise be imposed pursuant to subsection (b);

(4) is acting for, or on behalf of, a person or entity referred to in paragraph (1), (2), or (3);

(5) is an entity that is owned or controlled (directly or indirectly) by security and intelligence services, from which 1 or more persons or entities described in paragraph (1) derive significant revenue or financial benefit; or

(6) has knowingly—

(A) provided significant financial, material, or technological support—

(i) to a foreign person or entity described in paragraph (1) in furtherance of any of the acts described in subparagraph (A) or (B) of such paragraph; or

(ii) to any entity owned or controlled by such person or entity or an immediate family member of such person; or

(B) received significant financial, material, or technological support from a foreign person or entity described in paragraph (1) or an entity owned or controlled by such person or entity or an immediate family member of such person.

(b) SANCTIONS; EXCEPTIONS.—

(1) SANCTIONS.—

(A) ASSET BLOCKING.—Notwithstanding section 202 of the International Emergency Economic Powers Act (50 U.S.C. 1701), the exercise of all powers granted to the President by such Act to the extent necessary to block and prohibit all transactions in all property and interests in property of a foreign person the President determines meets 1 or more of the criteria described in subsection (a) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(B) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(i) VISAS, ADMISSION, OR PAROLE.—An alien who the Secretary of State or the Secretary of Homeland Security (or a designee of one of such Secretaries) knows, or has reason to believe, meets any of the criteria described in subsection (a)—

(I) is inadmissible to the United States;

(II) is ineligible to receive a visa or other documentation to enter the United States; and

(III) is otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(ii) CURRENT VISAS REVOKED.—

(I) IN GENERAL.—The issuing consular officer, the Secretary of State, or a designee of the Secretary of State, in accordance with section 221(i) of the Immigration and Nationality Act (8 U.S.C. 1201(i)), shall revoke any visa or other entry documentation issued to an alien described in clause (i) regardless of when the visa or other entry documentation was issued.

(II) EFFECT OF REVOCATION.—A revocation under subclause (I) shall take effect immediately and shall automatically cancel any other valid visa or entry documentation that is in the alien's possession.

(2) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under paragraph (1)(B) shall not apply with respect to an alien if admitting or paroling the alien into the United States is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations.

(3) PENALTIES.—Any person that violates, attempts to violate, conspires to violate, or causes a violation of this section or any regulation, license, or order issued to carry out subsection (b) shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of such section.

(4) IMPLEMENTATION.—The President—

(A) may exercise all authorities provided under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this section; and

(B) shall issue such regulations, licenses, and orders as may be necessary to carry out this section.

(5) EXCEPTION TO COMPLY WITH NATIONAL SECURITY.—Activities subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) and any authorized intelligence or law enforcement activities of the United States shall be exempt from sanctions under this section.

(c) WAIVER.—The President may annually waive the application of sanctions imposed on a foreign person pursuant to subsection (a) if the President—

(1) determines that such waiver with respect to such foreign person is in the national interest of the United States; and

(2) not later than the date on which such waiver will take effect, submits notice of, and justification for, such waiver to—

(A) the appropriate congressional committees;

(B) the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(C) the Committee on Financial Services of the House of Representatives.

(d) SUNSET.—The requirement to impose sanctions under this section shall cease to be effective on December 31, 2026.

SA 4817. Ms. SINEMA submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. LAND TAKEN INTO TRUST FOR BENEFIT OF THE GILA RIVER INDIAN COMMUNITY.

(a) DEFINITIONS.—In this section:

(1) BLACKWATER TRADING POST LAND.—The term ''Blackwater Trading Post Land'' means the approximately 55.3 acres of land as depicted on the map that—

(A) is located in Pinal County, Arizona, and bordered by Community land to the east, west, and north and State Highway 87 to the south; and

(B) is owned by the Community.

(2) COMMUNITY.—The term ''Community'' means the Gila River Indian Community of the Reservation.

(3) MAP.—The term ''map'' means the map entitled ''Results of Survey, Ellis Property, A Portion of the West ½ of Section 12, Township 5 South, Range 7 East, Gila and Salt River Meridian, Pinal County, Arizona'' and dated October 15, 2012.

(4) RESERVATION.—The term ''Reservation'' means the land located within the exterior boundaries of the reservation created under sections 3 and 4 of the Act of February 28, 1859 (11 Stat. 401, chapter LXVI), and Executive orders of August 31, 1876, June 14, 1879,

May 5, 1882, November 15, 1883, July 31, 1911, June 2, 1913, August 27, 1914, and July 19, 1915, and any other lands placed in trust for the benefit of the Community.

(5) SECRETARY.—The term ''Secretary'' means the Secretary of the Interior.

(b) LAND TAKEN INTO TRUST FOR BENEFIT OF THE GILA RIVER INDIAN COMMUNITY.—

(1) IN GENERAL.—The Secretary shall take the Blackwater Trading Post Land into trust for the benefit of the Community, after the Community—

(A) conveys to the Secretary all right, title, and interest of the Community in and to the Blackwater Trading Post Land;

(B) submits to the Secretary a request to take the Blackwater Trading Post Land into trust for the benefit of the Community;

(C) conducts a survey (to the satisfaction of the Secretary) to determine the exact acreage and legal description of the Blackwater Trading Post Land, if the Secretary determines a survey is necessary; and

(D) pays all costs of any survey conducted under subparagraph (C).

(2) AVAILABILITY OF MAP.—Not later than 180 days after the Blackwater Trading Post Land is taken into trust under paragraph (1), the map shall be on file and available for public inspection in the appropriate offices of the Secretary.

(3) LANDS TAKEN INTO TRUST PART OF RESERVATION.—After the date on which the Blackwater Trading Post Land is taken into trust under paragraph (1), the land shall be treated as part of the Reservation.

(4) GAMING.—Class II and class III gaming under the Indian Gaming Regulatory Act (25 U.S.C. 2701 et seq.) shall not be allowed at any time on the land taken into trust under paragraph (1).

(5) DESCRIPTION.—Not later than 180 days after the date of enactment of this Act, the Secretary shall cause the full metes-and-bounds description of the Blackwater Trading Post Land to be published in the Federal Register. The description shall, on publication, constitute the official description of the Blackwater Trading Post Land.

SA 4818. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of title XII, add the following:

Subtitle H—Long Wars Commission Act of 2021

SEC. 1291. SHORT TITLE.

This subtitle may be cited as the ''Long Wars Commission Act of 2021''.

SEC. 1292. ESTABLISHMENT OF COMMISSION.

(a) ESTABLISHMENT.—There is established the Long Wars Commission (in this subtitle referred to as the ''Commission'').

(b) MEMBERSHIP.—

(1) IN GENERAL.—The Commission shall be composed of 12 members appointed as follows:

(A) One member appointed by the chair of the Committee on Armed Services of the Senate.

(B) One member appointed by the ranking minority member of the Committee on Armed Services of the Senate.

(C) One member appointed by the chair of the Committee on Foreign Relations of the Senate.

(D) One member appointed by the ranking minority member of the Committee on Foreign Relations of the Senate.

(E) One member appointed by the chair of the Committee on Armed Services of the House of Representatives.

(F) One member appointed by the ranking minority member of the Committee on Armed Services of the House of Representatives.

(G) One member appointed by the chair of the Committee on Foreign Affairs of the House of Representatives.

(H) One member appointed by the ranking minority member of the Committee on Foreign Affairs of the House of Representatives.

(I) One member appointed by the chair of the Senate Select Committee on Intelligence.

(J) One member appointed by the ranking minority member of the Senate Select Committee on Intelligence.

(K) One member appointed by the chair of the House Permanent Select Committee on Intelligence.

(L) One member appointed by the ranking minority member of the House Permanent Select Committee on Intelligence.

(2) DATE.—The appointments of the members of the Commission shall be made not later than 90 days after the date of enactment of this Act.

(3) PROHIBITIONS.—A member of the Commission appointed under subparagraph (A) may not—

(A) be a current member of Congress, or a former member of Congress, who served in Congress after January 3, 2001;

(B) have served in military or civilian positions having significant operational or strategic decisionmaking responsibilities for conducting United States Government actions in Afghanistan during the applicable period; or

(C) have been a party to any United States or coalition defense contract during the applicable period.

(c) PERIOD OF APPOINTMENT; VACANCIES.—Members shall be appointed for the life of the Commission. Any vacancy in the Commission shall be filled in the same manner as the original appointment.

(d) MEETINGS.—

(1) INITIAL MEETING.—Not later than 30 days after the date on which all members of the Commission have been appointed, the Commission shall hold the first meeting of the Commission.

(2) FREQUENCY.—The Commission shall meet at the call of the co-chairs.

(3) QUORUM.—A majority of the members of the Commission shall constitute a quorum, but a lesser number of members may hold hearings.

(e) CO-CHAIRS.—

(1) DESIGNATION BY COMMITTEE CHAIRS.—The chair of the Committee on Armed Services of the Senate, the chair of the Committee on Foreign Relations of the Senate, the chair of the Committee on Armed Services of the House of Representatives, the chair of the Committee on Foreign Affairs of the House of Representatives, the chair of the Senate Select Committee on Intelligence, and the chair of the House Permanent Select Committee on Intelligence shall jointly designate one member of the Commission to serve as co-chair of the Commission.

(2) DESIGNATION BY RANKING MINORITY MEMBERS.—The ranking minority member of the Committee on Armed Services of the Senate, the ranking minority member of the Committee on Foreign Relations of the Senate, the ranking minority member of the Committee Armed Services of the House of Representatives, and the ranking minority member of the Committee on Foreign Affairs of the House of Representatives, the ranking minority member of the Senate Select Committee on Intelligence, and the ranking minority member of the House Permanent Select Committee on Intelligence shall jointly designate one member of the Commission to serve as co-chair of the Commission.

