4350, supra; which was ordered to lie on the table.

SA 4692. 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, supra; which was ordered to lie on the table.

SA 4693. 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, supra; which was ordered to lie on the table.

SA 4694. 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, supra; which was ordered to lie on the table.

SA 4695. 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, supra; which was ordered to lie on the table.

SA 4696. 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, supra; which was ordered to lie on the table.

SA 4697. 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, supra; which was ordered to lie on the table.

SA 4698. 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, supra; which was ordered to lie on the table.

SA 4699. 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, supra; which was ordered to lie on the table.

SA 4700. 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, supra; which was ordered to lie on the table.

SA 4701. 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, supra; which was ordered to lie on the table.

SA 4702. 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, supra; which was ordered to lie on the table.

SA 4703. 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, supra; which was ordered to lie on the table.

SA 4704. 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, supra; which was ordered to lie on the table.

SA 4705. 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 4706. Mr. COTTON 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 4707. Mr. WHITEHOUSE (for himself and Ms. HASSAN) submitted an amendment intended to be proposed by him to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4708. Mr. WHITEHOUSE (for himself and Mr. GRASSLEY) submitted an amendment intended to be proposed by him to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4709. Mr. VAN HOLLEN (for himself and Mr. SULLIVAN) 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 4710. Mr. CASSIDY (for himself and Mr. SCHATZ) 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 4711. Mr. MCCONNELL (for himself, Mr. DURBIN, Mr. YOUNG, Mr. GRASSLEY, Mr. GRAHAM, Mr. HAGERTY, and Mr. CARDIN) 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 4712. Mr. WHITEHOUSE (for himself and Mr. PORTMAN) 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 4713. Mr. PADILLA 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 4714. Mr. REED (for himself and Mr. INHOFE) 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 4715. Mr. ROUNDS (for Mr. INHOFE) 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 4716. Mr. HAGERTY (for himself and 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 4717. Mr. BROWN 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 4718. 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 4719. Mr. BROWN (for himself and Mr. CASEY) 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 4720. Mr. ROUNDS (for Mr. INHOFE) submitted an amendment intended to be proposed to amendment SA 4431 submitted by Mr. INHOFE and intended to be proposed to the amendment SA 3867 proposed by Mr. REED to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4721. Mr. WARNOCK 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 4722. 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 4723. Mr. DAINES (for himself 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, supra; which was ordered to lie on the table.

SA 4724. 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, supra; which was ordered to lie on the table.

SA 4725. Ms. CORTEZ MASTO (for herself and Mr. KAINE) 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 4726. 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, supra; which was ordered to lie on the table.

SA 4727. Mr. SULLIVAN 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 4728. 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 4729. 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 4730. Mr. MENENDEZ (for himself and Mr. RISCH) 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 4731. Mr. THUNE submitted an amendment intended to be proposed by him to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4732. Mr. REED 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 4660. 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 end of subtitle B of title XII, add the following:

SEC. 1216. OPPOSITION TO ALLOCATION OF SPECIAL DRAWING RIGHTS BY INTERNATIONAL MONETARY FUND THAT WOULD BENEFIT TALIBAN.

Section 6 of the Special Drawing Rights Act (22 U.S.C. 286q) is amended by adding at the end the following:

''(c) OPPOSITION TO ALLOCATION OF SPECIAL DRAWING RIGHTS THAT WOULD BENEFIT TALIBAN.—

''(1) IN GENERAL.—Unless Congress by law authorizes such action, neither the President nor any person or agency shall on behalf of the United States—

''(A) vote to allocate Special Drawing Rights under article XVIII, sections 2 and 3, of the Articles of Agreement of the Fund to Afghanistan if Afghanistan would receive Special Drawing Rights under the allocation and the Taliban or any associate of the Taliban would benefit from the allocation; or

''(B) act as a counterparty, directly or indirectly, for any exchange with the Government of Afghanistan of Special Drawing Rights for currencies while the Government of Afghanistan is controlled by the Taliban, is organized by the Taliban, or is constituted so that the Taliban is part of that Government.

''(2) TALIBAN DEFINED.—In this subsection, the term 'Taliban' means the entity—

''(A) known as the Taliban and designated as a specially designated global terrorist organization under Executive Order 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism); or

''(B) a successor entity.''.

SA 4661. Mr. COTTON 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 Defense 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, 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 eliminate their dependence on non-allied countries for critical minerals to the maximum extent practicable.

(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 in detail 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 discontinuing the use of critical minerals from foreign entities of concern (as defined in section 9901(6) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (15 U.S.C. 4651(6))) 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.

SA 4662. 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 of subtitle G of title X, add the following:

SEC. 1064. REPORT ON CYBERSECURITY CERTIFICATIONS AND LABELING.

Not later than October 1, 2022, the National Cyber Director, in consultation with the Director of the National Institute of Standards and Technology and the Director of the Cybersecurity and Infrastructure Security Agency, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives a report that—

(1) identifies and assesses existing efforts by the Federal Government to create, administer, or otherwise support the use of certifications or labels to communicate the security or security characteristics of information technology or operational technology products and services; and

(2) assesses the viability of and need for a new program at the Department of Homeland Security, or at other Federal agencies as appropriate, to better address information technology and operational technology product and service security certification and labeling efforts across the Federal Government and between the Federal Government and the private sector.

SA 4663. Mr. BLUMENTHAL (for himself and 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 in title VI, insert the following:

Subtitle ____—Arbitration Rights of Members of the Armed Forces and Veterans

SEC. 6____. SHORT TITLE.

This subtitle may be cited as the ''Justice for Servicemembers Act of 2021''.

SEC. 6____. PURPOSES.

The purposes of this subtitle are—

(1) to prohibit predispute arbitration agreements that force arbitration of disputes arising from claims brought under chapter 43 of title 38, United States Code, or the Servicemembers Civil Relief Act (50 U.S.C. 3901 et seq.); and

(2) to prohibit agreements and practices that interfere with the right of persons to participate in a joint, class, or collective action related to disputes arising from claims brought under the provisions of the laws described in paragraph (1).

SEC. 6____. ARBITRATION OF DISPUTES INVOLVING THE RIGHTS OF SERVICEMEMBERS AND VETERANS.

(a) IN GENERAL.—Title 9, United States Code, is amended by adding at the end the following:

''CHAPTER 4—ARBITRATION OF SERVICEMEMBER AND VETERAN DISPUTES

''Sec.
''401. Definitions.
''402. No validity or enforceability.

''§ 401. Definitions

''In this chapter:

''(1) PREDISPUTE ARBITRATION AGREEMENT.—The term 'predispute arbitration agreement' means an agreement to arbitrate a dispute that has not yet arisen at the time of the making of the agreement.

''(2) PREDISPUTE JOINT-ACTION WAIVER.—The term 'predispute joint-action waiver' means an agreement, whether or not part of a predispute arbitration agreement, that would prohibit, or waive the right of, one of the parties to the agreement to participate in a joint, class, or collective action in a judicial, arbitral, administrative, or other forum, concerning a dispute that has not yet arisen at the time of the making of the agreement.

''§ 402. No validity or enforceability

''(a) IN GENERAL.—Notwithstanding any other provision of this title, no predispute arbitration agreement or predispute joint-action waiver shall be valid or enforceable with respect to a dispute relating to disputes arising under chapter 43 of title 38 or the Servicemembers Civil Relief Act (50 U.S.C. 3901 et seq.).

''(b) APPLICABILITY.—

''(1) IN GENERAL.—An issue as to whether this chapter applies with respect to a dispute shall be determined under Federal law. The applicability of this chapter to an agreement to arbitrate and the validity and enforceability of an agreement to which this chapter applies shall be determined by a court, rather than an arbitrator, irrespective of whether the party resisting arbitration challenges the arbitration agreement specifically or in conjunction with other terms of the contract containing such agreement, and irrespective of whether the agreement purports to delegate such determinations to an arbitrator.

''(2) COLLECTIVE BARGAINING AGREEMENTS.—Nothing in this chapter shall apply to any arbitration provision in a contract between an employer and a labor organization or between labor organizations, except that no such arbitration provision shall have the effect of waiving the right of a worker to seek judicial enforcement of a right arising under a provision of the Constitution of the United States, a State constitution, or a Federal or State statute, or public policy arising therefrom.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) IN GENERAL.—Title 9, United States Code, is amended—

(A) in section 1 by striking ''of seamen,'' and all that follows through ''interstate commerce'' and inserting ''persons and causes of action under chapter 43 of title 38 or the Servicemembers Civil Relief Act (50 U.S.C. 3901 et seq.)'';

(B) in section 2 by inserting ''or as otherwise provided in chapter 4'' before the period at the end;

(C) in section 208—

(i) in the section heading, by striking ''**Chapter 1; residual application**'' and inserting ''**Application**''; and

(ii) by adding at the end the following: ''This chapter applies to the extent that this chapter is not in conflict with chapter 4.''; and

(D) in section 307—

(i) in the section heading, by striking ''**Chapter 1; residual application**'' and inserting ''**Application**''; and

(ii) by adding at the end the following: ''This chapter applies to the extent that this chapter is not in conflict with chapter 4.''.

(2) TABLE OF SECTIONS.—

(A) CHAPTER 2.—The table of sections for chapter 2 of title 9, United States Code, is amended by striking the item relating to section 208 and inserting the following:

''208. Application.''.

(B) CHAPTER 3.—The table of sections for chapter 3 of title 9, United States Code, is amended by striking the item relating to section 307 and inserting the following:

''307. Application.''.

(3) TABLE OF CHAPTERS.—The table of chapters of title 9, United States Code, is amended by adding at the end the following:

''4. Arbitration of servicemember and veteran disputes ..... 401''.

SEC. 6____. LIMITATION ON WAIVER OF RIGHTS AND PROTECTIONS UNDER SERVICEMEMBERS CIVIL RELIEF ACT.

(a) AMENDMENTS.—Section 107(a) of the Servicemembers Civil Relief Act (50 U.S.C. 3918(a)) is amended—

(1) in the second sentence, by inserting ''and if it is made after a specific dispute has arisen and the dispute is identified in the waiver'' before the period at the end; and

(2) in the third sentence by inserting ''and if it is made after a specific dispute has arisen and the dispute is identified in the waiver'' before the period at the end.

(b) APPLICATION OF AMENDMENTS.—The amendments made by subsection (a) shall apply with respect to waivers made on or after the date of the enactment of this Act.

SEC. 6____. APPLICABILITY.

This subtitle, and the amendments made by this subtitle, shall apply with respect to any dispute or claim that arises or accrues on or after the date of the enactment of this Act.

SA 4664. 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 D of title VIII, add the following:

SEC. 844. UNFUNDED SMALL BUSINESS INNOVATION RESEARCH PROJECTS.

(a) IN GENERAL.—Not later than 10 days after the date on which the budget of the President for a fiscal year is submitted to Congress pursuant to section 1105 of title 31, United States Code, each Secretary of a military department and the Under Secretary of Defense for Research and Engineering shall submit to the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the congressional defense committees a report on unfunded priorities of the Department of Defense related to high priority Small Business Innovation Research and Small Business Technology Transfer projects.

(b) ELEMENTS.—

(1) IN GENERAL.—Each report under subsection (a) shall include identification of not more than five unfunded priority projects, with information for each project covered by such report, including the following information:

(A) A summary description of such priority, including the objectives to be achieved if such priority were to be funded (whether in whole or in part).

(B) The additional amount of funds recommended in connection with the objectives identified under subparagraph (A).

(C) Account information with respect to such priority, including, as applicable, the following:

(i) Line item number, in the case of applicable procurement accounts.

(ii) Program element number, in the case of applicable research, development, test, and evaluation accounts.

(iii) Sub-activity group, in the case of applicable operation and maintenance accounts.

(2) PRIORITY ORDER.—Each Secretary shall ensure that the unfunded priorities covered by a report under subsection (a) are listed in the order of urgency of priority, as determined by the Under Secretary.

(c) UNFUNDED PRIORITY DEFINED.—In this section, the term ''unfunded priority'', with respect to a fiscal year, means a project related to a successful project funded under Phase Two of the Small Business Innovation Research or Small Business Technology Transfer program that—

(1) is not funded in the budget of the President for that fiscal year, as submitted to Congress pursuant to section 1105 of title 31, United States Code;

(2) has the potential to—

(A) advance the national security capabilities of the United States;

(B) provide new technologies or processes, or new applications of existing technologies, that will enable new alternatives to existing programs; and

(C) provide future cost savings; and

(3) would have been recommended for funding through the budget referred to in paragraph (1) if—

(A) additional resources had been available for the budget to fund the program, activity, or mission requirement; or

(B) the program, activity, or mission requirement had emerged before the budget was formulated.

SA 4665. 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 end of subtitle E of title VIII, add the following:

SEC. 857. AIR FORCE STRATEGY FOR ACQUISITION OF COMBAT RESCUE AIRCRAFT AND EQUIPMENT.

The Secretary of the Air Force shall submit to the congressional defense committees a strategy for the Department of the Air Force for the acquisition of combat rescue aircraft and equipment that aligns with the stated capability and capacity requirements of the Air Force to meet the national defense strategy (required under section 113(g) of title 10, United States Code), taking into account regional strategies such as those relating to the Indo-Pacific and Arctic regions.

SA 4666. Mr. SULLIVAN (for himself, Mr. KING, and Ms. HIRONO) 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. BRIEFING ON PROGRAMMING AND BUDGETING FOR THE PACIFIC DETERRENCE INITIATIVE.

(a) BRIEFING.—Not later than 60 days after the date of the enactment of this Act, the Deputy Secretary of Defense shall provide to the congressional defense committees a briefing on the processes and guidance used to program and budget for the Pacific Deterrence Initiative, including—

(1) the allocation of fiscal toplines in the program objective memorandum process to support the Pacific Deterrence Initiative at the outset of the process;

(2) the role of the combatant commanders in setting requirements for the Pacific Deterrence Initiative;

(3) the role of the military departments and other components of the Armed Forces in proposing programmatic options to meet such requirements; and

(4) the role of the combatant commanders, the military departments and other components of the Armed Forces, the Cost Assessment and Program Evaluation Office, and the Deputy Secretary of Defense in adjudicating requirements and programmatic options—

(A) before the submission of the program objective memorandum for the Pacific Deterrence Initiative; and

(B) during program review.

(b) GUIDANCE.—In establishing program objective memorandum guidance for fiscal year 2024, the Deputy Secretary of Defense shall ensure that the processes and guidance used to program and budget the Pacific Deterrence Initiative align, as appropriate, with the processes and guidance used to program and budget for the European Deterrence Initiative, including through the allocation of fiscal toplines for each such initiative in the fiscal year 2024 process.

SA 4667. 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 the Navy, in consultation with the Chief of Naval Research, 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 4668. Mr. CRUZ (for himself, Mrs. GILLIBRAND, Ms. MURKOWSKI, Mr. COONS, Mr. CRAMER, Mr. HAWLEY, Mr. MARSHALL, Mr. LUJÁN, Ms. BALDWIN, Mr. BENNET, and Mr. HICKENLOOPER) 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. PROHIBITION ON LIMITING OF CERTAIN PARENTAL GUARDIANSHIP RIGHTS OF CADETS AND MIDSHIPMEN.

(a) PROHIBITION.—

(1) IN GENERAL.—The Secretary of Defense, the Secretary of Homeland Security, and the Secretary of Transportation, in consultation with the Secretaries of the military departments and the Superintendent of each Federal service academy, as appropriate, shall prescribe in regulations policies that include the option to preserve parental guardianship

rights of cadets and midshipmen are protected consistent with individual and academic responsibilities.

(2) DEVELOPMENT OF POLICY TO PROTECT PARENTAL RIGHTS.—

(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense, the Secretary of Homeland Security, and the Secretary of Transportation shall implement a policy that includes the option to preserve the parental rights of Federal service academy students who become pregnant or father a child while attending a Federal service academy.

(B) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, the Secretary of Homeland Security, and the Secretary of Transportation shall submit to the congressional defense committees a report on the legislative changes needed to support the policy developed pursuant to paragraph (1).

(3) OPTIONS FOR PREGNANT CADETS AND MIDSHIPMEN.—The regulations prescribed under paragraph (1) shall provide that females who become pregnant while enrolled at a Federal service academy shall have, at a minimum, the following options to be elected by the cadet or midshipman:

(A) At the conclusion of the current semester or when otherwise deemed medically appropriate, the individual may take an unpaid leave of absence from the Federal service academy for up to one year followed by a return to full cadet or midshipman status (if remaining otherwise qualified).

(B) Seek a transfer to a university with a Reserve Officer Training Program for military service under the military department concerned.

(C) Full release from the Federal service academy and any service or financially related obligations, regardless of commitment status.

(D) Enlistment in military active-duty service, with all of the attendant benefits.

(4) TREATMENT OF MALES WHO FATHER A CHILD WHILE ENROLLED AT A FEDERAL SERVICE ACADEMY.—The regulations prescribed under paragraph (1) shall provide for the following policies regarding males who may father a child while enrolled at a Federal service academy:

(A) Academy leadership shall establish policies to allow cadets and midshipmen at least two weeks of leave to attend the birth, which must be used in conjunction with the birth; and

(B) The academy shall provide the father the same options available to a cadet or midshipman who becomes a mother while enrolled by selecting one of the options outlined in subparagraphs (B) and (C) of paragraph (3).

(b) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as requiring or providing for the changing of admission requirements at any of the Federal service academies.

(c) FEDERAL SERVICE ACADEMY DEFINED.—In this section, the term ''Federal service academy'' means the following:

(1) The United States Military Academy, West Point, New York.

(2) The United States Naval Academy, Annapolis, Maryland.

(3) The United States Air Force Academy, Colorado Springs, Colorado.

(4) The United States Coast Guard Academy, New London, Connecticut.

(5) The United States Merchant Marine Academy, Kings Point, New York.

SA 4669. Mr. TOOMEY (for himself and Mr. CARDIN) 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—Iran Sanctions

SEC. 1291. SHORT TITLE.

This subtitle may be cited as the ''Masih Alinejad Harassment and Unlawful Targeting Act of 2021'' or the ''Masih Alinejad HUNT Act''.

SEC. 1292. FINDINGS.

Congress finds that the Government of the Islamic Republic of Iran surveils, harasses, terrorizes, tortures, abducts, and murders individuals who peacefully defend human rights and freedoms in Iran, and innocent entities and individuals considered by the Government of Iran to be enemies of that regime, including United States citizens on United States soil, and takes foreign nationals hostage, including in the following instances:

(1) In 2021, Iranian intelligence agents were indicted for plotting to kidnap United States citizen, women's rights activist, and journalist Masih Alinejad, from her home in New York City, in retaliation for exercising her rights under the First Amendment to the Constitution of the United States. Iranian agents allegedly spent at least approximately half a million dollars to capture the outspoken critic of the authoritarianism of the Government of Iran, and studied evacuating her by military-style speedboats to Venezuela before rendition to Iran.

(2) Prior to the New York kidnapping plot, Ms. Alinejad's family in Iran was instructed by authorities to lure Ms. Alinejad to Turkey. In an attempt to intimidate her into silence, the Government of Iran arrested 3 of Ms. Alinejad's family members in 2019, and sentenced her brother to 8 years in prison for refusing to denounce her.

(3) According to Federal prosecutors, the same Iranian intelligence network that allegedly plotted to kidnap Ms. Alinejad is also targeting critics of the Government of Iran who live in Canada, the United Kingdom, and the United Arab Emirates.

(4) In 2021, an Iranian diplomat was convicted in Belgium of attempting to carry out a 2018 bombing of a dissident rally in France.

(5) In 2021, a Danish high court found a Norwegian citizen of Iranian descent guilty of illegal espionage and complicity in a failed plot to kill an Iranian Arab dissident figure in Denmark.

(6) In 2021, the British Broadcasting Corporation (BBC) appealed to the United Nations to protect BBC Persian employees in London who suffer regular harassment and threats of kidnapping by Iranian government agents.

(7) In 2021, 15 militants allegedly working on behalf of the Government of Iran were arrested in Ethiopia for plotting to attack citizens of Israel, the United States, and the United Arab Emirates, according to United States officials.

(8) In 2020, Iranian agents allegedly kidnapped United States resident and Iranian-German journalist Jamshid Sharmahd, while he was traveling to India through Dubai. Iranian authorities announced they had seized Mr. Sharmahd in ''a complex operation'', and paraded him blindfolded on state television. Mr. Sharmahd is arbitrarily detained in Iran, allegedly facing the death penalty. In 2009, Mr. Sharmahd was the target of an alleged Iran-directed assassination plot in Glendora, California.

(9) In 2020, the Government of Turkey released counterterrorism files exposing how Iranian authorities allegedly collaborated with drug gangs to kidnap Habib Chabi, an Iranian-Swedish activist for Iran's Arab minority. In 2020, the Government of Iran allegedly lured Mr. Chabi to Istanbul through a female agent posing as a potential lover. Mr. Chabi was then allegedly kidnapped from Istanbul, and smuggled into Iran where he faces execution, following a sham trial.

(10) In 2020, a United States-Iranian citizen and an Iranian resident of California pleaded guilty to charges of acting as illegal agents of the Government of Iran by surveilling Jewish student facilities, including the Hillel Center and Rohr Chabad Center at the University of Chicago, in addition to surveilling and collecting identifying information about United States citizens and nationals who are critical of the Iranian regime.

(11) In 2019, 2 Iranian intelligence officers at the Iranian consulate in Turkey allegedly orchestrated the assassination of Iranian dissident journalist Masoud Molavi Vardanjani, who was shot while walking with a friend in Istanbul. Unbeknownst to Mr. Molavi, his ''friend'' was in fact an undercover Iranian agent and the leader of the killing squad, according to a Turkish police report.

(12) In 2019, around 1,500 people were allegedly killed amid a less than 2 week crackdown by security forces on anti-government protests across Iran, including at least an alleged 23 children and 400 women.

(13) In 2019, Iranian operatives allegedly lured Paris-based Iranian journalist Ruhollah Zam to Iraq, where he was abducted, and hanged in Iran for sedition.

(14) In 2019, a Kurdistan regional court convicted an Iranian female for trying to lure Voice of America reporter Ali Javanmardi to a hotel room in Irbil, as part of a foiled Iranian intelligence plot to kidnap and extradite Mr. Javanmardi, a critic of the Government of Iran.

(15) In 2019, Federal Bureau of Investigation agents visited the rural Connecticut home of Iran-born United States author and poet Roya Hakakian to warn her that she was the target of an assassination plot orchestrated by the Government of Iran.

(16) In 2019, the Government of Denmark accused the Government of Iran of directing the assassination of Iranian Arab activist Ahmad Mola Nissi, in The Hague, and the assassination of another opposition figure, Reza Kolahi Samadi, who was murdered near Amsterdam in 2015.

(17) In 2018, German security forces searched for 10 alleged spies who were working for Iran's al-Quds Force to collect information on targets related to the local Jewish community, including kindergartens.

(18) In 2017, Germany convicted a Pakistani man for working as an Iranian agent to spy on targets including a former German lawmaker and a French-Israeli economics professor.

(19) In 2012, an Iranian American pleaded guilty to conspiring with members of the Iranian military to bomb a popular Washington, D.C., restaurant with the aim of assassinating the ambassador of Saudi Arabia to the United States.

(20) In 1996, agents of the Government of Iran allegedly assassinated 5 Iranian dissident exiles across Turkey, Pakistan, and Baghdad, over a 5-month period that year.

(21) In 1992, the Foreign and Commonwealth Office of the United Kingdom expelled 2 Iranians employed at the Iranian Embassy in London and a third Iranian on a

student visa amid allegations they were plotting to kill Indian-born British American novelist Salman Rushdie, pursuant to the fatwa issued by then supreme leader of Iran, Ayatollah Ruhollah Khomeini.

(22) In 1992, 4 Iranian Kurdish dissidents were assassinated at a restaurant in Berlin, Germany, allegedly by Iranian agents.

(23) In 1992, singer, actor, poet, and gay Iranian dissident Fereydoun Farrokhzad was found dead with multiple stab wounds in his apartment in Germany. His death is allegedly the work of Iran-directed agents.

(24) In 1980, Ali Akbar Tabatabaei, a leading critic of Iran and then president of the Iran Freedom Foundation, was murdered in front of his Bethesda, Maryland, home by an assassin disguised as a postal courier. The Federal Bureau of Investigation had identified the ''mailman'' as Dawud Salahuddin, born David Theodore Belfield. Mr. Salahuddin was working as a security guard at an Iranian interest office in Washington, D.C., when he claims he accepted the assignment and payment of $5,000 from the Government of Iran to kill Mr. Tabatabaei.

(25) Other exiled Iranian dissidents alleged to have been victims of the Government of Iran's murderous extraterritorial campaign include Shahriar Shafiq, Shapour Bakhtiar, and Gholam Ali Oveissi.

(26) Iranian Americans face an ongoing campaign of intimidation both in the virtual and physical world by agents and affiliates of the Government of Iran, which aims to stifle freedom of expression and eliminate the threat Iranian authorities believe democracy, justice, and gender equality pose to their rule.

SEC. 1293. 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 Banking, Housing, and Urban Affairs and the Committee on Foreign Relations of the Senate; and

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

(3) CORRESPONDENT ACCOUNT; PAYABLE-THROUGH ACCOUNT.—The terms ''correspondent account'' and ''payable-through account'' have the meanings given those terms in section 5318A of title 31, United States Code.

(4) FOREIGN FINANCIAL INSTITUTION.—The term ''foreign financial institution'' has the meaning of that term as determined by the Secretary of the Treasury pursuant to section 104(i) of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (22 U.S.C. 8513(i)).

(5) FOREIGN PERSON.—The term ''foreign person'' means any individual or entity that is not a United States person.

(6) 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. 1294. REPORT AND IMPOSITION OF SANCTIONS WITH RESPECT TO PERSONS WHO ARE RESPONSIBLE FOR OR COMPLICIT IN ABUSES TOWARD DISSIDENTS ON BEHALF OF THE GOVERNMENT OF IRAN.

(a) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 45 days after the date of the enactment of this Act, the Secretary of State, in consultation with the Secretary of the Treasury, the Director of National Intelligence, and the Attorney General, shall submit to the appropriate congressional committees a report that—

(A) includes a detailed description and assessment of—

(i) the state of human rights and the rule of law inside Iran, including the rights and well-being of women, religious and ethnic minorities, and the LGBTQ community in Iran;

(ii) actions taken by the Government of Iran during the year preceding submission of the report to target and silence dissidents both inside and outside of Iran who advocate for human rights inside Iran;

(iii) the methods used by the Government of Iran to target and silence dissidents both inside and outside of Iran; and

(iv) the means through which the Government of Iran finances efforts to target and silence dissidents both inside and outside of Iran;

(B) identifies foreign persons working as part of the Government of Iran or acting on behalf of that Government (including members of paramilitary organizations such as Ansar-e-Hezbollah and Basij-e Mostaz'afin), that the Secretary of State determines, based on credible evidence, are knowingly responsible for, complicit in or involved in ordering, conspiring, planning or implementing the surveillance, harassment, kidnapping, illegal extradition, imprisonment, torture, killing, or assassination of citizens of Iran (including citizens of Iran of dual nationality) and citizens of the United States both inside and outside Iran who seek—

(i) to expose illegal or corrupt activity carried out by officials of the Government of Iran;

(ii) to obtain, exercise, defend, or promote internationally recognized human rights and freedoms, such as the freedoms of religion, expression, association, and assembly, and the rights to a fair trial and democratic elections, in Iran; or

(iii) to obtain, exercise, defend, or promote the rights and well-being of women, religious and ethnic minorities, and the LGBTQ community in Iran; and

(C) includes, for each foreign person identified subparagraph (B), a clear explanation for why the foreign person was so identified.

(2) UPDATES OF REPORT.—The report required by paragraph (1) shall be updated, and the updated version submitted to the appropriate congressional committees, during the 10-year period following the date of the enactment of this Act—

(A) not less frequently than annually; and

(B) with respect to matters relating to the identification of foreign persons under paragraph (1)(B), on an ongoing basis as new information becomes available.

(3) FORM OF REPORT.—

(A) IN GENERAL.—Each report required by paragraph (1) and each update required by paragraph (2) shall be submitted in unclassified form but may include a classified annex.

(B) PUBLIC AVAILABILITY.—The Secretary of State shall post the unclassified portion of each report required by paragraph (1) and each update required by paragraph (2) on a publicly available internet website of the Department of State.

(b) IMPOSITION OF SANCTIONS.—In the case of a foreign person identified under paragraph (1)(B) of subsection (a) in the most recent report or update submitted under that subsection, the President shall—

(1) if the foreign person meets the criteria for the imposition of sanctions under subsection (a) of section 1263 of the Global Magnitsky Human Rights Accountability Act (subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note), impose sanctions under subsection (b) of that section; and

(2) if the foreign person does not meet such criteria, impose the sanctions described in subsection (c).

(c) SANCTIONS DESCRIBED.—The sanctions to be imposed under this subsection with respect to a foreign person are the following:

(1) BLOCKING OF PROPERTY.—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 the 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) INELIGIBILITY FOR VISAS, ADMISSION, OR PAROLE.—

(A) IN GENERAL.—

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

(ii) CURRENT VISAS REVOKED.—

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

(II) IMMEDIATE EFFECT.—A revocation under subclause (I) shall—

(aa) take effect immediately; and

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

(d) TERMINATION OF SANCTIONS.—The President may terminate the application of sanctions under this section with respect to a person if the President determines and reports to the appropriate congressional committees, not later than 15 days before the termination of the sanctions that—

(1) credible information exists that the person did not engage in the activity for which sanctions were imposed;

(2) the person has been prosecuted appropriately for the activity for which sanctions were imposed; or

(3) the person has—

(A) credibly demonstrated a significant change in behavior;

(B) has paid an appropriate consequence for the activity for which sanctions were imposed; and

(C) has credibly committed to not engage in an activity described in subsection (a) in the future.

SEC. 1295. REPORT AND IMPOSITION OF SANCTIONS WITH RESPECT TO FOREIGN FINANCIAL INSTITUTIONS CONDUCTING SIGNIFICANT TRANSACTIONS WITH PERSONS RESPONSIBLE FOR OR COMPLICIT IN ABUSES TOWARD DISSIDENTS ON BEHALF OF THE GOVERNMENT OF IRAN.

(a) REPORT REQUIRED.—

(1) IN GENERAL.—Not earlier than 30 days and not later than 60 days after the Secretary of State submits to the appropriate congressional committees a report required by section 1294(a), the Secretary of the Treasury, in consultation with the Secretary of State, shall submit to the appropriate congressional committees a report that identifies any foreign financial institution that knowingly conducts a significant transaction with a foreign person identified in the report submitted under section 1294(a).