SEC. 1293. DUTIES.

(a) REVIEW.—The Commission shall review United States involvement in the conflicts in Afghanistan and Iraq beginning during the period prior to the September 11, 2001, attacks and ending on September 1, 2022, including military engagement, diplomatic engagement, training and advising of local forces, reconstruction efforts, foreign assistance, congressional oversight, and withdrawal in such conflicts.

(b) ASSESSMENT AND RECOMMENDATIONS.—The Commission shall—

(1) conduct a comprehensive assessment of United States involvement in the conflicts in Afghanistan and Iraq, including—

(A) United States military, diplomatic, and political objectives in the conflicts, and the extent to which those objectives were achievable;

(B) an evaluation of the interagency decisionmaking processes during the campaigns;

(C) an evaluation of the United States military's conduct during the campaigns and the extent to which its operational approach compromised campaign progress;

(D) any regional and geopolitical threats to the United States resulting from the conflicts;

(E) the extent to which initial United States national objectives for the conflicts were met;

(F) long-term impact on United States relations with allied nations who participated in the Iraq and Afghanistan conflicts;

(G) the effectiveness of counterterrorism, counterinsurgency, and security force assistance strategies employed by the United States military;

(H) the effect of United States involvement in the conflicts on the readiness of the United States Armed Forces;

(I) the effect of United States involvement in the conflicts on civil-military relations in the United States;

(J) the implications of the use of funds for overseas contingency operations as a mechanism for funding United States involvement in the conflicts; and

(K) any other matters in connection with United States involvement in the conflicts the Commission considers appropriate;

(2) identify circumstances in which a conflict presents a significant likelihood of developing into an irregular or civil war; and

(3) develop recommendations based on the assessment, as well as any other information the Commission considers appropriate, for relevant questions to be asked during future deliberations by Congress of an authorization for use of military force in conflicts that have the potential to develop into an irregular or civil war.

(c) REPORT.—

(1) FINAL REPORT.—Not later than 2 years after the date of the enactment of this Act, the Commission shall submit to the President, the Secretary of Defense, the Committee on Armed Services of the Senate, the Committee on Armed Services of the House of Representatives, the Committee on Foreign Relations of the Senate, the Committee on Foreign Affairs of the House of Representatives, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence a report on the findings, conclusions, and recommendations of the Commission under this section. The report shall do each of the following:

(A) Provide an assessment of the current security, political, humanitarian, and economic situation in Afghanistan and Iraq.

(B) Provide lessons learned from United States involvement in, and withdrawal from, the conflicts in Afghanistan and Iraq.

(C) Provide recommendations on questions to be asked during future deliberations by Congress of an authorization for use of military force in a conflict that has the potential to develop into an irregular war.

(D) Address any other matters with respect to United States involvement in the conflicts in Afghanistan and Iraq that the Commission considers appropriate.

(E) Provide recommendations about United States instruments of power, including the use of military force and nation-building, in future foreign policy engagements.

(F) Provide recommendations about the need to foster any new alliances necessary to future foreign policy engagements.

(2) INTERIM BRIEFING.—Not later than one year after the date of the enactment of this Act, the Commission shall provide to the committees of Congress and the officials referred to in paragraph (1) a briefing on the status of its review and assessment under subsection (b), together with a discussion of any interim recommendations developed by the Commission as of the date of the briefing.

(3) FORM OF REPORT.—The report submitted to Congress under paragraph (1) shall be submitted in unclassified form. The report shall also include a classified annex.

SEC. 1294. POWERS OF COMMISSION.

(a) HEARINGS.—The Commission may hold such hearings, sit and act at such times and places, take such testimony, and receive such evidence as the Commission considers advisable to carry out this subtitle.

(b) ASSISTANCE FROM FEDERAL AGENCIES.—

(1) INFORMATION.—

(A) IN GENERAL.—The Commission may secure directly from a Federal department or agency such information as the Commission considers necessary to carry out this subtitle.

(B) FURNISHING INFORMATION.—On request of the co-chairs of the Commission, the head of the department or agency shall expeditiously furnish the information to the Commission.

(2) GENERAL SERVICES.—Upon the request of the Commission, the Administrator of General Services shall provide to the Commission, on a reimbursable basis, the administrative support services and office space necessary for the Commission to carry out its purposes and functions under this subtitle.

(c) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as other departments and agencies of the Federal Government.

(d) GIFTS.—The Commission may accept, use, and dispose of gifts or donations of services or property.

(e) COOPERATION FROM UNITED STATES GOVERNMENT.—

(1) IN GENERAL.—The Commission shall receive the full and timely cooperation of the Secretary of Defense, the Secretary of State, and the Director of National Intelligence in providing the Commission with analyses, briefings, and other information necessary for the discharge of the duties of the Commission.

(2) LIAISON.—The Secretary of Defense, the Secretary of State, and the Director of National Intelligence shall each designate at least one officer or employee of their respective organizations to serve as a liaison officer to the Commission.

SEC. 1295. COMMISSION PERSONNEL MATTERS.

(a) COMPENSATION OF MEMBERS.—A member of the Commission who is not an officer or employee of the Federal Government shall be compensated at a rate equal to the daily equivalent of the annual rate of basic pay prescribed for level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day (including travel time) during which the member is engaged in the performance of the duties of the Commission.

(b) TRAVEL EXPENSES.—A member of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Commission.

(c) STAFF.—

(1) IN GENERAL.—The co-chairs of the Commission, may, without regard to the civil service laws (including regulations), appoint and terminate an executive director and such other additional personnel as may be necessary to enable the Commission to perform its duties, except that the employment of an executive director shall be subject to confirmation by the Commission.

(2) QUALIFICATIONS FOR PERSONNEL.—The co-chairs of the Commission shall give preference in such appointments to individuals with significant professional experience in national security, such as a position in the Department of Defense, the Department of State, the intelligence community, the United States Agency for International Development, or an academic or scholarly institution.

(3) COMPENSATION.—The co-chairs may fix the compensation of the executive director and other personnel without regard to chapter 51 and subchapter III of chapter 53 of title 5, United States Code, relating to classification of positions and General Schedule pay rates, except that the rate of pay for the executive director and other personnel may not exceed the rate payable for level V of the Executive Schedule under section 5316 of that title.

(d) DETAIL OF GOVERNMENT EMPLOYEES.—A Federal Government employee may be detailed to the Commission without reimbursement, and such detail shall be without interruption or loss of civil service status or privilege.

(e) PROCUREMENT OF TEMPORARY AND INTERMITTENT SERVICES.—The co-chairs of the Commission, may procure temporary and intermittent services under section 3109(b) of title 5, United States Code, at rates for individuals that do not exceed the daily equivalent of the annual rate of 3 basic pay prescribed for level V of the Executive Schedule under section 5316 of that title.

SEC. 1296. TERMINATION OF COMMISSION.

The Commission shall terminate 90 days after the date on which the Commission submits the report required under section 1293(c).

SEC. 1297. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—There is authorized to be appropriated to the Commission such amounts as necessary to carry out activities under this subtitle.

(b) AVAILABILITY.—Any sums appropriated under the authorization contained in this section shall remain available, without fiscal year limitation, until the date of the termination of the Commission under section 1296.

SA 4819. Mr. SULLIVAN (for himself and Mr. WHITEHOUSE) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. 1054. REPORT ON EFFORTS OF COMBATANT COMMANDS TO COMBAT THREATS POSED BY ILLEGAL, UNREPORTED, AND UNREGULATED FISHING.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the chair and deputy chairs of the Interagency Working Group on IUU Fishing and the heads of other relevant agencies, as determined by the Secretary, shall submit to the appropriate committees of Congress a report on the maritime domain awareness efforts of the combatant commands to combat the threats posed by illegal, unreported, and unregulated fishing.

(b) ELEMENTS.—The report required by subsection (a) shall include a detailed summary of each of the following for each combatant command:

(1) Activities undertaken as of the date on which the report is submitted to combat the threats posed by illegal, unreported, and unregulated fishing in the geographic area of the combatant command, including the steps taken to build the capacity of partners to combat those threats.

(2) Coordination among the United States Armed Forces, partner countries, and public-private partnerships to combat the threats described in paragraph (1).

(3) Efforts undertaken to support unclassified data integration, analysis, and delivery with regional partners to combat the threats described in paragraph (1).

(4) Information sharing and coordination with efforts of the Interagency Working Group on IUU Fishing.

(5) Best practices and lessons learned from ongoing and previous efforts relating to the threats described in paragraph (1), including strategies for coordination and successes in public-private partnerships.

(6) Limitations related to affordability, resource constraints, or other gaps or factors that constrain the success or expansion of efforts related to the threats described in paragraph (1).

(7) Any new authorities needed to support efforts to combat the threats described in paragraph (1).

(c) FORM.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Committee on Natural Resources, the Committee on Transportation and Infrastructure, the Committee on Foreign Affairs, and the Committee on Appropriations of the House of Representatives.

(2) INTERAGENCY WORKING GROUP ON IUU FISHING.—The term ''Interagency Working Group on IUU Fishing'' means the working group established by section 3551 of the Maritime Security and Fisheries Enforcement Act (16 U.S.C. 8031).

SA 4820. Mr. COTTON (for himself, Mr. MANCHIN, Mr. TUBERVILLE, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of title XIV, add the following:

Subtitle D—Extraction and Processing of Critical Minerals in the United States

SEC. 1431. SHORT TITLE.

This subtitle may be cited as the ''Restoring Essential Energy and Security Holdings Onshore for Rare Earths and Critical Minerals Act of 2021'' or the ''REEShore Critical Minerals Act of 2021''.

SEC. 1432. DEFINITIONS.