(2) FORM OF REPORT.—

(A) IN GENERAL.—Each report required by paragraph (1) shall be submitted in unclassified form but may include a classified annex.

(B) PUBLIC AVAILABILITY.—The Secretary of the Treasury shall post the unclassified portion of each report required by paragraph (1) on a publicly available internet website of the Department of the Treasury.

(b) IMPOSITION OF SANCTIONS.—The Secretary of the Treasury may prohibit the opening, or prohibit or impose strict conditions on the maintaining, in the United States of a correspondent account or a payable-through account by a foreign financial institution identified under subsection (a)(1).

SEC. 1296. EXCEPTIONS; WAIVERS; IMPLEMENTATION.

(a) EXCEPTIONS.—

(1) EXCEPTION FOR INTELLIGENCE, LAW ENFORCEMENT, AND NATIONAL SECURITY ACTIVITIES.—Sanctions under sections 1294 and 1295 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 section 1294(c)(2) 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 subtitle, the authorities and requirements to impose sanctions authorized 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 application of sanctions under section 1294 with respect to a person if the President—

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

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

(c) 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 subtitle.

(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of section 1294(b)(1) or 1295(b) or any regulation, license, or order issued to carry out either such 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.

SA 4670. 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 XII, add the following:

SEC. 1283. REMOVAL OF MEMBERS OF THE UNITED NATIONS HUMAN RIGHTS COUNCIL THAT COMMIT HUMAN RIGHTS ABUSES.

The President shall direct the Permanent Representative of the United States to the United Nations to use the voice, vote, and influence of the United States—

(1) to reform the process for removing members of the United Nations Human Rights Council that commit gross and systemic violations of human rights, including—

(A) lowering the threshold vote at the United Nations General Assembly for removal to a simple majority;

(B) ensuring that information detailing the member country's human rights record is publicly available before the vote on removal; and

(C) making the vote of each country on the removal from the United Nations Human Rights Council publicly available;

(2) to reform the rules on electing members to the United Nations Human Rights Council to ensure that United Nations members which have committed gross and systemic violations of human rights are not elected to the Human Rights Council; and

(3) to oppose the election to the Human Rights Council of any United Nations member—

(A) that is currently designated as—

(i) a country engaged in a consistent pattern of gross violations of internationally recognized human rights pursuant to section 116 or section 502B of the Foreign Assistance Act of 1961 (22 U.S.C. 2151n and 2304);

(ii) a state sponsor of terrorism; or

(iii) a Tier 3 country under the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7101 et seq.);

(B) the government of which is identified on the list published by the Secretary of State pursuant to section 404(b) of the Child Soldiers Prevention Act of 2008 (22 U.S.C. 2370c–1(b)) as a government that recruits and uses child soldiers; or

(C) the government of which the United States determines to have committed genocide or crimes against humanity.

SA 4671. Mr. TOOMEY (for himself and Mr. CASEY) 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 II, add the following:

SEC. 246. BRIEFING ON ADDITIVE MANUFACTURING CAPABILITIES.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Army Combat Capabilities Development Command shall brief the congressional defense committees on—

(1) current research and development activities to leverage robotics, autonomy, and artificial intelligence to enhance additive manufacturing capabilities in forward-deployed, expeditionary bases; and

(2) courses of action being considered to successfully transition additive manufacturing capabilities into sustained operational capabilities.

(b) ELEMENTS.—The briefing required by subsection (a) shall include the following:

(1) A summary of research advances and innovations in expeditionary manufacturing enabled by past investments combining artificial intelligence and additive manufacturing.

(2) A summary of plans and ongoing activities to engage with operational programs and programs of record to ensure that such advances and innovations can be successfully transitioned and supported to maximize mission readiness and force resiliency.

(3) An assessment of the feasibility of initiating pilot programs between institutions of higher education, the defense industrial base, and the Army Combat Capabilities Development Command related to experimentation and demonstrations of expeditionary manufacturing techniques.

SA 4672. 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 end of subtitle G of title X, add the following:

SEC. 1064. SYSTEM FOR ELECTRONIC SUBMISSION OF COMPLAINTS ABOUT THE DELIVERY OF HEALTH CARE SERVICES BY THE DEPARTMENT OF VETERANS AFFAIRS.

Section 7309A(c) of title 38, United States Code, is amended by adding at the end the following new paragraph:

''(3) Beginning not later than 18 months after the date of the enactment of this paragraph, the Director shall establish an information technology system that will allow a veteran (or the designated representative of a veteran) to electronically—

''(A) file a complaint that will be received by the appropriate patient advocate; and

''(B) at any time view the status of the complaint, including interim and final actions that have been taken to address the complaint.''.

SA 4673. Mr. PETERS (for himself and Mr. PORTMAN) 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.—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. 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 4674. Mr. PETERS (for himself and Mr. PORTMAN) 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 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).

SA 4675. Mr. SULLIVAN 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 VIII, add the following:

SEC. 857. PROHIBITION ON CONTRACTS THAT BENEFIT CHINESE COMMUNIST PARTY.

(a) IN GENERAL.—The Secretary of Defense may not enter into a contract for defense articles or services that are—

(1) developed or manufactured by, or include parts from, the Chinese Communist Party;

(2) provided by an entity that has suspected ties to the Chinese Communist Party; or

(3) provided by an entity that provides defense articles or services, including research, engineering, and technology, to the Chinese Communist Party.

(b) DEFENSE ARTICLES OR SERVICES DEFINED.—In this section, the term ''defense articles or services'' means defense articles or services designated by the President under section 38(a)(1) of the Arms Export Control Act (22 U.S.C. 2778(a)(1)).

SA 4676. Ms. KLOBUCHAR 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:

SEC. _____. VETERANS CYBERSECURITY AND DIGITAL LITERACY GRANT PROGRAM.

(a) FINDINGS.—Congress finds the following:

(1) Adversaries from Russia, China, and Iran are using information warfare to influence democracies across the world, and extremist organizations often use digital communications to recruit members. Influence campaigns from foreign adversaries reached tens of millions of voters during the 2016 and 2018 elections with racially and divisively targeted messages. The Unites States can fight these influences by ensuring that citizens of the United States possess the necessary skills to discern disinformation and misinformation and protect themselves from foreign influence campaigns.

(2) Researchers have documented persistent, pervasive, and coordinated online targeting of members of the Armed Forces, veterans, and their families by foreign adversaries seeking to undermine United States democracy in part because of public trust placed in these communities.

(3) A 2017 report by the University of Oxford's Graphika Institute, titled ''Social Media Disinformation Campaigns Against US Military Personnel and Veterans'', concluded that ''The pubic tends to place trust in military personnel and veterans, making them potentially influential voters and community leaders. Given this trust and their role in ensuring national security, these individuals have the potential to become particular targets for influence operations and information campaigns conducted on social media. There are already reports of US service personnel being confronted by foreign intelligence agencies while posted abroad, with details of their personal lives gleaned from social media.''.

(4) The Select Committee on Intelligence of the Senate found in its investigation of the interference in the 2016 election that social media posts by the Internet Research Agency (IRA) of Russia reached tens of millions of voters in 2016 and were meant to pit the people of the United States against one another and sow discord. Volume II of the Committee's investigation found that the Internet Research Agency's Instagram account with the second largest reach used the handle ''@american.veterans'' and was ''aimed at patriotic, conservative audiences, collected 215,680 followers, and generated nearly 18.5 million engagements.''.

(5) A 2019 investigative report by the Vietnam Veterans of America (VVA) titled ''An Investigation into Foreign Entities who are Targeting Troops and Veterans Online'', found that the Internet Research Agency targeted veterans and the followers of several congressionally chartered veterans service organizations with at least 113 advertisements during and following the 2016 election and that ''this represents a fraction of the Russian activity that targeted this community with divisive propaganda.''. The report also found that foreign actors have been impersonating veterans through social-media accounts and interacting with veterans and veterans groups on social media to spread propaganda and disinformation. To counter these acts, Vietnam Veterans of America recommended that the Department of Veterans Affairs ''immediately develop plans to make the cyber-hygiene of veterans an urgent priority within the Department of Veterans Affairs. The VA must educate and train veterans on personal cybersecurity: how to mitigate vulnerabilities, vigilantly maintain safe practices, and recognize threats, including how to identify instances of online manipulation.''.

(6) The Cyberspace Solarium Commission, a bicameral and bipartisan commission, established by section 1652 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232), concluded in its finished report that the ''U.S. government should promote digital literacy, civics education, and public awareness to build societal resilience to foreign, malign cyber-enabled information operations and that the U.S. government must ensure that individual Americans have both the digital literacy tools and the civics education they need to secure their networks and their democracy from cyber-enabled information operations.''. The report recommended that Congress authorizing grant programs to do this.

(b) SENSE OF CONGRESS.—It is the sense of Congress that, given the threat foreign influence campaigns pose for United States democracy and the findings and recommendations of Congress and experts, Congress must immediately act to pass legislative measures

to increase digital and media literacy as well as cyber-hygiene among veterans.

(c) PROGRAM REQUIRED.—The Secretary shall establish a program to promote digital citizenship and media literacy, through which the Secretary shall award grants to eligible entities to enable those eligible entities to carry out the activities described in subsection (e).

(d) APPLICATION.—An eligible entity seeking a grant under the program required by subsection (c) shall submit to the Secretary an application therefor at such time, in such manner, and containing such information as the Secretary may require, including, at a minimum the following:

(1) A description of the activities the eligible entity intends to carry out with the grant funds.

(2) An estimate of the costs associated with such activities.

(3) Such other information and assurances as the Secretary may require.

(e) ACTIVITIES.—An eligible entity shall use the amount of a grant awarded under the program required by subsection (c) to carry out one or more of the following activities to improve cyber-hygiene and increase digital and media literacy among veterans:

(1) Develop competencies in cyber-hygiene.

(2) Develop media literacy and digital citizenship competencies by promoting veterans'—

(A) research and information fluency;

(B) critical thinking and problem solving skills;

(C) technology operations and concepts;

(D) information and technological literacy;

(E) concepts of media and digital representation and stereotyping;

(F) understanding of explicit and implicit media and digital messages;

(G) understanding of values and points of view that are included and excluded in media and digital content;

(H) understanding of how media and digital content may influence ideas and behaviors;

(I) understanding of the importance of obtaining information from multiple media sources and evaluating sources for quality;

(J) understanding how information on digital platforms can be altered through algorithms, editing, and augmented reality;

(K) ability to create media and digital content in civically and socially responsible ways; and

(L) understanding of influence campaigns conducted by foreign adversaries and the tactics employed by foreign adversaries for conducting influence campaigns.

(f) REPORTING.—

(1) REPORTS BY GRANT RECIPIENTS.—Each recipient of a grant under the program required by subsection (c) shall, not later than one year after the date on which the recipient first receives funds pursuant to the grant, submit to the Secretary a report describing the activities the recipient carried out using grant funds and the effectiveness of those activities.

(2) REPORT BY THE SECRETARY.—Not later than 90 days after the date on which the Secretary receives the last report the Secretary expects to receive under paragraph (1), the Secretary shall submit to Congress a report describing the activities carried out under this section and the effectiveness of those activities.

(g) SENSE OF CONGRESS.—It is the sense of Congress that the Secretary should—

(1) establish and maintain a list of eligible entities that receive a grant under the program required by subsection (c), and individuals designated by those eligible entities as participating individuals; and

(2) make that list available to those eligible entities and participating individuals in order to promote communication and further exchange of information regarding sound digital citizenship and media literacy practices among recipients of grants under the program required by subsection (c).

(h) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $20,000,000 for fiscal year 2022.

(i) DEFINITIONS.—In this section:

(1) CYBER-HYGIENE.—The term ''cyber-hygiene'' means practices and steps that users of computers and other internet connected devices take to maintain and improve online security, maintain the proper functioning of computers devices, and protect computers and devices from cyberattacks and unauthorized use.

(2) DIGITAL CITIZENSHIP.—The term ''digital citizenship'' means the ability to—

(A) safely, responsibly, and ethically use communication technologies and digital information technology tools and platforms;

(B) create and share media content using principles of social and civic responsibility and with awareness of the legal and ethical issues involved; and

(C) participate in the political, economic, social, and cultural aspects of life related to technology, communications, and the digital world by consuming and creating digital content, including media.

(3) ELIGIBLE ENTITY.—The term ''eligible entity'' means—

(A) a civil society organization, including community groups, nongovernmental organizations, nonprofit organization, labor organizations, indigenous groups, charitable organizations, professional associations, and foundations; and

(B) congressionally chartered veterans service organizations.

(4) MEDIA LITERACY.—The term ''media literacy'' means the ability to—

(A) access relevant and accurate information through media in a variety of forms;

(B) critically analyze media content and the influences of different forms of media;

(C) evaluate the comprehensiveness, relevance, credibility, authority, and accuracy of information;

(D) make educated decisions based on information obtained from media and digital sources;

(E) operate various forms of technology and digital tools; and

(F) reflect on how the use of media and technology may affect private and public life.

(5) SECRETARY.—The term ''Secretary'' means the Secretary of Veterans Affairs.

SA 4677. Ms. KLOBUCHAR 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 A of title XII, add the following:

SEC. 1210. GLOBAL ELECTORAL EXCHANGE PROGRAM.

(a) SHORT TITLE.—This section may be cited as the ''Global Electoral Exchange Act of 2021''.

(b) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) recent elections globally have illustrated the urgent need for the promotion and exchange of international best election practices, particularly in the areas of cybersecurity, results transmission, transparency of electoral data, election dispute resolution, and the elimination of discriminatory registration practices and other electoral irregularities;

(2) the advancement of democracy worldwide promotes United States interests, as stable democracies provide new market opportunities, improve global health outcomes, and promote economic freedom and regional security;

(3) credible elections are the cornerstone of a healthy democracy and enable all persons to exercise their basic human right to have a say in how they are governed;

(4) inclusive elections strengthen the credibility and stability of democracies more broadly;

(5) at the heart of a strong election cycle is the professionalism of the election management body and an empowered civil society;

(6) the development of local expertise via peer-to-peer learning and exchanges promotes the independence of such bodies from internal and external influence; and

(7) supporting the efforts of peoples in democratizing societies to build more representative governments in their respective countries is in the national interest of the United States.

(c) GLOBAL ELECTORAL EXCHANGE.—

(1) IN GENERAL.—The Global Engagement Center (referred to in this section as the ''Center'') at the Department of State is authorized to establish and administer a Global Electoral Exchange Program (referred to in this section as the ''Program'') to promote the utilization of sound election administration practices around the world.

(2) PURPOSE.—The purpose of the Program shall include the promotion and exchange of international best election practices, including in the areas of—

(A) cybersecurity;

(B) the protection of election systems against influence campaigns;

(C) results transmission;

(D) transparency of electoral data;

(E) election dispute resolution;

(F) the elimination of discriminatory registration practices and electoral irregularities;

(G) inclusive and equitable promotion of candidate participation;

(H) equitable access to polling places, voter education information, and voting mechanisms (including by persons with disabilities); and

(I) other sound election administration practices.