In this subtitle:

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

(A) the Committee on Armed Services, the Committee on Foreign Relations, the Committee on Energy and Natural Resources, the Committee on Commerce, Science, and Transportation, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Armed Services, the Committee on Foreign Affairs, the Committee on Natural Resources, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) CRITICAL MINERAL.—The term ''critical mineral'' has the meaning given that term in section 7002(a) of the Energy Act of 2020 (division Z of Public Law 116–260; 30 U.S.C. 1606(a)).

(3) DEFENSE MINERAL PRODUCT.—The term ''defense mineral product'' means any product—

(A) formed or comprised of, or manufactured from, one or more critical minerals; and

(B) used in critical military defense technologies or other related applications of the Department of Defense.

(4) PROCESSED OR REFINED.—The term ''processed or refined'' means any process by which a defense mineral is extracted, separated, or otherwise manipulated to render the mineral usable for manufacturing a defense mineral product.

SEC. 1433. REPORT ON STRATEGIC CRITICAL MINERAL AND DEFENSE MINERAL PRODUCTS RESERVE.

(a) FINDINGS.—Congress finds that the storage of substantial quantities of critical minerals and defense mineral products will—

(1) diminish the vulnerability of the United States to the effects of a severe supply chain interruption; and

(2) provide limited protection from the short-term consequences of an interruption in supplies of defense mineral products.

(b) SENSE OF CONGRESS.—It is the sense of Congress that, in procuring critical minerals and defense mineral products, the Secretary of Defense should prioritize procurement of critical minerals and defense mineral products from sources in the United States, including that are mined, produced, separated, and manufactured within the United States.

(c) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of the Interior, acting through the United States Geologic Survey, and the Secretary of Defense, in consultation with the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, the Secretary of Commerce, and the Director of National Intelligence, shall jointly submit to the appropriate congressional committees a report—

(A) describing the existing authorities and funding levels of the Federal Government to stockpile critical minerals and defense mineral products;

(B) assessing whether those authorities and funding levels are sufficient to meet the requirements of the United States; and

(C) including recommendations to diminish the vulnerability of the United States to disruptions in the supply chains for critical minerals and defense mineral products through changes to policy, procurement regulation, or existing law, including any additional statutory authorities that may be needed.

(2) CONSIDERATIONS.—In developing the report required by paragraph (1), the Secretary of the Interior, the Secretary of Defense, the Secretary of Commerce, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the Director of National Intelligence shall take into consideration the needs of the Armed Forces of the United States, the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))), the defense industrial and technology sectors, and any places, organizations, physical infrastructure, or digital infrastructure designated as critical to the national security of the United States.

SEC. 1434. REPORT ON DISCLOSURES CONCERNING CRITICAL MINERALS BY CONTRACTORS OF DEPARTMENT OF DEFENSE.

(a) REPORT REQUIRED.—Not later than December 31, 2022, the Secretary of Defense, after consultation with the Secretary of Commerce, the Secretary of State, and the Secretary of the Interior, shall submit to the appropriate congressional committees a report that includes—

(1) a review of the existing disclosure requirements with respect to the provenance of magnets used within defense mineral products;

(2) a review of the feasibility of imposing a requirement that any contractor of the Department of Defense provide a disclosure with respect to any system with a defense mineral product that is a permanent magnet, including an identification of the country or countries in which—

(A) the critical minerals used in the magnet were mined;

(B) the critical minerals were refined into oxides;

(C) the critical minerals were made into metals and alloys; and

(D) the magnet was sintered or bonded and magnetized; and

(3) recommendations to Congress for implementing such a requirement, including methods to ensure that any tracking or provenance system is independently verifiable.

SEC. 1435. REPORT ON PROHIBITION ON ACQUISITION OF DEFENSE MATERIALS FROM NON-ALLIED FOREIGN NATIONS.

The Secretary of Defense shall study and submit to the appropriate congressional committees a report on the potential impacts of imposing a restriction that, for any contract entered into or renewed on or after December 31, 2026, for the procurement of a system the export of which is restricted or controlled under the Arms Export Control Act (22 U.S.C. 2751 et seq.), no critical minerals processed or refined in the People's Republic of China may be included in the system.

SEC. 1436. PRODUCTION IN AND USES OF CRITICAL MINERALS BY UNITED STATES ALLIES.

(a) POLICY.—It shall be the policy of the United States to encourage countries that are allies of the United States to identify alternatives, to the maximum extent practicable, to the use of critical minerals from foreign entities of concern.

(b) REPORT REQUIRED.—Not later than December 31, 2022, and annually thereafter, the Secretary of Defense, in coordination with the Secretary of State, shall submit to the appropriate congressional committees a report—

(1) describing the discussions of such Secretaries with countries that are allies of the United States concerning supply chain security for critical minerals;

(2) assessing the likelihood of those countries identifying alternatives, to the maximum extent practicable, to the use of critical minerals from foreign entities of concern or countries that such Secretaries deem to be of concern; and

(3) assessing initiatives in other countries to increase critical mineral mining and production capabilities.

(c) FOREIGN ENTITY OF CONCERN DEFINED.—In this section, the term ''foreign entity of concern'' has the meaning given that term in section 9901(6) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (15 U.S.C. 4651(6)).

SA 4821. Mr. BROWN (for himself and Mr. WARNER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place in title II, insert the following:

SEC. _____. MINORITY INSTITUTE FOR DEFENSE RESEARCH.

(a) PLAN TO PROMOTE DEFENSE RESEARCH AT MINORITY INSTITUTIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this section, the Secretary of Defense shall submit to the congressional defense committees a plan (in this section referred to as the ''Plan'')—

(A) to promote defense research activities at minority institutions to elevate the defense research capacity of minority institutions; and

(B) for the establishment of the Minority Institute for Defense Research (in this section referred to as the ''Consortium'').

(2) ELEMENTS.—The Plan shall include the following:

(A) An assessment relating to the engineering, research, and development capability, including the workforce, administrative support, and physical research infrastructure, of minority institutions and their ability to participate in defense research and engineering activities and effectively compete for defense research contracts.

(B) An assessment of the activities and investments necessary to elevate minority institutions or a consortium of minority institutions, including historically Black colleges and universities, to the level of R1 research institutions and increase their participation

in, and ability to effectively compete for, defense research and engineering activities.

(C) Recommendations relating to actions that may be taken by the Department of Defense, Congress, and minority institutions to establish the Consortium within 3 years.

(D) The specific goals, incentives, and metrics developed by the Secretary in subsection (c) to increase and measure the capacity of minority institutions to address the research and development needs of the Department.

(3) CONSULTATION.—In developing the plan under paragraph (1), the Secretary shall consult with such other public and private sector organizations as the Secretary considers appropriate.

(4) PUBLICLY AVAILABLE.—The Secretary shall post the Plan on a publicly available website of the Department.

(5) MINORITY INSTITUTION DEFINED.—In this subsection, the term ''minority institution'' means—

(A) a part B institution (as such term is defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061)); or

(B) an accredited minority institution (as such term is defined in section 365 of the Higher Education Act of 1965 (20 U.S.C. 1067k)).

(b) ACTIVITIES TO SUPPORT RESEARCH AND ENGINEERING CAPACITY OF HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY-SERVING INSTITUTIONS OF HIGHER EDUCATION.—Subsection (c) of section 2362 of title 10, United States Code, is amended—

(1) by redesignating paragraph (4) as paragraph (5); and

(2) by inserting after paragraph (3) the following new paragraph (4):

''(4) Developing the capability, including workforce, administrative support, and research infrastructure (including physical), of covered educational institutions to more effectively compete for Federal research and engineering funding opportunities.''.

(c) INCREASING INCENTIVES FOR NATIONAL SECURITY RESEARCH AND ENGINEERING ORGANIZATIONS TO COLLABORATE WITH HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY-SERVING INSTITUTIONS OF HIGHER EDUCATION.—Subsection (d) of such section is amended—

(1) by striking ''The Secretary of Defense may develop'' and inserting ''The Secretary of Defense shall—

''(1) develop'';

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

(3) by adding at the end the following new paragraph:

''(2) establish goals and incentives for each federally funded research and development center, science and technology reinvention laboratory, and university-affiliated research center funded by the Department of Defense to increase and measure the capacity of covered educational institutions to address the research and development needs of the Department through partnerships and collaborations.''.

(d) INCREASING PARTNERSHIPS FOR MINORITY INSTITUTIONS WITH NATIONAL SECURITY RESEARCH AND ENGINEERING ORGANIZATIONS.—Such section is amended—

(1) by redesignating subsections (e) and (f) as (f) and (g) respectively; and

(2) by inserting after subsection (d) the following new subsection (e):

''(e) PARTNERSHIPS.—The Secretary of Defense shall—

''(1) require the core capabilities of each university-affiliated research center to include partnerships with covered educational institutions;

''(2) require in each indefinite delivery indefinite quantity established or renewed with a university-affiliated research center to establish or maintain a partnership with a specific covered educational institution or consortium of covered educational institutions for the purpose of capacity building at such covered educational institution or covered educational institutions;

''(3) require each university-affiliated research center to report annually on their subcontracts and other activities with covered educational institutions; and

''(4) post on a publicly available website of the Department a list of covered educational institutions and their defense research capabilities.''.

(e) DEFINITION OF UNIVERSITY-AFFILIATED RESEARCH CENTERS.—Subsection (g) of such section, as redesignated by subsection (d)(1), is amended to read as follows:

''(f) DEFINITIONS.—In this section:

''(1) the term 'covered educational institution' means—

''(A) an institution of higher education eligible for assistance under title III or V of the Higher Education Act of 1965 (20 U.S.C. 1051 et seq.); or

''(B) an accredited postsecondary minority institution.

''(2) The term 'university-affiliated research center' means a research organization within an institution of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) that—

''(A) provides or maintains Department essential engineering, research, or development capabilities; and

''(B) receives sole source contract funding from the Department pursuant to section 2304(c)(3)(B) of this title.''.

SEC. _____. FUNDING FOR APPLIED AND ADVANCED TECHNOLOGY DEVELOPMENT AT HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY INSTITUTIONS.

(a) ADDITIONAL FUNDING.—

(1) APPLIED RESEARCH.—(A) The amount authorized to be appropriated for fiscal year 2022 by section 201 for research, development, test, and evaluation is hereby increased by $10,000,000, with the amount of the increase to be available for Advancement of S&T Priorities (PE 0602251D8Z).

(B) The amount available under subparagraph (A) shall be available for minority institutions.

(2) ADVANCED TECHNOLOGY DEVELOPMENT.—(A) The amount authorized to be appropriated for fiscal year 2022 by section 201 for research, development, test, and evaluation is hereby increased by $10,000,000, with the amount of the increase to be available for Advanced Research (PE 0603180C).

(B) The amount available under subparagraph (A) shall be available for minority institutions.

(b) OFFSET.—The amount authorized to be appropriated for fiscal year 2022 by section 301 for operation and maintenance is hereby decreased by $20,000,000, with the amount of the decrease to be taken from amounts available as specified in the funding table in section 4301 for the Afghanistan Security Forces Fund, Afghan Air Force Sustainment.

(c) MINORITY INSTITUTION DEFINED.—In this subsection, the term ''minority institution'' means—

(1) a part B institution (as such term is defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061)); or

(2) an accredited minority institution (as such term is defined in section 365 of the Higher Education Act of 1965 (20 U.S.C. 1067k)).

SA 4822. Mrs. BLACKBURN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

Strike section 853 and insert the following:

SEC. 853. DETERMINATION WITH RESPECT TO OPTICAL FIBER FOR DEPARTMENT OF DEFENSE PURPOSES.

(a) DETERMINATION.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Commerce, in consultation with the Secretary of Defense and the Director of the Cybersecurity and Infrastructure Security Agency, shall determine whether access, metro, and long-haul passive optical fiber and optical fiber cable that is manufactured or produced by an entity owned or controlled by the People's Republic of China pose an unacceptable risk to the national security of the United States or the security and safety of United States persons pursuant to section 2(b)(1) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(b)(1)).

(2) APPLICABILITY.—If the Secretary of Commerce makes a determination that any such optical fiber or optical fiber cable would pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, and the Commission makes the determination required under section 2(b)(2) of the Secure and Trusted Communications Networks Act (47 U.S.C. 1601(b)(2)), the inclusion of such optical fiber and optical fiber cable on the covered communications equipment and services list shall apply only to such optical fiber or optical fiber cable deployed after such determination.

(b) NOTIFICATION REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce shall notify the congressional defense committees, the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on Energy and Commerce of the House of Representatives of the findings of the review and determination required under subsection (a), publish the determination in the Federal Register, and submit that determination to the relevant Federal agencies, including the Department of Defense, the Cybersecurity and Infrastructure Security Agency, and the Federal Communications Commission.

(c) SAVINGS CLAUSE.—No determination made under section (a) shall impact the current filing and reimbursement process for the Secure and Trusted Communications Networks Reimbursement Program at the Federal Communications Commission.

(d) DEFINITIONS.—In this section:

(1) The term ''access'' means optical fiber and optical fiber cable that connects subscribers (residential and business) and radio sites to a service provider.

(2) The term ''control'' means the ability to determine the outcome of decision-making for a company through the strategic policy setting exercised by boards of directors or similar organizational governance bodies and the day-to-day management and administration of business operations as overseen by principals.

(3) The term ''long haul'' means optical fiber and optical fiber cable that connects cities and metropolitan areas.

(4) The term ''metro'' means optical fiber and optical fiber cable that connects city

business districts and central city and suburban areas.

(5) The term ''passive'' means unpowered optical fiber and optical fiber cable.

SA 4823. Mr. MARKEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

Strike section 6505 and insert the following:

SEC. 6505. BRIEFING ON CONSULTATIONS WITH UNITED STATES ALLIES REGARDING NUCLEAR POSTURE REVIEW.

(a) IN GENERAL.—Not later than January 31, 2022, the Secretary of Defense, in coordination with the Secretary of State, shall brief the appropriate congressional committees on all consultations with United States allies and related matters regarding the 2021 Nuclear Posture Review.

(b) ELEMENTS.—The briefing required by subsection shall include the following:

(1) A listing of all countries consulted with respect to the 2021 Nuclear Posture Review, including the dates and circumstances of each such consultation and the countries present.

(2) An overview of the topics and concepts discussed with each such country during such consultations, including any discussion of potential changes to the nuclear declaratory policy of the United States.

(3) A summary of any feedback provided during such consultations.

(4) A description of the consultations conducted by the Department of Defense and the Department of State with experts outside such Departments and civil society organizations with respect to the 2021 Nuclear Posture Review.

(5) A listing of the consultants who participated in the 2021 Nuclear Posture Review in a formal or informal capacity.

(6) An identification of the options related to United States nuclear force structure and nuclear doctrine that were presented to the President by the Department of Defense.

SA 4824. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. 1064. ENSURING CONSIDERATION OF THE NATIONAL SECURITY IMPACTS OF URANIUM AS A CRITICAL MINERAL.

(a) IN GENERAL.—The Secretary of Defense, in coordination with the Secretary of Energy, the Secretary of the Interior (acting through the Director of the United States Geological Survey), and the Secretary of Commerce, shall conduct an assessment of the effect on national security that may result from uranium ceasing to be designated as a critical mineral by the Secretary of the Interior pursuant to section 7002(c) of the Energy Act of 2020 (division Z of Public Law 116–260; 30 U.S.C. 1606(c)).

(b) REPORT REQUIRED.—Not later than 180 days after enactment of this Act, the Secretary of Defense shall submit to the appropriate committees of Congress a report on the findings of the assessment conducted under subsection (a), including an assessment of—

(1) any effects the change in designation described in that subsection may have on domestic uranium production;

(2) any effects of the reliance of the United States on imports of uranium from foreign sources, including from state-owned entities, to supply fuel for commercial reactors;

(3) the effects of such reliance and other factors on the domestic production, conversion, fabrication, and enrichment of uranium as it relates to national security, including energy security purposes; and

(4) any effects on Federal national security programs, including existing and future uses of unobligated, United States-origin uranium.

(c) RECOMMENDATION ON URANIUM CRITICAL MINERAL DESIGNATION.—The report required by subsection (b) shall include a recommendation to the Secretary of the Interior regarding whether it is in the interest of the United States to consider uranium for future designation as a critical mineral pursuant to section 7002(c) of the Energy Act of 2020 (division Z of Public Law 116–260; 30 U.S.C. 1606(c)).

(d) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Armed Services, the Committee on Energy and Natural Resources, the Committee on Commerce, Science, and Transportation of the Senate; and

(2) the Committee on Armed Services, the Committee on Energy and Commerce, and the Committee on Natural Resources of the House of Representatives.

SA 4825. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. HA–LEU FOR ADVANCED NUCLEAR REACTORS.

Section 2001 of the Energy Act of 2020 (42 U.S.C. 16281) is amended—

(1) in subsection (a)—

(A) in paragraph (2)—

(i) in subparagraph (D)—

(I) in clause (v)(III), by adding ''or'' after the semicolon at the end;

(II) by striking clause (vi); and

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

(ii) in subparagraph (E), by striking ''for domestic commercial use'' and inserting ''to meet the needs of commercial, government, academic, and international entities''; and

(B) by redesignating paragraphs (6) and (7) as paragraphs (8) and (6), respectively, and moving the paragraphs so as to appear in numerical order;

(2) in subsection (b)(2)—

(A) by striking ''subsection (a)(1)'' each place it appears and inserting ''subsection (b)(1)'';

(B) in subparagraph (B)(viii), by striking ''subsection (a)(2)(F)'' and inserting ''subsection (b)(2)(F)''; and

(C) in subparagraph (D)(vi), by striking ''subsection (a)(2)(A)'' and inserting ''subsection (b)(2)(A)'';

(3) in subsection (c)—

(A) by redesignating paragraphs (1) through (5) as subparagraphs (A) through (E), respectively, and indenting appropriately; and

(B) in the matter preceding subparagraph (A) (as so redesignated)—

(i) by striking ''There are'' and inserting the following:

''(7) AUTHORIZATION OF APPROPRIATIONS.—There are''; and

(ii) by striking ''in this section'' and inserting ''under this subsection'';

(4) in subsection (d)—

(A) by redesignating paragraphs (1) through (6) as paragraphs (2), (3), (5), (6), (7), and (8), respectively;

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

''(1) ADVANCED NUCLEAR REACTOR.—The term 'advanced nuclear reactor' has the meaning given the term in section 951(b) of the Energy Policy Act of 2005 (42 U.S.C. 16271(b)).''; and

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

''(4) DEPARTMENT.—The term 'Department' means the Department of Energy.'';

(5) by moving paragraph (7) of subsection (c) (as designated by paragraph (3)(B)(i)) so as to appear after paragraph (6) of subsection (a) (as redesignated by paragraph (1)(B));

(6) by striking subsection (c);

(7) by redesignating subsections (a), (b), and (d) as subsections (b), (g), and (a), respectively, and moving the subsections so as to appear in alphabetical order; and

(8) by inserting after subsection (b) (as so redesignated) the following:

''(c) HA–LEU FOR ADVANCED NUCLEAR REACTOR DEMONSTRATION PROJECTS.—

''(1) ACTIVITIES.—Not later than 30 days after the date of enactment of the National Defense Authorization Act for Fiscal Year 2022, the Secretary shall initiate activities to make available HA–LEU, produced from inventories owned by the Department, for use by advanced nuclear reactors, with priority given to the awards made pursuant to the funding opportunity announcement of the Department numbered DE–FOA–0002271 for Pathway 1, Advanced Reactor Demonstrations, with additional HA–LEU to be made available to members of the consortium established under subsection (b)(2)(F), as available.