(3) EXCHANGE OF ELECTORAL AUTHORITIES.—

(A) IN GENERAL.—The Center, in consultation, as appropriate, with the United States Agency for International Development, may award grants to any United States-based organization that—

(i) is described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code;

(ii) has experience in, and a primary focus on, foreign comparative election systems or subject matter expertise in the administration or integrity of such systems; and

(iii) submits an application in such form, and satisfying such requirements, as the Center may require.

(B) TYPES OF GRANTS.—An organization described in subparagraph (A) may receive a grant under this paragraph to design and implement programs that—

(i) bring to the United States election administrators and officials, including government officials, poll workers, civil society representatives, members of the judiciary, and others who participate in the organization and administration of public elections in a foreign country that faces challenges to

its electoral process to study election procedures in the United States for educational purposes; or

(ii) take election administrators and officials of the United States or of another country, including government officials, poll workers, civil society representatives, members of the judiciary, and others who participate in the organization and administration of public elections to another country to study and discuss election procedures in such country for educational purposes.

(C) LIMITS ON ACTIVITIES.—Activities administered under the Program may not—

(i) include observation of an election for the purposes of assessing the validity or legitimacy of that election;

(ii) facilitate any advocacy for a certain electoral result by a grantee when participating in the Program; or

(iii) be carried out without proper consultation with State and local authorities in the United States that administer elections.

(D) SENSE OF CONGRESS.—It is the sense of Congress that the Center should establish and maintain a network of Global Electoral Exchange Program alumni, to promote communication and further exchange of information regarding sound election administration practices among current and former Program participants.

(E) LIMITATION.—A recipient of a grant under the Program may only use such grant for the purpose for which such grant was awarded, unless otherwise authorized by the Center.

(F) NONDUPLICATIVE.—Grants made under this paragraph may not be duplicative of any other grants made under any other provision of law for similar or related purposes.

(4) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $5,000,000 for each of the fiscal years 2022 through 2026 to carry out this subsection.

(d) CONGRESSIONAL OVERSIGHT.—Not later than 1 year after the date of the enactment of this Act and annually thereafter for the following 2 years, the Center shall provide a briefing to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives regarding the status of any activities carried out pursuant to subsection (c) during the preceding year, which shall include—

(1) a summary of all exchanges conducted under the Global Electoral Exchange Program, including information regarding grantees, participants, and the locations where program activities were held;

(2) a description of the criteria used to select grantees under the Global Electoral Exchange Program; and

(3) recommendations for the improvement of the Global Electoral Exchange Program in furtherance of the purpose specified in subsection (c)(2).

SA 4678. Mr. SCHUMER (for himself and 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 appropriate place in title X, insert the following:

SEC. _____. COMPTROLLER GENERAL OF THE UNITED STATES STUDY ON OPPORTUNITIES FOR USE OF VETERANS EDUCATIONAL ASSISTANCE TO PURSUE CAREERS IN OUTDOOR RECREATION.

(a) STUDY REQUIRED.—The Comptroller General of the United States shall conduct a study on the use by veterans of educational assistance provided under laws administered by the Secretary of Veterans Affairs to pursue careers in outdoor recreation.

(b) ELEMENTS.—The study required by subsection (a) shall include the following:

(1) Identification of opportunities for veterans to use educational assistance provided under laws administered by the Secretary of Veterans Affairs to pursue careers in outdoor recreation in the private sector and in the public sector.

(2) Identification of any difficulties with using the educational assistance provided under laws administered by the Secretary to veterans to pursue careers in outdoor recreation in the private and public sector, including trained, apprentice, assistant, and certified guides.

(3) Assessment of the availability of opportunities for careers in outdoor recreation at the following:

(A) The Department of Agriculture.

(B) The Department of the Interior.

(C) The Army Corps of Engineers.

(D) The National Oceanic and Atmospheric Administration.

(4) Identification of any challenges veterans may have pursuing careers in outdoor recreation at the agencies list under paragraph (3).

(5) Identification of options to increase opportunities for veterans to pursue careers in outdoor recreation at the agencies listed under paragraph (3).

(c) STAKEHOLDER PERSPECTIVES.—In conducting the study required by subsection (a), the Comptroller General shall obtain the perspectives of the outdoor recreation industry, veterans groups focusing on the outdoors, nongovernmental organizations, and other interested stakeholders.

(d) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 240 days after the date of the enactment of this Act, the Comptroller General shall provide the Committee on Veterans' Affairs of the Senate and the Committee on Veterans' Affairs of the House of Representatives a briefing on the study required by subsection (a).

(2) REPORT.—After providing the briefing required by paragraph (1), the Comptroller General shall submit to the committees described in such paragraph a report on the findings of the Comptroller General with respect to the study completed under subsection (a).

(e) OUTDOOR RECREATION DEFINED.—In this section, the term ''outdoor recreation'' means recreational activities undertaken for pleasure that—

(1) generally involve some level of intentional physical exertion; and

(2) occur in nature-based environments outdoors.

SA 4679. 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 appropriate place, insert the following:

SEC. _____. TREATMENT OF HOURS WORKED UNDER A QUALIFIED TRADE-OF-TIME ARRANGEMENT.

Section 5542 of title 5, United States Code, is amended by adding at the end the following:

''(h)(1)(A) Notwithstanding any other provision of this section or section 5545b, any hours worked by a firefighter under a qualified trade-of-time arrangement shall be disregarded for purposes of any determination relating to eligibility for, or the amount of, any overtime pay under this section, including overtime pay under the Fair Labor Standards Act in accordance with subsection (c).

''(B) The Director of the Office of Personnel Management—

''(i) shall identify the situations in which a firefighter shall be deemed to have worked hours actually worked by a substituting firefighter under a qualified trade-of-time arrangement; and

''(ii) may adopt necessary policies governing the treatment of both a substituting and substituted firefighter under a qualified trade-of-time arrangement, without regard to how those firefighters would otherwise be treated under other provisions of law or regulation.

''(2) In this subsection—

''(A) the term 'firefighter' means an employee—

''(i) the work schedule of whom includes 24-hour duty shifts; and

''(ii) who—

''(I) is a firefighter, as defined in section 8331(21) or 8401(14);

''(II) in the case of an employee who holds a supervisory or administrative position and is subject to subchapter III of chapter 83, but who does not qualify to be considered a firefighter within the meaning of section 8331(21), would so qualify if such employee had transferred directly to such position after serving as a firefighter within the meaning of such section;

''(III) in the case of an employee who holds a supervisory or administrative position and is subject to chapter 84, but who does not qualify to be considered a firefighter within the meaning of section 8401(14), would so qualify if such employee had transferred directly to such position after performing duties described in section 8401(14)(A) and (B) for at least 3 years; and

''(IV) in the case of an employee who is not subject to subchapter III of chapter 83 or chapter 84, holds a position that the Office of Personnel Management determines would satisfy subclause (I), (II), or (III) if the employee were subject to subchapter III of chapter 83 or chapter 84; and

''(B) the term 'qualified trade-of-time arrangement' means an arrangement under which 2 firefighters who are subject to the supervision of the same fire chief agree, solely at their option and with the approval of the employing agency, to substitute for one another during scheduled work hours in the performance of work in the same capacity.''.

SA 4680. Mr. BENNET (for himself, Mr. HICKENLOOPER, and Mr. CRAMER) 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 A of title XV, add the following:

SEC. 1516. RESEARCH AND EDUCATIONAL ACTIVITIES TO SUPPORT SPACE TECHNOLOGY DEVELOPMENT.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Air Force and the Chief of Space Operations, in coordination with the Chief Technology and Innovation Office of the Space Force, may carry out research and educational activities to support space technology development.

(b) ACTIVITIES.—Activities carried out under subsection (a) shall support the research, development, and demonstration needs of the Space Force, including by addressing and facilitating the advancement of capabilities related to—

(1) space domain awareness;

(2) position, navigation, and timing;

(3) autonomy;

(4) data analytics;

(5) communications;

(6) space-based power generation;

(7) space applications for cybersecurity; and

(8) any other matter the Secretary of the Air Forces considers relevant.

(c) EDUCATION AND TRAINING.—Activities carried out under subsection (a) shall—

(1) promote education and training for students in order to support the future national security space workforce of the United States; and

(2) explore opportunities for international collaboration.

SA 4681. Mr. LUJÁN 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 VIII, insert the following:

SEC. 821. USE OF DOMESTICALLY SOURCED COMPONENTS IN DEPARTMENT OF DEFENSE SATELLITES.

(a) IN GENERAL.—Subchapter II of chapter 385 of title 10, United States Code, is amended by inserting after section 4864 the following new section:

''§ 4865. Domestic source requirement for certain satellite components

''(a) IN GENERAL.—The Secretary of Defense may not acquire a covered component for a Department of Defense satellite unless the covered component is manufactured in the United States.

''(b) WAIVER.—

''(1) IN GENERAL.—The Secretary may waive the prohibition under subsection (a) with respect to the acquisition of a covered component if the Secretary—

''(A) determines that—

''(i) no significant national security concerns regarding counterfeiting, quality, or unauthorized access would be created by waiving the prohibition;

''(ii) the acquisition of the covered component is required to support national security; and

''(iii) the covered component is not available from a source inside the United States of satisfactory quality, in sufficient quantity, in the required form, and at reasonable cost; and

''(B) submits to the congressional defense committees a report on the determination under subparagraph (A).

''(2) PROHIBITION ON ACQUISITION FROM COVERED NATIONS.—A waiver under paragraph (1) may not authorize the acquisition of a covered component from a covered nation.

''(c) APPLICABILITY.—This section applies respect to contracts entered into on or after October 1, 2022.

''(d) DEFINITIONS.—In this section:

''(1) COVERED COMPONENT.—The term 'covered component' means a space-qualified solar cell, cell-interconnect-coverglass (CIC) assembly, solar panel, or solar array.

''(2) COVERED NATION.—The term 'covered nation' means—

''(A) the Democratic People's Republic of North Korea;

''(B) the People's Republic of China;

''(C) the Russian Federation; and

''(D) the Islamic Republic of Iran.

''(3) DEPARTMENT OF DEFENSE SATELLITE.—The term 'Department of Defense satellite' means a satellite the principal purpose of which is to support the needs of the Department of Defense.''.

(b) CLERICAL AMENDMENT.—The table of sections for chapter 385 of such title is amended by inserting after the item relating to section 4864 the following new item:

''4865. Domestic source requirement for certain satellite components.''.

(c) EFFECTIVE DATE.—The amendments made by this section take effect on January 1, 2022.

SA 4682. Mr. RISCH 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. LIMITATION ON REMOVING GOVERNMENT OF CUBA FROM STATE SPONSORS OF TERRORISM LIST UNTIL PRESIDENT CERTIFIES CUBA NO LONGER PROVIDES SANCTUARY TO TERRORISTS.

The President may not remove Cuba from the list of state sponsors of terrorism until the President, without delegation, certifies and reports to Congress that the Government of Cuba has ceased to provide sanctuary to terrorists.

SA 4683. Mr. LANKFORD 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. DELAY OF COVID–19 VACCINE MANDATE FOR MEMBERS OF THE ARMED FORCES AND ADDITIONAL REQUIREMENTS RELATING TO VACCINE MANDATES.

(a) DELAY OF VACCINE MANDATE.—The Secretary of Defense may not require members of the Armed Forces to receive the vaccination for coronavirus disease 2019 (commonly known as ''COVID–19'') or penalize such members for not receiving such vaccine until the date on which all religious and medical accommodation requests seeking an exemption from such a requirement have been individually evaluated with a final determination and all appeal processes in connection with any such requests have been exhausted.

(b) PRIVATE RIGHT OF ACTION RELATING TO COVID–19 VACCINATION.—A member of the Armed Forces whose religious accommodation request relating to the vaccination for coronavirus disease 2019 is denied without written individualized consideration or consultation with the Office of the Chief of Chaplains for the military department concerned to confirm that there is a compelling interest in having the member receive such vaccination and that mandating vaccination is the least restrictive means of furthering that interest shall have a cause of action for financial damages caused by the harm to their military career, retirement, or benefits.

(c) CONSULTATION WITH OFFICES OF CHIEF OF CHAPLAINS REGARDING RELIGIOUS ACCOMMODATIONS.—

(1) IN GENERAL.—The final accommodation authority for each military department shall consult with the Office of the Chief of Chaplains for the military department concerned before denying any religious accommodation request.

(2) PROCEDURES FOR RELIGIOUS EXEMPTION REQUESTS.—The Secretary of Defense shall consult with the members of the Armed Forces Chaplains Board in determining the general procedure for processing religious exemption requests.

(3) DETERMINATIONS RELATING TO RELIGIOUS BELIEF OR CONSCIENCE.—No determinations shall be made regarding the sincerity of the religious belief or conscience of a member of the Armed Forces by the final accommodation authority without the documented consultation of a chaplain with the member.

(d) INSPECTOR GENERAL INVESTIGATION REGARDING RELIGIOUS ACCOMMODATIONS.—Not later than 60 days after the date of the enactment of this Act, the Inspector General of the Department of Defense shall complete an investigation into whether each of the military departments has complied with Federal law (including the Religious Freedom Restoration Act of 1993 (42 U.S.C. 2000bb et seq.)), Department of Defense Instruction 1300.17, and other policies of the military departments relevant to determining religious accommodations for vaccination requirements.

SA 4684. 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. ___. REQUIREMENT TO EXPEDITE REQUESTS FOR COST MODIFICATIONS TO DEPARTMENT OF DEFENSE CONTRACTS RESULTING FROM SUPPLY CHAIN CHALLENGES.

The Secretary of Defense shall expedite any request for a cost modification to a contract of the Department of Defense that results from supply chain challenges.

SA 4685. 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 Defense shall review access, metro, and long-haul passive optical fiber and optical fiber cable that is manufactured or produced by an entity owned or partially owned by the People's Republic of China for potential inclusion on the list of covered communications equipment pursuant to section 2 of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601).

(2) APPLICABILITY.—If the Secretary of Defense 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 should be included on the list, any such inclusion shall apply 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 Defense shall notify the congressional defense committees 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 Commerce 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 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 ''long haul'' means optical fiber and optical fiber cable that connects cities and metropolitan areas.

(3) The term ''metro'' means optical fiber and optical fiber cable that connects city business districts and central city and suburban areas.

(4) The term ''passive'' means unpowered optical fiber and optical fiber cable.

SA 4686. Mr. CORNYN (for himself and Mr. KING) 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:

SEC. ____. STUDY ON SUPPLY CHAINS CRITICAL TO NATIONAL SECURITY.

Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in coordination with the Director of the Central Intelligence Agency and the heads of such elements of the intelligence community as the Director of National Intelligence considers appropriate—

(1) complete a study—

(A) to identify—

(i) supply chains that are critical to the national security, economic security, or public health or safety of the United States; and

(ii) important vulnerabilities in such supply chains; and

(B) to develop recommendations for legislative or administrative action to secure the supply chains identified under subparagraph (A)(i); and

(2) submit to the congressional intelligence committees (as that term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), the Committee on Armed Services of the Senate, and the Committee on Armed Services of the House of Representatives the findings of the directors with respect to the study conducted under paragraph (1).

SA 4687. Mr. BENNET (for himself, Mr. HICKENLOOPER, and Mr. CRAMER) 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 A of title XV, add the following:

SEC. 1516. RESEARCH AND EDUCATIONAL ACTIVITIES TO SUPPORT SPACE TECHNOLOGY DEVELOPMENT.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Air Force and the Chief of Space Operations, in coordination with the Chief Technology and Innovation Office of the Space Force, may carry out research and educational activities to support space technology development.