''(2) OWNERSHIP.—HA–LEU made available under this subsection—

''(A) shall remain the property of, and title shall remain with, the Department; and

''(B) shall not be subject to the requirements of section 3112(d)(2) and 3113 of the USEC Privatization Act (42 U.S.C. 2297h–10(d)(2), 2297h–11).

''(3) QUANTITY.—In carrying out activities under this subsection, the Secretary, to the maximum extent practicable, shall make available—

''(A) by September 30, 2024, not less than 3 metric tons of HA–LEU; and

''(B) by December 31, 2025, not less than an additional 15 metric tons of HA–LEU.

''(4) FACTORS FOR CONSIDERATION.—In carrying out activities under this subsection, the Secretary shall take into consideration—

''(A) options for providing HA–LEU from a stockpile of uranium owned by the Department (including the National Nuclear Security Administration), including—

''(i) fuel that—

''(I) directly meets the needs of the end-users described in paragraph (1); but

''(II) has been previously used or fabricated for another purpose;

''(ii) fuel that can meet the needs of the end-users described in paragraph (1) after removing radioactive or other contaminants that resulted from a previous use or fabrication of the fuel for research, development, demonstration, or deployment activities of the Department (including activities of the National Nuclear Security Administration);

''(iii) fuel from a high-enriched uranium stockpile, which can be blended with lower assay uranium to become HA–LEU to meet the needs of the end-users described in paragraph (1); and

''(iv) fuel from uranium stockpiles intended for other purposes, but for which material could be swapped or replaced in time in such a manner that would not negatively impact the missions of the Department;

''(B) options for providing HA–LEU from domestically enriched HA–LEU procured by the Department through a competitive process pursuant to the HA–LEU Bank established under subsection (d)(3)(C); and

''(C) options to replenish, as needed, Department stockpiles of uranium made available pursuant to subparagraph (A) with domestically enriched HA–LEU procured by the Department through a competitive process pursuant to the HA–LEU Bank established under subsection (d)(3)(C).

''(5) LIMITATION.—The Secretary shall not barter or otherwise sell or transfer uranium in any form in exchange for services relating to—

''(A) the final disposition of radioactive waste from uranium that is the subject of a contract for sale, resale, transfer, or lease under this subsection; or

''(B) environmental cleanup activities.

''(6) APPROPRIATIONS.—In addition to amounts otherwise made available, there is appropriated to the Secretary to carry out this subsection, out of any amounts in the Treasury not otherwise appropriated, $200,000,000 for each of fiscal years 2022 through 2026.

''(7) SUNSET.—The authority of the Secretary to carry out activities under this subsection shall terminate on the earlier of—

''(A) September 30, 2027; and

''(B) the date on which the HA–LEU needs of the end-users described in paragraph (1) can be fully met by commercial enrichers in the United States.

''(d) COMMERCIAL HA–LEU AVAILABILITY.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of the National Defense Authorization Act for Fiscal Year 2022, the Secretary shall establish a program (referred to in this subsection as the 'program') to accelerate the availability of commercially produced HA–LEU in the United States in accordance with this subsection.

''(2) PURPOSES.—The purposes of the program are—

''(A) to provide for the availability of HA–LEU enriched, deconverted, and fabricated in the United States;

''(B) to address nuclear supply chain issues in the United States; and

''(C) to support strategic nuclear fuel cycle capabilities in the United States.

''(3) CONSIDERATIONS.—In carrying out the program, the Secretary shall consider and, as appropriate, execute—

''(A) options to establish, through a competitive process, a commercial HA–LEU production capability of not less than 20 metric tons of HA–LEU per year by—

''(i) December 31, 2026; or

''(ii) the earliest operationally feasible date thereafter;

''(B) options that provide for an array of HA–LEU—

''(i) enrichment levels;

''(ii) output levels to meet demand; and

''(iii) fuel forms; and

''(C) options to establish, through a competitive process, a HA–LEU Bank—

''(i) to replenish Department stockpiles of material used in carrying out activities under subsection (c); and

''(ii) after replenishing those stockpiles, to make HA–LEU available to members of the consortium established under subsection (b)(2)(F).

''(4) APPROPRIATIONS.—In addition to amounts otherwise made available, there is appropriated to the Secretary to carry out this subsection, out of any amounts in the Treasury not otherwise appropriated, $150,000,000 for each of fiscal years 2022 through 2031.

''(e) COST RECOVERY.—

''(1) IN GENERAL.—In carrying out activities under subsections (c) and (d), the Secretary shall ensure that any HA–LEU acquired, provided, or made available under those subsections for members of the consortium established under subsection (b)(2)(F) is subject to cost recovery in accordance with subsection (b)(2)(G).

''(2) AVAILABILITY OF CERTAIN FUNDS.—Notwithstanding section 3302 of title 31, United States Code, revenues received from the sale or transfer of fuel feed material and other activities related to making HA–LEU available pursuant to this section—

''(A) shall be available to the Department for carrying out the purposes of this section, to reduce the need for further appropriations for those purposes; and

''(B) shall remain available until expended.

''(f) EXCLUSION.—In carrying out activities under this section, the Secretary shall not make available, or provide funding for, uranium that is recovered, downblended, converted, or enriched by an entity that—

''(1) is owned or controlled by the Government of the Russian Federation or the Government of the People's Republic of China; or

''(2) is organized under the laws of, or otherwise subject to the jurisdiction of, the Russian Federation or the People's Republic of China.''.

SA 4826. Mr. TOOMEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. STATE AND LOCAL LAW ENFORCEMENT ACCESS TO LIFESAVING FEDERAL EQUIPMENT.

(a) UNENFORCEABILITY OF CERTAIN REGULATIONS UNLESS ENACTED INTO LAW.—

(1) IN GENERAL.—No regulation, rule, guidance, policy, or recommendations issued on or after May 15, 2015, that limits the sale or donation of property of the Federal Government, including excess property of the Department of Defense, to State and local agencies for law enforcement activities (whether pursuant to section 2576a of title 10, United States Code, or any other provision of law, or as a condition on the use of Federal funds) shall have any force or effect after the date of the enactment of this Act unless enacted into law by Congress.

(2) PROHIBITION ON USE OF FUNDS TO ENFORCE REGULATIONS.—No agency or instrumentality of the Federal Government may use any Federal funds, fees, or resources to implement or carry out a regulation, rule, guidance, policy, or recommendation issued as described in subsection (a) that is not enacted into law by Congress.

(b) RETURN OR REISSUE OF EQUIPMENT RECALLED OR SEIZED PURSUANT TO REGULATIONS.—Any property recalled or seized on or after May 15, 2015, pursuant to a regulation, rule, guidance, policy, or recommendation issued as described in subsection (a) shall be returned, replaced, or re-issued to the agency from which recalled or seized, at no cost to such agency, as soon as practicable after the date of the enactment of this Act.

SA 4827. Mr. ROUNDS (for himself and Mr. VAN HOLLEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. 1283. SENSE OF CONGRESS ON THE NECESSITY OF MAINTAINING THE UNITED NATIONS ARMS EMBARGO ON SOUTH SUDAN UNTIL CONDITIONS FOR PEACE, STABILITY, DEMOCRACY, AND DEVELOPMENT EXIST.

It is the sense of Congress that—

(1) the signatories to the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan, signed on September 12, 2018, have delayed implementation, leading to continued conflict and instability in South Sudan;

(2) despite years of fighting, 2 peace agreements, punitive actions by the international community, and widespread suffering among civilian populations, the leaders of South Sudan have failed to build sustainable peace;

(3) the United Nations arms embargo on South Sudan, most recently extended by 1 year to May 31, 2022, through United Nations Security Council Resolution 2577 (2021), is a necessary act by the international community to stem the illicit transfer and destabilizing accumulation and misuse of small arms and light weapons in perpetuation of the conflict in South Sudan;

(4) the United States should call on other member states of the United Nations to redouble efforts to enforce the United Nations arms embargo on South Sudan; and

(5) the United States, through the United States Mission to the United Nations, should use its voice and vote in the United Nations Security Council in favor of maintaining the United Nations arms embargo on South Sudan until—

(A) the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan is fully implemented; or

(B) credible, fair, and transparent democratic elections are held in South Sudan.

SA 4828. Mr. BLUMENTHAL submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle B of title XII, insert the following:

SEC. 1216. STRATEGY TO SUPPORT NATIONALS OF AFGHANISTAN WHO ARE APPLICANTS FOR SPECIAL IMMIGRANT VISAS OR FOR REFERRAL TO THE UNITED STATES REFUGEE ADMISSIONS PROGRAM.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the United States should increase support for nationals of Afghanistan who aided the United States mission in Afghanistan during the past 20 years and are now under threat from the Taliban, specifically such nationals of Afghanistan, in Afghanistan or third countries, who are applicants for—

(1) special immigrant visas under the Afghan Allies Protection Act of 2009 (8 U.S.C. 1101 note; Public Law 111–8) or section 1059 of the National Defense Authorization Act for Fiscal Year 2006 (8 U.S.C. 1101 note; Public Law 109–163); or

(2) referral to the United States Refugee Admissions Program as refugees (as defined in section 101(a)(42) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(42))), including as Priority 2 refugees.

(b) STRATEGY.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of State, in coordination with the Secretary of Homeland Security and the heads of other relevant Federal departments and agencies, shall submit to the appropriate committees of Congress a strategy for the safe processing abroad of nationals of Afghanistan described in subsection (a).