(b) ACTIVITIES.—Activities carried out under subsection (a) shall support the research, development, and demonstration needs of the Space Force, including by addressing and facilitating the advancement of capabilities related to—

(1) space domain awareness;

(2) position, navigation, and timing;

(3) autonomy;

(4) data analytics;

(5) communications;

(6) space-based power generation;

(7) space applications for cybersecurity; and

(8) any other matter the Secretary of the Air Forces considers relevant.

(c) EDUCATION AND TRAINING.—Activities carried out under subsection (a) shall—

(1) promote education and training for students in order to support the future national security space workforce of the United States; and

(2) explore opportunities for international collaboration.

SA 4688. Ms. CORTEZ MASTO (for herself 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 appropriate place in title X, insert the following:

SEC. ____. NATIONAL SCIENCE AND TECHNOLOGY STRATEGY.

Title II of the National Science and Technology Policy, Organization, and Priorities Act of 1976 (42 U.S.C. 6611 et seq.) is amended by striking section 206 and inserting the following:

''SEC. 206. NATIONAL SCIENCE AND TECHNOLOGY STRATEGY.

''(a) STRATEGY REQUIRED.—Not later than the end of each calendar year immediately after the calendar year in which a review under section 206A(b) is completed, the Director of the Office of Science and Technology Policy, in consultation with the National Science and Technology Council, shall develop and submit to Congress a comprehensive national science and technology strategy of the United States to meet national research and development objectives for the following 4-year period (in this section referred to as the 'national science and technology strategy').

''(b) REQUIREMENTS.—Each national science and technology strategy required by subsection (a) shall delineate a national science and technology strategy consistent with—

''(1) the recommendations and priorities developed pursuant to the review most recently completed under section 206A(b);

''(2) the most recent national security strategy report submitted pursuant to section 1032 of the National Defense Authorization Act for Fiscal Year 2012 (50 U.S.C. 3043);

''(3) other relevant national plans; and

''(4) the strategic plans of relevant Federal departments and agencies.

''(c) CONSULTATION.—The Director of the Office of Science and Technology Policy shall consult, as necessary, with the Director of the Office of Management and Budget and other appropriate elements of the Executive Office of the President to ensure that the recommendations and priorities delineated in the science and technology strategy are incorporated in the development of annual budget requests.

''(d) ANNUAL REPORTS.—

''(1) IN GENERAL.—The President shall submit to Congress each year a comprehensive report on the national science and technology strategy of the United States.

''(2) CONTENTS.—Each report submitted under paragraph (1) shall include a description of the following:

''(A) The strategic objectives and priorities necessary to maintain the leadership of the United States in science and technology and to advance science and technology to address

societal and national challenges, including near-term, medium-term, and long-term research priorities.

''(B) The programs, policies, and activities that the President recommends across all Federal agencies to achieve the strategic objectives in subparagraph (A).

''(C) The global trends in science and technology, including potential threats to the leadership of the United States in science and technology and opportunities for international collaboration in science and technology.

''(e) PUBLICATION.—The Director shall, consistent to the maximum extent practicable with the protection of national security and other sensitive matters, make each report submitted under subsection (d) publicly available on an internet website of the Office of Science and Technology Policy.

''SEC. 206A. INTERAGENCY QUADRENNIAL INNOVATION AND TECHNOLOGY REVIEW.

''(a) DEFINITIONS.—In this section:

''(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term 'appropriate committees of Congress' means—

''(A) the Committee on Commerce, Science, and Transportation, the Committee on Armed Services, the Committee on Appropriations, the Committee on Environment and Public Works, the Committee on Foreign Relations, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

''(B) the Committee on Energy and Commerce, the Committee on Armed Services, the Committee on Appropriations, the Committee on Foreign Affairs, the Committee Science, Space, and Technology and the Committee on Homeland Security of the House of Representatives.

''(2) INTERAGENCY.—The term 'interagency' with respect to a review means that the review is conducted in consultation and coordination between Federal agencies, including the Department of Commerce, the Department of Transportation, the Department of Defense, the Department of Energy, the Environmental Protection Agency, and such other related agencies as the Director of the Office of Science and Technology Policy considers appropriate, as well as the following:

''(A) The National Science and Technology Council.

''(B) The President's Council of Advisors on Science and Technology.

''(C) The National Science Board.

''(D) the National Security Council.

''(E) The Council of Economic Advisers.

''(F) The National Economic Council.

''(G) The Domestic Policy Council.

''(H) The Office of the United States Trade Representative.

''(b) INTERAGENCY QUADRENNIAL INNOVATION AND TECHNOLOGY REVIEW REQUIRED.—

''(1) IN GENERAL.—Not later than 1 year after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2022, and every 4 years thereafter, the Director of the Office of Science and Technology Policy shall complete an interagency review of the science and technology enterprise of the United States (in this section referred to as the 'quadrennial innovation and technology review').

''(2) SCOPE.—The quadrennial science and technology review shall be a comprehensive examination of the science and technology strategy of the United States, including recommendations for maintaining global leadership in science and technology and advancing science and technology to address the societal and national challenges and guidance on the coordination of programs, assets, capabilities, budget, policies, and authorities across all Federal research and development programs.

''(3) CONSULTATION.—In carrying out each quadrennial innovation and technology review, the Director of the Office of Science and Technology Policy shall consult with the following:

''(A) Congress.

''(B) Federal agencies, including Federal agencies not described in subsection (a)(2).

''(C) Experts in national security.

''(D) Representatives of specific technology industries, as the Director considers appropriate.

''(E) Academics.

''(F) State, local, and Tribal governments.

''(G) Nongovernmental organizations.

''(H) The public.

''(c) CONTENTS.—In each quadrennial innovation and technology review, the Director shall—

''(1) provide an integrated view of, and recommendations for, science and technology policy across the Federal Government, while considering economic and national security and other societal and national challenges;

''(2) assess and recommend priorities for research, development, and demonstration programs to maintain American leadership in science and technology;

''(3) assess and recommend priorities for research, development, and demonstration programs to address societal and national challenges;

''(4) assess the global competition in science and technology and identify potential threats to the leadership of the United States in science and technology opportunities for international collaboration;

''(5) assess and make recommendations on the science, technology, engineering, mathematics, and computer science workforce in the United States;

''(6) assess and make recommendations to improve regional innovation across the United States;

''(7) assess and make recommendations to improve translation of basic research and the enhancement of technology transfer of federally funded research;

''(8) assess and identify the infrastructure and tools needed to maintain the leadership of the United States in science and technology and address other societal and national challenges; and

''(9) review administrative or legislative policies that affect the science and technology enterprise and identify and make recommendations on policies that hinder research and development in the United States.

''(d) COORDINATION.—The Director shall ensure that each quadrennial innovation and technology review conducted under this section is coordinated with efforts to carry out other relevant statutorily required reviews, and to the maximum extent practicable incorporates information and recommendations from other reviews in order to avoid duplication.

''(e) REPORTING.—

''(1) IN GENERAL.—Not later than December 31 of the year in which a quadrennial innovation and technology review is conducted, the Director shall submit to Congress a report of the review.

''(2) PUBLICATION.—The Director shall, consistent to the maximum extent possible with the protection of national security and other sensitive matters, make each report submitted under paragraph (1) publicly available on an internet website of the Office of Science and Technology Policy.''.

SA 4689. Mr. SCHUMER 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. 10___. INCLUSION ON THE VIETNAM VETERANS MEMORIAL WALL OF THE NAMES OF THE LOST CREW MEMBERS OF THE U.S.S. FRANK E. EVANS KILLED ON JUNE 3, 1969.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary of Defense shall authorize the inclusion on the Vietnam Veterans Memorial Wall in the District of Columbia of the names of the 74 crew members of the U.S.S. Frank E. Evans killed on June 3, 1969.

(b) REQUIRED CONSULTATION.—The Secretary of Defense shall consult with the Secretary of the Interior, the American Battlefield Monuments Commission, and other applicable authorities with respect to any adjustments to the nomenclature and placement of names pursuant to subsection (a) to address any space limitations on the placement of additional names on the Vietnam Veterans Memorial Wall.

(c) NONAPPLICABILITY OF COMMEMORATIVE WORKS ACT.—Chapter 89 of title 40, United States Code (commonly known as the ''Commemorative Works Act''), shall not apply to any activities carried out under subsection (a) or (b).

SA 4690. Mr. SULLIVAN 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. DISCLOSURES REQUIRED BY UNITED STATES FINANCIAL INSTITUTIONS INVESTING IN PEOPLE'S REPUBLIC OF CHINA.

(a) IN GENERAL.—The Secretary of Defense shall—

(1) require any United States financial institution that makes an investment described subsection (b) to disclose the amount and purpose, and potential impacts on the national defense, of such investments to the Secretary on an annual basis; and

(2) make such disclosures available to the public.

(b) INVESTMENTS DESCRIBED.—An investment described in this subsection is a monetary investment, in an amount that exceeds a threshold to be determined by the Secretary, directly or indirectly—

(1) to—

(A) the People's Republic of China;

(B) an entity owned or controlled by the Chinese Communist Party; or

(C) the People's Liberation Army; or

(2) for the benefit of any key industrial sector sponsored by the Chinese Communist Party.

(c) CONSOLIDATED REPORT.—Not less frequently than annually, the Secretary shall compile the disclosures submitted under subsection (a) and submit that compilation and

a summary of those disclosures to the congressional defense committees.

(d) REGULATIONS.—The Secretary shall prescribe such regulations as are necessary to carry out this section, which may include—

(1) requirements for documents and information to be submitted with disclosures required under subsection (a); and

(2) procedures for the determining the amount under subsection (b).

(e) UNITED STATES FINANCIAL INSTITUTION DEFINED.—In this section, the term ''United States financial institution'' means a financial institution (as defined in section 5312 of title 31, United States Code) organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such an institution.

SA 4691. 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 B of title X, add the following:

SEC. 1013. PROTECTING AMERICANS AGAINST FENTANYL AND OTHER SYNTHETIC OPIOIDS.

(a) STATEMENT OF POLICY.—It is the policy of the United States that all cabinet officials and other Government officers shall, in advancing American interests by working with other countries and international organizations, advocate for treating fentanyl and other synthetic opioids as weapons of mass destruction.

(b) HOMELAND SECURITY ACT OF 2002.—Section 1921 of the Homeland Security Act of 2002 (6 U.S.C. 591g) is amended by inserting ''fentanyl or synthetic opioid,'' after ''chemical,''.

(c) DEFENSE AGAINST WEAPONS OF MASS DESTRUCTION ACT OF 1996.—Section 1403(1) of the Defense Against Weapons of Mass Destruction Act of 1996 (50 U.S.C. 2302(1)) is amended—

(1) in subparagraph (B), by striking ''or'' at the end;

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

(3) by adding at the end the following:

''(D) illicit fentanyl, fentanyl analogues, or synthetic opioids.''.

(d) FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.—Section 101(p)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(p)(2)) is amended by inserting '', including illicit fentanyl, fentanyl analogues, or synthetic opioids'' after ''precursors''.

SA 4692. 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 F of title X, add the following:

SEC. 1054. REPORT ON USE OF DRUG DETECTION TECHNOLOGY AT THE BORDER.

Not later than 6 months after the date of the enactment of this Act, and annually thereafter, the Secretary of Homeland Security shall submit a report to Congress that describes—

(1) the technology that has been authorized by U.S. Customs and Border Protection to detect drug contraband entering the United States at or between ports of entry;

(2) the resources Congress has provided in furtherance of the technology described in paragraph (1);

(3) the technology that has been utilized at the United States border to detect drug contraband entering the United States at or between ports of entry; and

(4) the resources that the Department of Homeland Security has expended in furtherance of such technology.

SA 4693. 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 F of title X, add the following:

SEC. 1054. STUDY AND REPORT ON BILATERAL EFFORTS TO ADDRESS CHINESE FENTANYL TRAFFICKING.

(a) FINDINGS.—Congress finds the following:

(1) In January 2020, the DEA named China as the primary source of United States-bound illicit fentanyl and synthetic opioids.

(2) While in 2019 China instituted domestic controls on the production and exportation of fentanyl, some of its variants, and 2 precursors known as NPP and 4–ANPP, China has not yet expanded its class scheduling to include many fentanyl precursors such as 4–AP, which continue to be trafficked to second countries in which they are used in the final production of United States-bound fentanyl and other synthetic opioids.

(3) The DEA currently maintains a presence in Beijing but continues to seek Chinese approval to open offices in the major shipping hubs of Guangzhou and Shanghai.

(b) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on the Judiciary of the Senate;

(B) the Committee on Foreign Relations of the Senate;

(C) the Committee on the Judiciary of the House of Representatives; and

(D) the Committee on Foreign Affairs of the House of Representatives.

(2) CHINA.—The term ''China'' means the People's Republic of China.

(3) DEA.—The term ''DEA'' means the Drug Enforcement Administration.

(4) PRECURSORS.—The term ''precursors'' means chemicals used in the illicit production of fentanyl and related synthetic opioid variants.

(c) CHINA'S CLASS SCHEDULING OF FENTANYL AND SYNTHETIC OPIOID PRECURSORS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State and the Attorney General shall submit to the appropriate committees of Congress an unclassified written report, with a classified annex, that includes—

(1) a description of United States Government efforts to gain a commitment from the Chinese Government to submit unregulated fentanyl precursors such as 4–AP to controls; and

(2) a plan for future steps the United States Government will take to urge China to combat illicit fentanyl production and trafficking originating in China.

(d) ESTABLISHMENT OF DEA OFFICES IN CHINA.—Not later than 180 days after enactment of this Act, the Secretary of State and Attorney General shall provide to the appropriate committees of Congress a classified briefing on—

(1) outreach and negotiations undertaken by the United States Government with the Chinese Government aimed at securing its approval for the establishment of DEA offices in Shanghai and Guangzhou, China; and

(2) additional efforts to establish new partnerships with provincial-level authorities to counter the illicit trafficking of fentanyl, fentanyl analogues, and their precursors.

(e) REPORT ON DRUG SEIZURES.—Not later than 6 months after the date of the enactment of this Act, and annually thereafter, the Administrator of the Drug Enforcement Administration, in coordination with the Office of National Drug Control Policy, U.S. Customs and Border Protection, the Department of Homeland Security, the Department of Justice, the Coast Guard, the Centers for Disease Control and Prevention, the Office of the United States Trade Representative, the Office of the Director of National Intelligence, the Central Intelligence Agency , the Department of Defense, the United States Postal Service, and other relevant agencies, shall submit a report to Congress that describes—

(1) with respect to illicit fentanyl, fentanyl analogues, synthetic opioids, the precursors for illicit fentanyl, fentanyl analogues, or synthetic opioids, methamphetamine, or methamphetamine precursors seized at the United States borders and ports of entry—

(A) the source countries from which such drugs originated and the third party countries through which such drugs traveled;

(B) the amounts of illicit fentanyl, fentanyl analogues, synthetic opioids, the precursors for illicit fentanyl, fentanyl analogues, or synthetic opioids, methamphetamine, or methamphetamine precursors; and

(C) the lethality of the amounts of illicit fentanyl, fentanyl analogues, synthetic opioids, the precursors for illicit fentanyl, fentanyl analogues, or synthetic opioids, methamphetamine, or methamphetamine precursors seized;

(2) with respect to illicit fentanyl, fentanyl analogues, synthetic opioids, the precursors for illicit fentanyl, fentanyl analogues, or synthetic opioids, methamphetamine, or methamphetamine precursors seized within the United States—

(A) the source countries from which such drugs originated and the third party countries through which such drugs traveled;

(B) the amounts of illicit fentanyl, fentanyl analogues, synthetic opioids, the precursors for illicit fentanyl, fentanyl analogues, or synthetic opioids, methamphetamine, or methamphetamine precursors seized; and

(C) the lethality of the amounts of illicit fentanyl, fentanyl analogues, synthetic opioids, the precursors for illicit fentanyl, fentanyl analogues, or synthetic opioids, methamphetamine, or methamphetamine precursors seized; and

(3) the activities conducted by Chinese entities and nationals in furtherance of illicit fentanyl production in Mexico for drug trafficking purposes.