(2) ELEMENTS.—The strategy required by paragraph (1) shall include a detailed plan—

(A) to prioritize for evacuation from Afghanistan nationals of Afghanistan described in subsection (a);

(B) to provide for expedited initial security vetting for such nationals of Afghanistan, to be conducted remotely before their departure from Afghanistan;

(C) to facilitate, after such vetting, the rapid departure from Afghanistan by air charter and land passage of such nationals of Afghanistan who satisfy the requirements of such vetting;

(D) to provide letters of support, diplomatic notes, and other documentation, as appropriate, to ease transit for such nationals of Afghanistan;

(E) to engage governments of relevant countries to better facilitate evacuation of such nationals of Afghanistan;

(F) to disseminate frequent updates to such nationals of Afghanistan and relevant nongovernmental organizations with respect to evacuation from Afghanistan;

(G) to identify and establish sufficient locations outside Afghanistan and the United States that will accept such nationals of Afghanistan during application processing (including during the processes of vetting and establishing the eligibility of such nationals of Afghanistan before their travel to the United States, which shall include any required in-person interviews) for—

(i) the special immigrant visas described in paragraph (1) of subsection (a); or

(ii) referral to the United States Refugee Admissions Program described in paragraph (2) of that subsection;

(H) to identify necessary resource, personnel, and equipment requirements to increase capacity to better support such nationals of Afghanistan and reduce their application processing times, while ensuring strict and necessary security vetting, including, to the extent practicable, by allowing such nationals of Afghanistan to receive referrals to the United States Refugee Admissions Program while they are still in Afghanistan so as to initiate application processing more expeditiously; and

(I) to provide for relocation outside Afghanistan to third countries for nationals of Afghanistan described in subsection (a) who are unable to successfully complete security vetting and application processing to establish eligibility to travel to the United States.

(3) FORM.—The strategy required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(c) MONTHLY REPORT.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, and monthly thereafter until December 31, 2022, the Secretary of State, in coordination with the Secretary of Homeland Security and the heads of other relevant Federal departments and agencies, shall submit to the appropriate committees of Congress a report on efforts to support nationals of Afghanistan described in subsection (a).

(2) ELEMENTS.—Each report required by paragraph (1) shall include the following:

(A) The number of nationals of Afghanistan referred to the United States Refugee Admissions Program as Priority 1 and Priority 2 refugees since August 29, 2021.

(B) An assessment of whether each such refugee—

(i) remains in Afghanistan; or

(ii) is outside Afghanistan.

(C) With respect to nationals of Afghanistan who have applied for referral to the United States Refugee Program, the number applications that—

(i) have been approved;

(ii) have been denied; and

(iii) are pending adjudication.

(D) The number of nationals of Afghanistan who have pending applications for special immigrant visas described in subsection (a)(1), disaggregated by the special immigrant visa processing steps completed with respect to such individuals.

(E) A description of the measures taken to implement the strategy under subsection (b).

(d) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Foreign Relations, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs; and the Committee on Armed Services of the Senate; and

(2) the Committee on Foreign Affairs, the Committee on the Judiciary, the Committee on Homeland Security, and the Committee on Armed Services of the House of Representatives.

SA 4829. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. RELEASE OF REVERSIONARY INTEREST OF THE UNITED STATES IN NON-FEDERAL LAND IN SALT LAKE CITY, UTAH.

(a) RELEASE.—There is released to the University of Utah, without consideration, the reversionary interest of the United States in the non-Federal land described in subsection (b).

(b) DESCRIPTION OF NON-FEDERAL LAND.—The non-Federal land referred to in subsection (a) is the approximately 593 acres of land of the University of Utah—

(1) depicted as ''U of U Research Park'' on the map—

(A) prepared by the Bureau of Land Management;

(B) entitled ''University of Utah-Research Park''; and

(C) dated September 23, 2021;

(2) identified in the patent—

(A) numbered 43–99–0012; and

(B) dated October 18, 1968; and

(3) more particularly described as tracts D (excluding the parcels numbered 1, 2, 3, 4, and 5), G, and J, T. 1 S., R. 1 E., Salt Lake Meridian.

SA 4830. Mr. MANCHIN (for himself, Mrs. CAPITO, Mrs. HYDE-SMITH, Mr. ROMNEY, Mr. COTTON, Mrs. BLACKBURN, and Mr. TESTER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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

SEC. 1043. HONORING HERSHEL WOODROW "WOODY" WILLIAMS AS THE LAST SURVIVING MEDAL OF HONOR RECIPIENT OF WORLD WAR II.

(a) USE OF ROTUNDA.—Upon his death, Hershel Woodrow ''Woody'' Williams, who is the last surviving recipient of the Medal of Honor for acts performed during World War II, shall be permitted to lie in state in the rotunda of the United States Capitol if he or his next of kin so elects.

(b) IMPLEMENTATION.—The Architect of the Capitol, under the direction of the President pro tempore of the Senate and the Speaker of the House of Representatives, shall take the necessary steps to implement subsection (a).

SA 4831. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

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, privacy, disclosure, and sharing of information;'';

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

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

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

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

''(1) develop, and in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies; and'';

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

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

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

(D) by adding at the end the following:

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

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

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

(2) in section 3553—

(A) 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 consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director,'' before ''overseeing'';

(ii) in paragraph (5), 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 cyber threat intelligence;

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

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

''(10) any other information the Director of the Cybersecurity and Infrastructure Security Agency determines relevant.''; 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 consultation 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 majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

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

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

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

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

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

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

''(B) may include a classified annex.

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

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

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

(b) 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''.

(c) 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''.

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

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

(2) in subsection (b)(1)(A), by striking ''the Secretary of Homeland Security'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(3) by 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 cyber 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 in consultation with the National Cyber Director, shall issue guidance to agencies on sharing relevant information in a consistent, automated, and machine readable manner with the 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 cyber threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and

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

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) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 6203 of this division.

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 or subcontract at any tier, grant, cooperative agreement, or other transaction agreement, unless that entity 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 section 2232(a) and 2233 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 briefings required under subsection (c);

''(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 National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—

''(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.—A covered entity, except for an individual or a small organization, that makes a ransom payment as the result of a ransomware attack against the covered 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 covered 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 a covered 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, the Department of Justice, and 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 is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

''(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 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 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 that is a Federal contractor 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.

''(5) AUTHENTICATION.—

''(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

''(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

''(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

''(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate Federal regulatory agency 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 Federal regulatory agency 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); or

''(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

''(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b); or

''(2) issued a subpoena pursuant to subsection (c).

''(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

''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 or 2233 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 cyber incident reported pursuant to section 2232 or 2233 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 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, including any independent establishment (as defined in section 104 of title 5, United States Code), 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. The Director shall share and coordinate each report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 6103 of this title.

(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, the Attorney General, 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 Attorney General, 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, the Attorney General, 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 paragraph (11), by striking ''and'' at the end;

(2) in the first paragraph (12)—

(A) by striking ''section 2215'' and inserting ''section 2217''; and

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

(3) 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 use or threat of use of unauthorized or malicious code on an information system, or the use or 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 CONTROL.—The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

''(25) 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.

''(26) SHARING.—The term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

''(27) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber incident within the supply chain of an information system that an adversary can leverage to jeopardize 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.

''(28) 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.

''(29) 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)—

(i) in subparagraph (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))''; and

(ii) in subparagraph (B)(ii), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(D) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)''; and

(ii) in paragraph (1)(E)(ii)(II), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(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) in subsection (d)(2), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(B) 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.'';

(11) in section 2218(c)(4)(A), as so redesignated, by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; 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 item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''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 paragraphs (16) and (17) and inserting the following:

''(16) SECURITY CONTROL.—The term 'security control' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(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(b) (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 (6 U.S.C. 1524)—

(A) in subsection (a)—

(i) in paragraph (1), by striking ''section 2213'' and inserting ''section 2200'';

(ii) in paragraph (2), by striking ''section 102'' and inserting ''section 2200 of the Homeland Security Act of 2002'';

(iii) in paragraph (4), by striking ''section 2210(b)(1)'' and inserting ''section 2210(a)(1)''; and

(iv) 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(b) of the Homeland Security Act of 2002 (6 U.S.C. 660(b))''.

(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)'' and inserting ''section 2200''; 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 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)''.

(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) of the Homeland Security Act of 2002 (6 U.S.C. 659(m))'' and inserting ''section 2209(l) of the Homeland Security Act of 2002 (6 U.S.C. 659(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''.

TITLE LXIII—FEDERAL CYBERSECURITY REQUIREMENTS

SEC. 6301. EXEMPTION FROM FEDERAL CYBERSECURITY REQUIREMENTS.

(a) IN GENERAL.—Section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) is amended to read as follows:

''(2) EXCEPTION.—

''(A) IN GENERAL.—A particular requirement under paragraph (1) shall not apply to an agency information system of an agency if—

''(i) with respect to the agency information system, the head of the agency submits to the Director an application for an exemption from the particular requirement, in which the head of the agency personally certifies to the Director with particularity that—

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

''(II) the particular requirement is not necessary to secure the agency information system or agency information stored on or transiting the agency information system; and

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

''(ii) the head of the agency or the designee of the head of the agency has submitted the certification described in clause (i) to the appropriate congressional committees and any other congressional committee with jurisdiction over the agency; and

''(iii) the Director grants the exemption from the particular requirement.

''(B) DURATION OF EXEMPTION.—

''(i) IN GENERAL.—An exemption granted under subparagraph (A) shall expire on the date that is 1 year after the date on which the Director grants the exemption.

''(ii) RENEWAL.—Upon the expiration of an exemption granted to an agency under subparagraph (A), the head of the agency may apply for an additional exemption.''.