SA 4694. 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 E of title III, add the following:

SEC. 376. BRIEFING ON DEPOT MAINTENANCE.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Assistant Secretary of Defense for Readiness shall brief the congressional defense committees on the source of repair decision-making process of the Department of Defense for depots.

(b) ELEMENTS.—The briefing required under subsection (a) shall include—

(1) information on how costs and risks to readiness of the Armed Forces are being addressed in the process described in subsection (a);

(2) a timeline for decision making under such process; and

(3) an assessment of the objective balance of workload between the public and private sectors under such process.

SA 4695. 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 C of title XV, add the following:

SEC. 1548. REPORT ON INCREASING TRAINING CAPACITY FOR WEAPONS OF MASS DESTRUCTION CIVIL SUPPORT TEAMS.

Not later than December 31, 2022, the Secretary of Defense, in consultation with the Chief of the National Guard Bureau and the Secretary of Energy, shall submit to the congressional defense committees a report—

(1) assessing the feasibility of increasing training capacity for weapons of mass destruction civil support teams, including through—

(A) the establishment of new facilities and programs to provide such training; and

(B) the augmentation of existing facilities and programs to provide such training;

(2) estimating the costs associated with increasing training capacity as described in paragraph (1); and

(3) identifying facilities and programs that could be established or augmented as described in paragraph (1).

SA 4696. 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 appropriate place, insert the following:

SEC. 10__. ADVANCE CONSULTATION WITH STATE AND LOCAL OFFICIALS AND MONTHLY REPORTS TO CONGRESS REGARDING THE RESETTLEMENT, TRANSPORTATION, AND RELOCATION OF ALIENS IN THE UNITED STATES.

(a) CONSULTATION REQUIREMENT.—Not later than 3 business days before any resettlement, transportation, or relocation of non-detained aliens in the United States that is directed, administered, or funded by the Federal Government, the Secretary of Health and Human Services (in the case of minors) or the Secretary of Homeland Security (in the case of adults), as appropriate, shall consult with the governors and municipal chief executives of the directly affected States and local jurisdictions regarding the proposed resettlement, transportation, or relocation.

(b) REPORTS REQUIRED.—Not later than 7 days after the date of the enactment of this Act, and monthly thereafter, the Secretary of Health and Human Services and the Secretary of Homeland Security, in consultation with other appropriate Federal officials, shall—

(1) submit a State-specific report regarding the resettlement, transportation, or relocation of non-detained aliens in the United States during the previous month that was directed, administered, or funded by the Federal Government or that involved aliens subject to the U.S. Immigration and Customs Enforcement's Alternatives to Detention program that contains the information described in subsection (c) to—

(A) the Committee on the Judiciary of the Senate;

(B) the Committee on Appropriations of the Senate;

(C) the Committee on the Judiciary of the House of Representatives;

(D) the Committee on Appropriations of the House of Representatives; and

(E) the governor of each of the affected States; and

(2) make the report described in paragraph (1) available on a publicly accessible website.

(c) CONTENTS.—Each report under subsection (b) shall contain, with respect to each State—

(1) the number of aliens resettled, transported, or relocated during the previous month and the current calendar year, disaggregated by—

(A) the numbers of single adults, members of family units, and minors;

(B) age;

(C) sex; and

(D) country of origin;

(2) the methods used to determine the ages of such aliens;

(3) the methods used to verify the familial status of such aliens;

(4) the types of settings in which such aliens are being resettled, transported, or relocated, which may be aggregated by the general type of setting;

(5) a summary of the educational or occupational resources or assistance provided to such aliens;

(6) whether such aliens are granted permits to work and how any such aliens without a work permit will financially support themselves;

(7) the amounts and types of Federal resources spent on alien resettlement, transportation, or relocation; and

(8) whether the aliens are being resettled, transported, or relocated on a temporary or permanent basis, disaggregated by—

(A) the numbers of single adults, members of family units, and minors;

(B) age;

(C) sex; and

(D) country of origin.

SA 4697. 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 X, add the following:

SEC. 1064. GUIDANCE ON FOREIGN TRANSPORTATION NETWORK COMPANIES.

Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense, in concurrence with the Secretary of State and the Director of National Intelligence, shall assess the security vulnerabilities associated with the use members of the Armed Forces and Department of Defense civilian personnel of foreign transportation network companies and provide guidance on the appropriate use of such companies. The assessment shall include a review of the data privacy and national security risks inherent to third-party transportation operators with ties to foreign government agencies that provide transportation services to members of the Armed Forces, including the exposure of trip and route details and personally identifiable information.

SA 4698. 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 C of title XII, add the following:

SEC. 1224. CONGRESSIONAL REVIEW OF CERTAIN ACTIONS RELATING TO SANCTIONS IMPOSED WITH RESPECT TO IRAN.

(a) SUBMISSION TO CONGRESS OF PROPOSED ACTION.—

(1) IN GENERAL.—Notwithstanding any other provision of law, before taking any action described in paragraph (2), the President shall submit to the appropriate congressional committees and leadership a report that describes the proposed action and the reasons for that action.

(2) ACTIONS DESCRIBED.—

(A) IN GENERAL.—An action described in this paragraph is—

(i) an action to terminate the application of any sanctions described in subparagraph (B);

(ii) with respect to sanctions described in subparagraph (B) imposed by the President with respect to a person, an action to waive the application of those sanctions with respect to that person; or

(iii) a licensing action that significantly alters United States foreign policy with respect to Iran.

(B) SANCTIONS DESCRIBED.—The sanctions described in this subparagraph are sanctions with respect to Iran provided for under—

(i) the Iran Sanctions Act of 1996 (Public Law 104–172; 50 U.S.C. 1701 note);

(ii) the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (22 U.S.C. 8501 et seq.);

(iii) section 1245 of the National Defense Authorization Act for Fiscal Year 2012 (22 U.S.C. 8513a);

(iv) the Iran Threat Reduction and Syria Human Rights Act of 2012 (22 U.S.C. 8701 et seq.);

(v) the Iran Freedom and Counter-Proliferation Act of 2012 (22 U.S.C. 8801 et seq.);

(vi) the International Emergency Economic Powers Act (50 U.S.C. 1701 note); or

(vii) any other statute or Executive order that requires or authorizes the imposition of sanctions with respect to Iran.

(3) DESCRIPTION OF TYPE OF ACTION.—Each report submitted under paragraph (1) with respect to an action described in paragraph (2) shall include a description of whether the action—

(A) is not intended to significantly alter United States foreign policy with respect to Iran; or

(B) is intended to significantly alter United States foreign policy with respect to Iran.

(4) INCLUSION OF ADDITIONAL MATTER.—

(A) IN GENERAL.—Each report submitted under paragraph (1) that relates to an action that is intended to significantly alter United States foreign policy with respect to Iran shall include a description of—

(i) the significant alteration to United States foreign policy with respect to Iran;

(ii) the anticipated effect of the action on the national security interests of the United States; and

(iii) the policy objectives for which the sanctions affected by the action were initially imposed.

(B) REQUESTS FROM BANKING AND FINANCIAL SERVICES COMMITTEES.—The Committee on Banking, Housing, and Urban Affairs of the Senate or the Committee on Financial Services of the House of Representatives may request the submission to the Committee of the matter described in clauses (ii) and (iii) of subparagraph (A) with respect to a report submitted under paragraph (1) that relates to an action that is not intended to significantly alter United States foreign policy with respect to Iran.

(5) CONFIDENTIALITY OF PROPRIETARY INFORMATION.—Proprietary information that can be associated with a particular person with respect to an action described in paragraph (2) may be included in a report submitted under paragraph (1) only if the appropriate congressional committees and leadership provide assurances of confidentiality, unless that person otherwise consents in writing to such disclosure.

(6) RULE OF CONSTRUCTION.—Paragraph (2)(A)(iii) shall not be construed to require the submission of a report under paragraph (1) with respect to the routine issuance of a license that does not significantly alter United States foreign policy with respect to Iran.

(b) PERIOD FOR REVIEW BY CONGRESS.—

(1) IN GENERAL.—During the period of 30 calendar days beginning on the date on which the President submits a report under subsection (a)(1)—

(A) in the case of a report that relates to an action that is not intended to significantly alter United States foreign policy with respect to Iran, the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives should, as appropriate, hold hearings and briefings and otherwise obtain information in order to fully review the report; and

(B) in the case of a report that relates to an action that is intended to significantly alter United States foreign policy with respect to Iran, the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives should, as appropriate, hold hearings and briefings and otherwise obtain information in order to fully review the report.

(2) EXCEPTION.—The period for congressional review under paragraph (1) of a report required to be submitted under subsection (a)(1) shall be 60 calendar days if the report is submitted on or after July 10 and on or before September 7 in any calendar year.

(3) LIMITATION ON ACTIONS DURING INITIAL CONGRESSIONAL REVIEW PERIOD.—Notwithstanding any other provision of law, during the period for congressional review provided for under paragraph (1) of a report submitted under subsection (a)(1) proposing an action described in subsection (a)(2), including any additional period for such review as applicable under the exception provided in paragraph (2), the President may not take that action unless a joint resolution of approval with respect to that action is enacted in accordance with subsection (c).

(4) LIMITATION ON ACTIONS DURING PRESIDENTIAL CONSIDERATION OF A JOINT RESOLUTION OF DISAPPROVAL.—Notwithstanding any other provision of law, if a joint resolution of disapproval relating to a report submitted under subsection (a)(1) proposing an action described in subsection (a)(2) passes both Houses of Congress in accordance with subsection (c), the President may not take that action for a period of 12 calendar days after the date of passage of the joint resolution of disapproval.

(5) LIMITATION ON ACTIONS DURING CONGRESSIONAL RECONSIDERATION OF A JOINT RESOLUTION OF DISAPPROVAL.—Notwithstanding any other provision of law, if a joint resolution of disapproval relating to a report submitted under subsection (a)(1) proposing an action described in subsection (a)(2) passes both Houses of Congress in accordance with subsection (c), and the President vetoes the joint resolution, the President may not take that action for a period of 10 calendar days after the date of the President's veto.

(6) EFFECT OF ENACTMENT OF A JOINT RESOLUTION OF DISAPPROVAL.—Notwithstanding any other provision of law, if a joint resolution of disapproval relating to a report submitted under subsection (a)(1) proposing an action described in subsection (a)(2) is enacted in accordance with subsection (c), the President may not take that action.

(c) JOINT RESOLUTIONS OF DISAPPROVAL OR APPROVAL.—

(1) DEFINITIONS.—In this subsection:

(A) JOINT RESOLUTION OF APPROVAL.—The term ''joint resolution of approval'' means only a joint resolution of either House of Congress—

(i) the title of which is as follows: ''A joint resolution approving the President's proposal to take an action relating to the application of certain sanctions with respect to Iran.''; and

(ii) the sole matter after the resolving clause of which is the following: ''Congress approves of the action relating to the application of sanctions imposed with respect to Iran proposed by the President in the report submitted to Congress under section 1224(a)(1) of the National Defense Authorization Act for Fiscal Year 2022 on _____ relating to _____.'', with the first blank space being filled with the appropriate date and the second blank space being filled with a short description of the proposed action.

(B) JOINT RESOLUTION OF DISAPPROVAL.—The term ''joint resolution of disapproval'' means only a joint resolution of either House of Congress—

(i) the title of which is as follows: ''A joint resolution disapproving the President's proposal to take an action relating to the application of certain sanctions with respect to Iran.''; and

(ii) the sole matter after the resolving clause of which is the following: ''Congress disapproves of the action relating to the application of sanctions imposed with respect to Iran proposed by the President in the report submitted to Congress under section 1224(a)(1) of the National Defense Authorization Act for Fiscal Year 2022 on _____ relating to _____.'', with the first blank space being filled with the appropriate date and the second blank space being filled with a short description of the proposed action.

(2) INTRODUCTION.—During the period of 30 calendar days provided for under subsection (b)(1), including any additional period as applicable under the exception provided in subsection (b)(2), a joint resolution of approval or joint resolution of disapproval may be introduced—

(A) in the House of Representatives, by the majority leader or the minority leader; and

(B) in the Senate, by the majority leader (or the majority leader's designee) or the minority leader (or the minority leader's designee).

(3) FLOOR CONSIDERATION IN HOUSE OF REPRESENTATIVES.—If a committee of the House of Representatives to which a joint resolution of approval or joint resolution of disapproval has been referred has not reported the joint resolution within 10 calendar days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

(4) CONSIDERATION IN THE SENATE.—

(A) COMMITTEE REFERRAL.—A joint resolution of approval or joint resolution of disapproval introduced in the Senate shall be—

(i) referred to the Committee on Banking, Housing, and Urban Affairs if the joint resolution relates to a report under subsection (a)(3)(A) that relates to an action that is not intended to significantly alter United States foreign policy with respect to Iran; and

(ii) referred to the Committee on Foreign Relations if the joint resolution relates to a report under subsection (a)(3)(B) that relates to an action that is intended to significantly alter United States foreign policy with respect to Iran.

(B) REPORTING AND DISCHARGE.—If the committee to which a joint resolution of approval or joint resolution of disapproval was referred has not reported the joint resolution within 10 calendar days after the date of referral of the joint resolution, that committee shall be discharged from further consideration of the joint resolution and the joint resolution shall be placed on the appropriate calendar.

(C) PROCEEDING TO CONSIDERATION.—Notwithstanding Rule XXII of the Standing Rules of the Senate, it is in order at any time after the Committee on Banking, Housing, and Urban Affairs or the Committee on Foreign Relations, as the case may be, reports a joint resolution of approval or joint resolution of disapproval to the Senate or has been discharged from consideration of such a joint resolution (even though a previous motion to the same effect has been disagreed to) to move to proceed to the consideration of the joint resolution, and all points of order against the joint resolution (and against consideration of the joint resolution) are waived. The motion to proceed is not debatable. The motion is not subject to a motion to postpone. A motion to reconsider the vote by which the motion is agreed to or disagreed to shall not be in order.

(D) RULINGS OF THE CHAIR ON PROCEDURE.—Appeals from the decisions of the Chair relating to the application of the rules of the Senate, as the case may be, to the procedure relating to a joint resolution of approval or joint resolution of disapproval shall be decided without debate.

(E) CONSIDERATION OF VETO MESSAGES.—Debate in the Senate of any veto message with respect to a joint resolution of approval or joint resolution of disapproval, including all debatable motions and appeals in connection with the joint resolution, shall be limited to 10 hours, to be equally divided between, and controlled by, the majority leader and the minority leader or their designees.

(5) RULES RELATING TO SENATE AND HOUSE OF REPRESENTATIVES.—

(A) TREATMENT OF SENATE JOINT RESOLUTION IN HOUSE.—In the House of Representatives, the following procedures shall apply to a joint resolution of approval or a joint resolution of disapproval received from the Senate (unless the House has already passed a joint resolution relating to the same proposed action):

(i) The joint resolution shall be referred to the appropriate committees.

(ii) If a committee to which a joint resolution has been referred has not reported the joint resolution within 2 calendar days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

(iii) Beginning on the third legislative day after each committee to which a joint resolution has been referred reports the joint resolution to the House or has been discharged from further consideration thereof, it shall be in order to move to proceed to consider the joint resolution in the House. All points of order against the motion are waived. Such a motion shall not be in order after the House has disposed of a motion to proceed on the joint resolution. The previous question shall be considered as ordered on the motion to its adoption without intervening motion. The motion shall not be debatable. A motion to reconsider the vote by which the motion is disposed of shall not be in order.

(iv) The joint resolution shall be considered as read. All points of order against the joint resolution and against its consideration are waived. The previous question shall be considered as ordered on the joint resolution to final passage without intervening motion except 2 hours of debate equally divided and controlled by the sponsor of the joint resolution (or a designee) and an opponent. A motion to reconsider the vote on passage of the joint resolution shall not be in order.

(B) TREATMENT OF HOUSE JOINT RESOLUTION IN SENATE.—

(i) RECEIPT BEFORE PASSAGE.—If, before the passage by the Senate of a joint resolution of approval or joint resolution of disapproval, the Senate receives an identical joint resolution from the House of Representatives, the following procedures shall apply:

(I) That joint resolution shall not be referred to a committee.

(II) With respect to that joint resolution—

(aa) the procedure in the Senate shall be the same as if no joint resolution had been received from the House of Representatives; but

(bb) the vote on passage shall be on the joint resolution from the House of Representatives.

(ii) RECEIPT AFTER PASSAGE.—If, following passage of a joint resolution of approval or joint resolution of disapproval in the Senate, the Senate receives an identical joint resolution from the House of Representatives, that joint resolution shall be placed on the appropriate Senate calendar.

(iii) NO COMPANION MEASURE.—If a joint resolution of approval or a joint resolution of disapproval is received from the House, and no companion joint resolution has been introduced in the Senate, the Senate procedures under this subsection shall apply to the House joint resolution.

(C) APPLICATION TO REVENUE MEASURES.—The provisions of this paragraph shall not apply in the House of Representatives to a joint resolution of approval or joint resolution of disapproval that is a revenue measure.

(6) RULES OF HOUSE OF REPRESENTATIVES AND SENATE.—This subsection is enacted by Congress—

(A) as an exercise of the rulemaking power of the Senate and the House of Representatives, respectively, and as such is deemed a part of the rules of each House, respectively, and supersedes other rules only to the extent that it is inconsistent with such rules; and

(B) with full recognition of the constitutional right of either House to change the rules (so far as relating to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House.

(d) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP DEFINED.—In this section, the term ''appropriate congressional committees and leadership'' means—

(1) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the majority and minority leaders of the Senate; and

(2) the Committee on Financial Services, the Committee on Foreign Affairs, and the Speaker, the majority leader, and the minority leader of the House of Representatives.

SA 4699. 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. OFFICE OF GLOBAL WOMEN'S ISSUES AND THE WOMEN'S GLOBAL DEVELOPMENT AND PROSPERITY INITIATIVE.

Chapter 1 of part I of the Foreign Assistance Act of 1961 (22 U.S.C. 2151 et seq.) is amended by adding at the end the following:

''SEC. 138. OFFICE OF GLOBAL WOMEN'S ISSUES AND THE WOMEN'S GLOBAL DEVELOPMENT AND PROSPERITY INITIATIVE.

''(a) IN GENERAL.—The Secretary of State shall establish, in the Office of the Secretary of State, the Office of Global Women's Issues (referred to in this section as the 'Office').

''(b) PURPOSE; DUTIES.—

''(1) PURPOSE.—The purpose of the Office is to advance equal opportunity for women and the status of women and girls in United States foreign policy.

''(2) DUTIES.—In carrying out the purpose described in paragraph (1), the Office—

''(A)(i) shall advise the Secretary of State and provide input on all activities, policies, programs, and funding relating to equal opportunity for women and the advancement of women and girls internationally to all bureaus and offices of the Department of State; and

''(ii) may, as appropriate, provide to the international programs of other Federal agencies input on all activities, policies, programs, and funding relating to equal opportunity for women and the advancement of women and girls internationally;

''(B)(i) shall work to ensure that efforts to advance equal opportunity for women and men and women's and girls' empowerment are fully integrated into the programs, structures, processes, and capacities of all bureaus and offices of the Department of State; and

''(ii) may, as appropriate, work to ensure that efforts to advance equal opportunity for women and men and women's and girls' empowerment are fully integrated into the international programs of other Federal agencies;

''(C) shall implement the Women's Global Development and Prosperity Initiative, in accordance with subsection (c); and

''(D) may not engage in any activities not described in subparagraphs (A) through (C).

''(c) WOMEN'S GLOBAL DEVELOPMENT AND PROSPERITY INITIATIVE.—

''(1) ESTABLISHMENT.—The Secretary of State shall establish the Women's Global Development and Prosperity Initiative (referred to in this subsection as the 'Initiative') to carry out the activities described in paragraphs (2) through (4).

''(2) WOMEN PROSPERING IN THE WORKFORCE.—The Initiative shall advance women in the workforce by improving their access to quality vocational education and skills training, which will enable them to secure jobs in their local economies.

''(3) WOMEN SUCCEEDING AS ENTREPRENEURS.—The Initiative shall promote women's entrepreneurship and increasing access to capital, financial services, markets, technical assistance, and mentorship.

''(4) WOMEN ENABLED IN THE ECONOMY.—The Initiative shall identify and reduce the binding constraints in economic and property laws and practices that prevent women's full and free participation in the global economy and promote foundational legal reforms, including—

''(A) ensuring that women can fully participate in the workforce and engage in economic activities by—

''(i) ending impunity for violence against women;

''(ii) ensuring that women have the authority to sign legal documents, such as contracts and court documents; and

''(iii) addressing unequal access to courts and administrative bodies for women, whether officially or through lack of proper enforcement;

''(B) ensuring women's equal access to credit and capital to start and grow their businesses, savings, and investments, including prohibiting discrimination in access to credit on the basis of sex or marital status;

''(C) lifting restrictions on women's right to own, manage, and make decisions relating to the use of property, including repealing limitations on inheritance and ensuring the ability to transfer, purchase, or lease such property;

''(D) addressing constraints on women's freedom of movement, including sex-based restrictions on obtaining passports and identification documents; and

''(E) promoting the free and equal participation of women in the economy with regard to working hours, occupations, and occupational tasks.

''(d) SUPERVISION.—The Office shall be headed by an Ambassador-at-Large for Global Women's Issues and the Women's Global Development and Prosperity Initiative (referred to in this section as the 'Ambassador'), who shall—

''(1) be appointed by the President, with the advice and consent of the Senate;

''(2) report directly to the Secretary; and

''(3) have the rank and status of Ambassador-at-Large.

''(e) COORDINATION.—United States Government efforts to advance women's economic empowerment globally shall be closely aligned and coordinated with the Initiative.

''(f) ABORTION NEUTRALITY.—

''(1) PROHIBITIONS.—The Office, the Initiative, and the Ambassador may not—

''(A) lobby other countries, including through multilateral mechanisms and foreign nongovernmental organizations—

''(i) to change domestic laws or policies with respect to abortion; or

''(ii) to include abortion as a programmatic requirement of any foreign activities; or

''(B) provide Federal funding appropriated for foreign assistance to pay for or to promote abortion.

''(2) LIMITATIONS ON USE OF FUNDS.—Amounts appropriated for the Office or the Initiative may not be used—

''(A) to lobby other countries, including through multilateral mechanisms and foreign nongovernmental organizations—

''(i) to change domestic laws or policies with respect to abortion; or

''(ii) to include abortion as a programmatic requirement of any foreign activities; or

''(B) to provide Federal foreign assistance funding to pay for or to promote abortion.

''(3) CONSTRUCTION.—Nothing in this subsection may be construed to prevent—

''(A) the funding of activities for the purpose of treating injuries or illnesses caused by legal or illegal abortions; or

''(B) agencies or officers of the United States from engaging in activities in opposition to policies of coercive abortion or involuntary sterilization.

''(g) REPORT.—Not later than 180 days after the date of the enactment of this section, and not less frequently than annually thereafter, the Secretary of State shall—

''(1) submit a written report to the Committee on Appropriations of the Senate, the Committee on Foreign Relations of the Senate, the Committee on Appropriations of the House of Representatives, and the Committee on Foreign Affairs of the House of Representatives that describes the implementation of this section, including—

''(A) measures taken to ensure compliance with subsection (f); and

''(B) with respect to funds appropriated pursuant to subsection (h)—

''(i) amounts awarded to prime recipients and subrecipients since the end of the previous reporting period; and

''(ii) descriptions of each program for which such funds are used; and

''(2) make such report publicly available.

''(h) FUNDING.—

''(1) IN GENERAL.—There shall be reserved to carry out this section, from funds made available for development assistance programs of the United States Agency for International Development, $200,000,000, for each of the fiscal years 2022 through 2026, which shall be—

''(A) deposited into the Women's Global Development and Prosperity Fund (W–GDP);

''(B) administered by the United States Agency for International Development;

''(C) expended solely for the purpose, duties, and activities set forth in subsections (b) and (c); and

''(D) expended, to the greatest extent practicable, in support of removing legal barriers to women's economic freedom in accordance with the findings of the W–GDP Women's Economic Freedom Index report published by the Council of Economic Advisers in February 2020.

''(2) REQUIREMENT.—Notwithstanding paragraph (1), amounts reserved under paragraph (1) for fiscal year 2023, or for any later fiscal year, may not be obligated or expended unless the most recent report submitted pursuant to subsection (g)(1) includes the information required under subparagraphs (A) and (B) of subsection (g)(1).

''(3) OVERSIGHT.—The expenditure of amounts reserved under paragraph (1) shall be jointly overseen by—

''(A) the United States Agency for International Development;

''(B) the Ambassador; and

''(C) the Initiative.''.

SA 4700. 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 appropriate place, insert the following:

SEC. _____. DISCLOSE GOVERNMENT CENSORSHIP.

(a) DEFINITIONS.—In this section:

(1) INFORMATION CONTENT PROVIDER; INTERACTIVE COMPUTER SERVICE.—The terms ''information content provider'' and ''interactive computer service'' have the meanings given the terms in section 230 of the Communications Act of 1934 (47 U.S.C. 230).

(2) LEGITIMATE LAW ENFORCEMENT PURPOSE.—The term ''legitimate law enforcement purpose'' means for the purpose of investigating a criminal offense by a law enforcement agency that is within the lawful authority of that agency.

(3) NATIONAL SECURITY PURPOSE.—The term ''national security purpose'' means a purpose that relates to—

(A) intelligence activities;

(B) cryptologic activities related to national security;

(C) command and control of military forces;

(D) equipment that is an integral part of a weapon or weapons system; or

(E) the direct fulfillment of military or intelligence missions.

(b) DISCLOSURES.—

(1) IN GENERAL.—Except as provided in paragraph (3), any officer or employee in the executive or legislative branch shall disclose and, in the case of a written communication, make available for public inspection, on a public website in accordance with paragraph (4), any communication by that officer or employee with a provider or operator of an interactive computer service regarding action or potential action by the provider or operator to restrict access to or the availability of, bar or limit access to, or decrease the dissemination or visibility to users of, material posted by another information content provider, whether the action is or would be carried out manually or through use of an algorithm or other automated or semi-automated process.

(2) TIMING.—The disclosure required under paragraph (1) shall be made not later than 7 days after the date on which the communication is made.

(3) LEGITIMATE LAW ENFORCEMENT AND NATIONAL SECURITY PURPOSES.—

(A) IN GENERAL.—Any communication for a legitimate law enforcement purpose or national security purpose shall be disclosed and, in the case of a written communication, made available for inspection, to each House of Congress.

(B) TIMING.—The disclosure required under subparagraph (A) shall be made not later than 60 days after the date on which the communication is made.

(C) RECEIPT.—Upon receipt, each House shall provide copies to the chairman and ranking member of each standing committee with jurisdiction under the rules of the House of Representatives or the Senate regarding the subject matter to which the communication pertains. Such information shall be deemed the property of such committee and may not be disclosed except—

(i) in accordance with the rules of the committee;

(ii) in accordance with the rules of the House of Representatives and the Senate; and

(iii) as permitted by law.

(4) WEBSITE.—

(A) LEGISLATIVE BRANCH.—The Sergeant at Arms of the Senate and the Sergeant at Arms of the House of Representatives shall designate a single location on an internet website where the disclosures and communications of employees and officers in the legislative branch shall be published in accordance with paragraph (1).

(B) EXECUTIVE BRANCH.—The Director of the Office of Management and Budget shall designate a single location on an internet website where the disclosures and communications of employees and officers in the executive branch shall be published in accordance with paragraph (1).

(5) NOTICE.—The Sergeant at Arms of the Senate, the Sergeant at Arms of the House of Representatives, and the Director of the Office of Management and Budget shall take reasonable steps to ensure that each officer and employee of the legislative branch and executive branch, as applicable, are informed of the duties imposed by this section.

(6) CONFLICTS OF INTEREST.—Any person who is a former officer or employee of the executive branch of the United States (including any independent agency) or any person who is a former officer or employee of the legislative branch or a former Member of Congress, who personally and substantially participated in any communication under paragraph (1) while serving as an officer, employee, or Member of Congress, shall not, within 2 years after any such communication under paragraph (1) or 1 year after termination of his or her service as an officer, employee, or Member of Congress, whichever is later, knowingly make, with the intent to influence, any communication to or appearance before any officer or employee of any department, agency, court, or court-martial of the United States, on behalf of any person with which the former officer or employee personally and substantially participated in such communication under paragraph (1).

(7) PENALTIES.—Any person who violates paragraph (1), (2), (3), or (6) shall be punished as provided in section 216 of title 18, United States Code.

SA 4701. 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 appropriate place, insert the following:

SEC. ___. REPORT ON 2020 GENERAL ELECTION.

(a) DEFINITIONS.—For purposes of this section:

(1) 2016 PRESIDENTIAL ELECTION.—The term ''2016 Presidential election'' means the general election for Federal office occurring in 2016.

(2) 2020 PRESIDENTIAL ELECTION.—The term ''2020 Presidential election'' means the general election for Federal office occurring in 2020.

(3) APPLICABLE ELECTION SECURITY FUNDS.—The term ''applicable election security funds'' means the amount of grant funding provided to the State by the Election Assistance Commission—

(A) from amounts appropriated under the heading ''Election Assistance Commission, Election Security Grants'' in the Financial Services and General Government Appropriations Act, 2020 (Public Law 116–93); or

(B) from amounts appropriated under the heading ''Election Assistance Commission, Election Security Grants'' in the Coronavirus Aid, Relief, and Economic Security Act (Public Law 116–136).

(4) STATE.—The term ''State'' has the meaning given such term under section 901 of the Help America Vote Act of 2002 (52 U.S.C. 21141), except that such term shall include the Commonwealth of the Northern Mariana Islands.