(b) REPORT ON EXEMPTIONS.—Section 3554(c)(1) of title 44, United States Code, as amended by section 5121 of this Act, is further amended—

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

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

(3) by adding at the end the following:

''(E) with respect to any exemptions the agency is granted by the Director of the Office of Management and Budget under section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) that is effective on the date of submission of the report, includes—

''(i) an identification of the particular requirements from which any agency information system (as defined in section 2210 of the Homeland Security Act of 2002 (6 U.S.C. 660)) is exempted; and

''(ii) for each requirement identified under subclause (I)—

''(I) an identification of the agency information system described in subclause (I) exempted from the requirement; and

''(II) an estimate of the date on which the agency will to be able to comply with the requirement.''.

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

SA 4832. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of title XII, add the following:

Subtitle H—Sanctions Relating to the Actions of the Russian Federation With Respect to Ukraine

SEC. 1291. DEFINITIONS.

In this subtitle:

(1) ADMISSION; ADMITTED; ALIEN.—The terms ''admission'', ''admitted'', and ''alien'' have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

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

(A) the Committee on Foreign Relations and the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives.

(3) DEFENSE ARTICLE; DEFENSE SERVICE.—The terms ''defense article'' and ''defense service'' have the meanings given those terms in section 47 of the Arms Export Control Act (22 U.S.C. 2794).

(4) FINANCIAL INSTITUTION.—The term ''financial institution'' means a financial institution specified in subparagraph (A), (B), (C), (D), (E), (F), (G), (H), (I), (J), (M), or (Y) of section 5312(a)(2) of title 31, United States Code.

(5) FOREIGN FINANCIAL INSTITUTION.—The term ''foreign financial institution'' has the meaning given that term in regulations prescribed by the Secretary of the Treasury.

(6) FOREIGN PERSON.—The term ''foreign person'' means an individual or entity that is not a United States person.

(7) KNOWINGLY.—The term ''knowingly'' with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.

(8) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States; or

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity.

SEC. 1292. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) it is in the national security interests of the United States to continue and deepen the security partnership between the United States and Ukraine, including through providing both lethal and non-lethal assistance to Ukraine;

(2) aggression and malign influence by the Government of the Russian Federation in Ukraine is a threat to the democratic sovereignty of Ukraine, a valued and key partner of the United States;

(3) economic and financial sanctions, when used as part of a coordinated and comprehensive strategy, are a powerful tool to advance United States foreign policy and national security interests;

(4) the United States should expedite the provision of lethal and non-lethal assistance to Ukraine, and use all available tools to support and bolster the defense of Ukraine against potential aggression and military escalation by the Government of the Russian Federation;

(5) the United States should work closely with partners and allies to encourage the provision of lethal and non-lethal assistance to support and bolster the defense of Ukraine; and

(6) substantial new sanctions should be imposed in the event that the Government of

the Russian Federation engages in escalatory military or other offensive operations against Ukraine.

SEC. 1293. DETERMINATION WITH RESPECT TO OPERATIONS OF THE RUSSIAN FEDERATION IN UKRAINE.

Not later than 15 days after the date of the enactment of this Act, and periodically as necessary thereafter, the President shall—

(1) determine whether—

(A) the Government of the Russian Federation is engaged in or knowingly supporting a significant escalation in hostilities or hostile action in or against Ukraine, compared to the level of hostilities or hostile action in or against Ukraine prior to November 1, 2021; and

(B) if so, whether such escalation has the aim of undermining, overthrowing, or dismantling the Government of Ukraine, occupying the territory of Ukraine, or interfering with the sovereignty or territorial integrity of Ukraine; and

(2) submit to the appropriate congressional committees a report on that determination.

SEC. 1294. IMPOSITION OF SANCTIONS WITH RESPECT TO OFFICIALS OF THE GOVERNMENT OF THE RUSSIAN FEDERATION RELATING TO OPERATIONS IN UKRAINE.

(a) IN GENERAL.—Upon making an affirmative determination under section 1293(1) and not later than 30 days following such a determination, the President shall impose the sanctions described in subsection (d) with respect to each of the officials specified in subsection (b).

(b) OFFICIALS SPECIFIED.—The officials specified in this subsection are the following:

(1) The President of the Russian Federation.

(2) The Prime Minister of the Russian Federation.

(3) The Foreign Minister of the Russian Federation.

(4) The Minister of Defense of the Russian Federation.

(5) The Chief of the General Staff of the Armed Forces of the Russian Federation.

(6) The Commander-in-Chief of the Land Forces of the Russian Federation.

(7) The Commander of the Aerospace Forces of the Russian Federation.

(8) The Commander of the Airborne Forces of the Russian Federation.

(9) The Commander in Chief of the Navy of the Russian Federation.

(10) The Commander of the Strategic Rocket Forces of the Russian Federation.

(11) The Commander of the Special Operations Forces of the Russian Federation.

(12) The Commander of Logistical Support of the Russian Armed Forces.

(c) ADDITIONAL OFFICIALS.—

(1) LIST REQUIRED.—Not later than 30 days after making an affirmative determination under section 1293(1), and every 90 days thereafter, the President shall submit to the appropriate congressional committees a list of foreign persons that the President determines are—

(A) senior officials of any branch of the armed forces of the Russian Federation leading any of the operations described in section 1293(1); or

(B) senior officials of the Government of the Russian Federation, including any branch of the armed forces or intelligence agencies of the Russian Federation, engaged in planning or implementing such operations.

(2) IMPOSITION OF SANCTIONS.—Upon the submission of each list required by paragraph (1), the President shall impose the sanctions described in subsection (d) with respect to each foreign person identified on the list.

(d) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a foreign person under this section are the following:

(1) PROPERTY BLOCKING.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (b) or (c) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

SEC. 1295. IMPOSITION OF SANCTIONS WITH RESPECT TO FOREIGN FINANCIAL INSTITUTIONS.

(a) IMPOSITION OF SANCTIONS.—

(1) IN GENERAL.—Upon making an affirmative determination under section 1293(1) and not later than 30 days following such a determination, the President shall impose the sanctions described in subsection (c) with respect to 3 or more of the following financial institutions:

(A) Sberbank.

(B) VTB.

(C) Gazprombank.

(D) VEB.RF.

(E) RDIF.

(F) Promsvyazbank.

(2) SUBSIDIARIES AND SUCCESSOR ENTITIES.—The President may impose the sanctions described in subsection (c) with respect to any subsidiary of, or successor entity to, a financial institution specified in paragraph (1).

(b) ADDITIONAL FOREIGN FINANCIAL INSTITUTIONS.—

(1) LIST REQUIRED.—Not later than 30 days after making an affirmative determination under section 1293(1), and every 90 days thereafter, the President shall submit to the appropriate congressional committees a list of foreign persons that the President determines—

(A) are significant financial institutions owned or operated by the Government of the Russian Federation; and

(B) should be sanctioned in the interest of United States national security.

(2) IMPOSITION OF SANCTIONS.—Upon the submission of each list required by paragraph (1), the President shall impose the sanctions described in subsection (c) with respect to each foreign person identified on the list.

(c) SANCTIONS DESCRIBED.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of a foreign person subject to subsection (a) or (b) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

SEC. 1296. PROHIBITION ON AND IMPOSITION OF SANCTIONS WITH RESPECT TO TRANSACTIONS INVOLVING RUSSIAN SOVEREIGN DEBT.

(a) PROHIBITION ON TRANSACTIONS.—Upon making an affirmative determination under section 1293(1) and not later than 30 days following such a determination, the President shall prohibit all transactions by United States persons involving the sovereign debt of the Government of the Russian Federation issued on or after the date of the enactment of this Act, including governmental bonds.

(b) IMPOSITION OF SANCTIONS WITH RESPECT TO STATE-OWNED ENTERPRISES.—

(1) IN GENERAL.—Not later than 60 days after making an affirmative determination under section 1293(1), the President shall identify and impose the sanctions described in subsection (d) with respect to foreign persons that the President determines engage in transactions involving the debt—

(A) of not less than 10 entities owned or controlled by the Government of the Russian Federation; and

(B) that is not subject to any other sanctions imposed by the United States.

(2) APPLICABILITY.—Sanctions imposed under paragraph (1) shall apply with respect to debt of an entity described in subparagraph (A) of that paragraph that is issued after the date that is 90 days after the President makes an affirmative determination under section 1293(1).

(c) LIST; IMPOSITION OF SANCTIONS.—Not later than 30 days after making an affirmative determination under section 1293(1), and every 90 days thereafter, the President shall—

(1) submit to the appropriate congressional committees a list of foreign persons that the President determines are engaged in transactions described in subsection (a); and

(2) impose the sanctions described in subsection (d) with respect to each such person.

(d) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a foreign person described in subsection (b) or (c) are the following:

(1) PROPERTY BLOCKING.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (b) or (c) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

SEC. 1297. IMPOSITION OF SANCTIONS WITH RESPECT TO NORD STREAM 2.

(a) IN GENERAL.—Upon making an affirmative determination under section 1293(1) and

not later than 30 days following such a determination, the President shall impose the sanctions described in subsection (b) with respect to a foreign person that is—

(1) any entity established for or responsible for the planning, construction, or operation of the Nord Stream 2 pipeline or a successor entity; and

(2) any corporate officer of an entity described in paragraph (1).

(b) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a foreign person under this section are the following:

(1) PROPERTY BLOCKING.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (a)(2) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

SEC. 1298. SANCTIONS WITH RESPECT TO RUSSIAN EXTRACTIVE INDUSTRIES.

(a) IDENTIFICATION.—Not later than 60 days after making an affirmative determination under section 1293(1), the President shall identify foreign persons in any of the sectors or industries described in subsection (b) that the President determines should be sanctioned in the interest of United States national security.

(b) SECTORS AND INDUSTRIES DESCRIBED.—The sectors and industries described in this subsection are the following:

(1) Oil and gas extraction and production.

(2) Coal extraction, mining, and production.

(3) Minerals extraction and processing.

(4) Any other sector or industry with respect to which the President determines the imposition of sanctions is in the United States national security interest.

(c) LIST; IMPOSITION OF SANCTIONS.—Not later than 90 days after making an affirmative determination under section 1293(1), the President shall—

(1) submit to the appropriate congressional committees a list of the persons identified under subsection (a); and

(2) impose the sanctions described in subsection (d) with respect to each such person.

(d) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a foreign person under subsection (c) are the following:

(1) PROPERTY BLOCKING.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (c) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

SEC. 1299. AUTHORIZATION FOR USE OF WAR RESERVE STOCKPILE FOR ARMED FORCES OF UKRAINE.

Notwithstanding section 514 of the Foreign Assistance Act of 1961 (22 U.S.C. 2321h) or any other authorized limits set in law, the Secretary of Defense, in concurrence with the Secretary of State, is authorized to transfer defense articles from any war reserve stockpile to Ukraine for the purpose of assisting and supporting the Armed Forces of Ukraine.

SEC. 1299A. USE OF DEPARTMENT OF DEFENSE LEASE AUTHORITY AND SPECIAL DEFENSE ACQUISITION FUND TO SUPPORT UKRAINE.

(a) USE OF SPECIAL DEFENSE ACQUISITION FUND.—The Secretary of Defense, in concurrence with the Secretary of State, shall utilize, to the maximum extent possible, the Special Defense Acquisition Fund established under section 51 of the Arms Export Control Act (22 U.S.C. 2795) to expedite the procurement and delivery of defense articles and defense services for the purpose of assisting and supporting the Armed Forces of Ukraine.

(b) USE OF LEASE AUTHORITY.—The Secretary of Defense, in concurrence with the Secretary of State, shall utilize, to the maximum extent possible, its lease authority, including with respect to no-cost leases, to provide defense articles to Ukraine for the purpose of assisting and supporting the Armed Forces of Ukraine.

SEC. 1299B. IMPLEMENTATION; REGULATIONS; PENALTIES.

(a) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this subtitle.

(b) REGULATIONS.—The President shall issue such regulations, licenses, and orders as are necessary to carry out this subtitle.

(c) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of this subtitle or any regulation, license, or order issued to carry out this subtitle shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

SEC. 1299C. EXCEPTIONS; WAIVER.

(a) EXCEPTIONS.—

(1) INTELLIGENCE ACTIVITIES.—This subtitle shall not apply with respect to activities subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) or any authorized intelligence activities of the United States.

(2) EXCEPTION COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT AND LAW ENFORCEMENT OBJECTIVES.—Sanctions under this subtitle shall not apply to an alien if admitting the alien into the United States—

(A) is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success on June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations of the United States; or

(B) would further important law enforcement objectives.

(3) EXCEPTION RELATING TO IMPORTATION OF GOODS.—

(A) IN GENERAL.—The authority or a requirement to impose sanctions under this subtitle shall not include the authority or a requirement to impose sanctions on the importation of goods.

(B) GOOD DEFINED.—In this paragraph, the term ''good'' means any article, natural or manmade substance, material, supply, or manufactured product, including inspection and test equipment, and excluding technical data.

(b) NATIONAL SECURITY WAIVER.—The President may waive the imposition of sanctions under this subtitle with respect to a person if the President—

(1) determines that such a waiver is in the national security interests of the United States; and

(2) submits to the appropriate congressional committees a notification of the waiver and the reasons for the waiver.

SEC. 1299D. TERMINATION.

The President may terminate the sanctions imposed under this subtitle after determining and certifying to the appropriate congressional committees that the Government of the Russian Federation has—

(1) verifiably withdrawn all of its forces from Ukrainian territory that was not occupied or subject to control by forces or proxies of the Government of the Russian Federation prior to November 1, 2021;

(2) ceased supporting proxies in Ukrainian territory described in paragraph (1); and

(3) has entered into an agreed settlement with a legitimate democratic government of Ukraine.

SEC. 1299E. SUNSET.

The provisions of this subtitle shall terminate on the date that is 3 years after the date of the enactment of this Act.

SA 4833. Mr. BARRASSO (for himself, Mr. CRUZ, and Mr. JOHNSON) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill 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; which was ordered to lie on the table; as follows:

At the end of subtitle D of title XII, add the following:

SEC. 1237. IMPOSITION OF SANCTIONS WITH RESPECT TO NORD STREAM 2.

(a) IN GENERAL.—Not later than 15 days after the date of the enactment of this Act, the President shall—

(1) impose sanctions under subsection (b) with respect to—

(A) Nord Stream 2 AG or a successor entity;

(B) Matthias Warnig; and

(C) any other corporate officer of or principal shareholder with a controlling interest in Nord Stream 2 AG or a successor entity; and

(2) impose sanctions under subsection (c) with respect to—

(A) Nord Stream 2 AG or a successor entity; and

(B) Matthias Warnig.

(b) INELIGIBILITY FOR VISAS, ADMISSION, OR PAROLE OF IDENTIFIED PERSONS AND CORPORATE OFFICERS.—

(1) IN GENERAL.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (a)(1) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien described in subsection (a)(1) shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

(c) BLOCKING OF PROPERTY OF IDENTIFIED PERSONS.—The President shall exercise all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of a person described in subsection (a)(2) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(d) IMPLEMENTATION; PENALTIES.—

(1) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this section.

(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of this section or any regulation, license, or order issued to carry out this section shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(e) EXCEPTIONS.—

(1) EXCEPTION FOR INTELLIGENCE, LAW ENFORCEMENT, AND NATIONAL SECURITY ACTIVITIES.—Sanctions under this section shall not apply to any authorized intelligence, law enforcement, or national security activities of the United States.

(2) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under this section shall not apply with respect to the admission of an alien to the United States if the admission of the alien is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, the Convention on Consular Relations, done at Vienna April 24, 1963, and entered into force March 19, 1967, or other applicable international obligations.

(3) EXCEPTION RELATING TO IMPORTATION OF GOODS.—

(A) IN GENERAL.—Notwithstanding any other provision of this section, the authorities and requirements to impose sanctions under this section shall not include the authority or a requirement to impose sanctions on the importation of goods.

(B) GOOD DEFINED.—In this paragraph, the term ''good'' means any article, natural or man-made substance, material, supply or manufactured product, including inspection and test equipment, and excluding technical data.

(f) SUNSET.—The authority to impose sanctions under this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(g) DEFINITIONS.—In this section:

(1) ADMISSION; ADMITTED; ALIEN.—The terms ''admission'' , ''admitted'' , and ''alien'' have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

(2) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity; or

(C) any person within the United States.

AUTHORITY FOR COMMITTEES TO MEET

Mr. TESTER. Mr. President, I have 6 requests for committees to meet during today's session of the Senate. They have the approval of the Majority and Minority Leaders.

Pursuant to rule XXVI, paragraph 5(a), of the Standing Rules of the Senate, the following committees are authorized to meet during today's session of the Senate:

COMMITIEE ON BANKING, HOUSING, AND URBAN AFFAIRS

The Committee on Banking, Housing, and Urban Affairs is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9:30 a.m., to conduct a hearing on a nomination.

COMMITIEE ON ENERGY AND NATURAL RESOURCES

The Committee on Energy and Natural Resources is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 10 a.m., to conduct a business meeting.

COMMITIEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

The Committee on Homeland Security and Governmental Affairs is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 10:15 a.m., to conduct a hearing on nominations.

COMMITIEE ON THE JUDICIARY

The Committee on the Judiciary is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9 a.m., to conduct a hearing.

SPECIAL COMMITIEE ON AGING

The Special Committee on Aging is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9:30 a.m., to conduct a hearing.

SUBCOMMITIEE ON WESTERN HEMISPHERE, TRANSNATIONAL CRIME, CIVILIAN SECURITY, DEMOCRACY, HUMAN RIGHTS, AND GLOBAL WOMEN'S ISSUES

The Subcommittee on Western Hemisphere, Transnational Crime, Civilian Security, Democracy, Human Rights, and Global Women's Issues of the Committee on Foreign Relations is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 10 a.m., to conduct a hearing.

PRIVILEGES OF THE FLOOR

Mr. REED. Mr. President, I ask unanimous consent that Leslie Ashton and Cami Pease, Government Accountability Office detailees to the Senate Armed Services Committee, have floor privileges during consideration of the fiscal year 2022 National Defense Authorization Act.

The PRESIDING OFFICER. Without objection, it is so ordered.

The PRESIDING OFFICER. The majority leader.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mr. SCHUMER. Madam President, I ask unanimous consent that the Senate proceed to executive session to consider the following nominations en bloc: Calendar Nos. 332 and 444; that the Senate vote on the nominations en bloc without intervening action or debate; that the motions to reconsider be considered made and laid upon the table with no intervening action or debate; that any statements related to the nominations be printed in the RECORD; that the President be immediately notified of the Senate's action, and the Senate resume legislative session.

There being no objection, the Senate proceeded to consider the nominations.

The PRESIDING OFFICER. The question is, Will the Senate advise and consent to the nominations of Lee Satterfield, of South Carolina, to be an Assistant Secretary of State (Educational and Cultural Affairs) and Jeffrey M. Hovenier, of Washington, a Career Member of the Senior Foreign Service, Class of Minister-Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Kosovo en bloc?

The nominations were confirmed en bloc.

LEGISLATIVE SESSION

The PRESIDING OFFICER. The Senate will now resume legislative session.

ORDERS FOR FRIDAY, NOVEMBER 19, 2021

Mr. SCHUMER. Madam President, I ask unanimous consent that when the