(5) UNSOLICITED MAIL-IN BALLOT.—The term ''unsolicited mail-in ballot'' means any ballot sent to a voter by mail if—

(A) such ballot was not specifically requested by the voter; or

(B) the ballot request by the voter was initiated by the mailing of a ballot application not specifically requested by the voter.

(6) UNSOLICITED MAIL-IN BALLOT PERCENTAGE.—The term ''unsolicited mail-in ballot percentage'' means the number of unsolicited mail-in ballots distributed in the State as a percentage of the number of total ballots provided to voters in the State.

(b) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General shall submit to Congress and make publicly available a report on the 2020 Presidential election.

(2) MATTERS INCLUDED.—The report submitted under paragraph (1) shall include the following with respect to each State: that received applicable election security funds:

(A) UNSOLICITED MAIL-IN BALLOT PERCENTAGE.—

(i) IN GENERAL.—An analysis of whether the unsolicited mail-in ballot percentage for State for the 2020 Presidential election was greater than the unsolicited mail-in ballot percentage for the State for the 2016 Presidential election.

(ii) RELEVANT AUTHORITY FOR ANY INCREASE.—If the Comptroller General determines that the unsolicited mail-in ballot percentage for the State for the 2020 Presidential election was greater than the unsolicited mail-in ballot percentage for the State for the 2016 Presidential election, the Comptroller General shall provide a description of any change in authority (including any statutory change relating to the distribution of unsolicited mail-in ballots), action, or directive concerning unsolicited mail-in ballots occurring between the 2016 Presidential election and 2020 Presidential election that may have led to such result.

(B) MAIL-IN VOTER VERIFICATION PROCEDURES.—

(i) IN GENERAL.—An analysis of whether there were changes in the State's methods and processes used to verify the identification of voters who vote using mail-in ballots, including signature verification requirements, that applied with respect to the 2020 Presidential election but did not apply to the 2016 Presidential election.

(ii) RELEVANT AUTHORITY FOR CHANGES.—If the Comptroller General determines that there were changes in the State's mail-in voter verification procedures described in clause (i), the Comptroller General shall provide a description of any authority (including any statutory authority), action, or directive that led to such change.

(C) OTHER ELECTION PROCEDURES.—

(i) IN GENERAL.—An analysis of whether the State materially altered or changed its election procedures for the 2020 Presidential election (other than procedures described in subparagraph (B)) from the procedures in effect for the 2016 Presidential election.

(ii) RELEVANT AUTHORITY FOR CHANGES.—If the Comptroller General determines that there were changes in the election procedures described in clause (i), the Comptroller General shall provide a description of any authority (including any statutory authority), action, or directive that led to such change.

(D) MAIL-IN BALLOT COLLECTION.—

(i) IN GENERAL.—An analysis of whether there were specific, documented allegations of a person other than a voter or a voter's family member or caregiver collecting or returning the voter's completed ballot in the 2020 Presidential election.

(ii) RELEVANT AUTHORITY FOR COLLECTION.—If the Comptroller General determines that there were specific, documented allegations described in clause (i), the Comptroller General shall provide a description of any authority (including any statutory authority), action, or directive permitting such collection or return.

(E) OBSERVATION OF BALLOT COUNTING.—An analysis of whether the State has a statute providing for third-party observation of ballot counting, and if so, whether there were specific, documented instances in connection with the 2020 Presidential election in which the State is alleged to have failed to comply with such statute.

(F) FAILURE TO ENFORCE.—An analysis of whether there were specific, documented instances in connection with the 2020 Presidential election in which the State allegedly failed to enforce one or more of its election statutes (other than a statute described in subparagraph (E)).

(G) USE OF APPLICABLE ELECTION SECURITY FUNDS.—In the case of a State that received applicable election security funds, an analysis of—

(i) whether such funds were used to make expenditures with respect to the 2020 Presidential election;

(ii) whether such funds were used in connection with any activity carried out pursuant to an authority, action, or directive described in subparagraph (A)(ii), (B)(ii), (C)(ii), or (D)(ii); and

(iii) whether the State complied with all statutory and other conditions imposed in connection with the receipt of such funds.

(H) SUBSEQUENT STATE ACTIONS.—A description of any of the following actions taken by the State legislature:

(i) The passage of a resolution expressing an opinion on, or the submission to Congress or the Comptroller General of a communication relating to, the items described in subparagraphs (A) through (G).

(ii) The enactment, after the completion of the 2020 Presidential election, of legislation regarding any authority, action, or directive described in subparagraph (A)(ii), (B)(ii), (C)(ii), or (D)(ii) or any failure described in subparagraph (E) or (F).

SEC. ___. TEMPORARY SUSPENSION OF, AND REQUIREMENTS FOR, FUTURE ELECTION ASSISTANCE GRANTS.

(a) IN GENERAL.—Subtitle D of title II of the Help America Vote Act of 2002 (52 U.S.C. 20901 et seq.) is amended by adding at the end the following new part:

''PART 7—REQUIREMENTS FOR ELECTION ASSISTANCE

''SEC. 297. SUSPENSION OF ELECTION ASSISTANCE.

''(a) IN GENERAL.—Notwithstanding any other provision of law, no grant may be awarded under this Act before July 1, 2022.

''(b) SUSPENSION OF PREVIOUS GRANTS.—No State may expend Federal funds provided under this Act before the date of the enactment of this section before July 1, 2022.

''SEC. 298. REQUIREMENTS FOR FUTURE ELECTION ASSISTANCE.

''(a) IN GENERAL.—Notwithstanding any other provision of law, no State may receive any grant awarded under this Act after the date of the enactment of this section unless the State has certified by resolution adopted by the State legislature, as a condition of receiving the grant, that it is in compliance with the requirements of subsection (b).

''(b) REQUIREMENTS.—

''(1) IN GENERAL.—A State satisfies the requirements of this section if, in connection with any election for Federal office—

''(A) the methods and processes used by the State to verify the identification of voters who vote using mail-in ballots are specifically set forth in statute;

''(B) except as specifically provided by statute—

''(i) the State does not use unsolicited mail-in balloting; and

''(ii) the State does not permit persons other than the voter or the voter's family members or caregivers to return a voter's completed ballot;

''(C) for any election after the last day that the public health emergency declared by the Secretary of Health and Human Services under section 319 of the Public Health Service Act (42 U.S.C. 247d) on January 31, 2020, with respect to COVID–19, is in effect, the State uses all voting procedures in place as of January 1, 2020 (except as modified by State statutes applying to elections after such date);

''(D) in the case of State that has a law providing for third-party observation of ballot counting, such ballot observation law is strictly followed in all instances;

''(E) the State complies with all requirements under title III; and

''(F) the State has taken documented, affirmative measures to address—

''(i) any prior failure to satisfy the requirements of subparagraphs (A) through (E) that is identified by the State legislature in a resolution (or other similar communication submitted to Congress and the Comptroller General); or

''(ii) any prior specific, documented instance in which the State—

''(I) failed to enforce one or more of its election statutes; or

''(II) materially altered or changed its election procedures without a corresponding state statutory enactment.

''(2) UNSOLICITED MAIL-IN BALLOTING.—For purposes of paragraph (1)(B), the term 'unsolicited mail-in balloting' means the process of sending ballots to a voter by mail if—

''(A) such ballot was not specifically requested by the voter; or

''(B) the ballot request by the voter was initiated by the mailing of a ballot application not specifically requested by the voter.

''PART 8—PROHIBITION ON USE OF FUNDS

''SEC. 299. PROHIBITION ON USE OF FUNDS.

''Notwithstanding any other provision of law, any amounts provided under this Act

shall not be used in furtherance of any election procedure that is not expressly set forth in a statute enacted by the State legislature.''.

(b) CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Help America Vote Act of 2002 is amended by inserting after the item relating to section 296 the following:

''PART 7—REQUIREMENTS FOR ELECTION ASSISTANCE

''Sec. 297. Suspension of election assistance.
''Sec. 298. Requirements for future election assistance.

''PART 8—PROHIBITION ON USE OF FUNDS

''Sec. 299. Prohibition on use of funds.''.

SA 4702. 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 appropriate place, insert the following:

SEC. _____. REASONABLE, NON-DISCRIMINATORY ACCESS TO ONLINE COMMUNICATIONS PLATFORMS; BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.

(a) IN GENERAL.—Part I of title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended—

(1) by striking section 230; and

(2) by adding at the end the following:

''SEC. 232. REASONABLE, NON-DISCRIMINATORY ACCESS TO ONLINE COMMUNICATIONS PLATFORMS; BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.

''(a) FINDINGS.—Congress finds the following:

''(1) The rapidly developing array of internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

''(2) These services often offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology continues to develop.

''(3) The internet and other interactive computer services offer a forum for a true diversity of political discourse and viewpoints, unique opportunities for cultural development, and myriad avenues for intellectual activity, and regulation of the internet must be tailored to supporting those activities.

''(4) The internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation, and regulation should be limited to what is necessary to preserve the societal benefits provided by the internet.

''(5) Increasingly Americans rely on internet platforms and websites for a variety of political, educational, cultural, and entertainment services and for communication with one another.

''(b) POLICY.—It is the policy of the United States—

''(1) to promote the continued development of the internet and other interactive computer services and other interactive media;

''(2) to preserve a vibrant and competitive free market for the internet and other interactive computer services;

''(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the internet and other interactive computer services, rather than control and censorship driven by interactive computer services;

''(4) to facilitate the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material;

''(5)(A) to ensure that the internet serves as an open forum for—

''(i) a true diversity of discourse and viewpoints, including political discourse and viewpoints;

''(ii) unique opportunities for cultural development; and

''(iii) myriad avenues for intellectual activity; and

''(B) given that the internet is the dominant platform for communication and public debate today, to ensure that major internet communications platforms, which function as common carriers in terms of their size, usage, and necessity, are available to all users on reasonable and non-discriminatory terms free from public or private censorship of religious and political speech;

''(6) to promote consumer protection and transparency regarding information and content management practices by major internet platforms to—

''(A) ensure that consumers understand—

''(i) the products they are using; and

''(ii) what information is being presented to them and why; and

''(B) prevent deceptive or undetectable actions that filter the information presented to consumers; and

''(7) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in online obscenity, stalking, and harassment.

''(c) REASONABLE AND NONDISCRIMINATORY ACCESS TO COMMON CARRIER TECHNOLOGY COMPANIES.—

''(1) IN GENERAL.—A common carrier technology company, with respect to the interactive computer service provided by the company—

''(A) shall furnish the interactive computer service to all persons upon reasonable request;

''(B) may not unjustly or unreasonably discriminate in charges, practices, classifications, regulations, facilities, treatment, or services for or in connection with the furnishing of the interactive computer service, directly or indirectly, by any means or device;

''(C) may not make or give any undue or unreasonable preference or advantage to any particular person, class of persons, political or religious group or affiliation, or locality; and

''(D) may not subject any particular person, class of persons, political or religious group or affiliation, or locality to any undue or unreasonable prejudice or disadvantage.

''(2) APPLICABILITY TO BROADBAND.—Paragraph (1) shall not apply with respect to the provision of broadband internet access service.

''(d) CONSUMER PROTECTION AND TRANSPARENCY REGARDING COMMON CARRIER TECHNOLOGY COMPANIES.—

''(1) IN GENERAL.—A common carrier technology company shall disclose, through a publicly available, easily accessible website, accurate material regarding the content management, moderation, promotion, account termination and suspension, and curation mechanisms and practices of the company sufficient to enable—

''(A) consumers to make informed choices regarding use of the interactive computer service provided by the company; and

''(B) persons to develop, market, and maintain consumer-driven content management mechanisms with respect to the interactive computer service provided by the company.

''(2) BEST PRACTICES.—The Commission, after soliciting comments from the public, shall publish best practices for common carrier technology companies to disclose content management, moderation, promotion, account termination and suspension, and curation mechanisms and practices in accordance with paragraph (1).

''(3) APPLICABILITY TO BROADBAND.—Paragraph (1) shall not apply with respect to the provision of broadband internet access service.

''(e) PROTECTION FOR 'GOOD SAMARITAN' BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.—

''(1) TREATMENT OF PUBLISHER OR SPEAKER.—

''(A) IN GENERAL.—No provider or user of an interactive computer service shall be treated as the publisher or speaker of any material provided by another information content provider.

''(B) EXCEPTION.—Subparagraph (A) shall not apply to any affirmative act by a provider or user of an interactive computer service with respect to material posted on the interactive computer service, whether the act is carried out manually or through use of an algorithm or other automated or semi-automated process, including—

''(i) providing its own material;

''(ii) commenting or editorializing on, promoting, recommending, or increasing or decreasing the dissemination or visibility to users of its own material or material provided by another information content provider;

''(iii) restricting access to or availability of material provided by another information content provider; or

''(iv) barring or limiting any information content provider from using the interactive computer service.

''(2) CIVIL LIABILITY.—

''(A) IN GENERAL.—No provider or user of an interactive computer service shall be held liable, under subsection (c) or otherwise, on account of—

''(i) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, promoting self-harm, or unlawful, whether or not such material is constitutionally protected; or

''(ii) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in clause (i).

''(B) DEFINITIONS.—For purposes of subparagraph (A)—

''(i) the term 'excessively violent', with respect to material, means material that—

''(I) is likely to be deemed violent and for mature audiences according to the V-chip regulations and TV Parental Guidelines of the Commission promulgated under sections 303(x) and 330(c)(4); or

''(II) constitutes or intends to advocate domestic terrorism or international terrorism, as defined in section 2331 of title 18, United States Code;

''(ii) the term 'harassing' means material that—

''(I) is—

''(aa) provided by an information content provider with the intent to abuse, threaten, or harass any specific person; and

''(bb) lacking in any serious literary, artistic, political, or scientific value;

''(II) violates the CAN-SPAM Act of 2003 (15 U.S.C. 7701 et seq.); or

''(III) is malicious computer code intended (whether or not by the immediate disseminator) to damage or interfere with the operation of a computer;

''(iii) the term 'in good faith', with respect to restricting access to or availability of specific material, means the provider or user—

''(I) restricts access to or availability of material consistent with publicly available online terms of service or use that—

''(aa) state plainly and with particularity the criteria that the provider or user of the interactive computer service employs in its content moderation practices, including by any partially or fully automated processes; and

''(bb) are in effect on the date on which the material is first posted;

''(II) has an objectively reasonable belief that the material falls within one of the categories listed in subparagraph (A)(i);

''(III)(aa) does not restrict access to or availability of material on deceptive or pretextual grounds; and

''(bb) does not apply its terms of service or use to restrict access to or availability of material that is similarly situated to material that the provider or user of the interactive computer service intentionally declines to restrict; and

''(IV) supplies the information content provider of the material with timely notice describing with particularity the reasonable factual basis for the restriction of access and a meaningful opportunity to respond, unless the provider or user of the interactive computer service has an objectively reasonable belief that—

''(aa) the material is related to terrorism or criminal activity; or

''(bb) such notice would risk imminent physical harm to others; and

''(iv) the terms 'obscene', 'lewd', 'lascivious', and 'filthy', with respect to material, mean material that—

''(I) taken as a whole—

''(aa) appeals to the prurient interest in sex or portrays sexual conduct in a patently offensive way; and

''(bb) does not have serious literary, artistic, political, or scientific value;

''(II) depicts or describes sexual or excretory organs or activities in terms patently offensive to the average person, applying contemporary community standards; or

''(III) signifies the form of immorality which has relation to sexual impurity, taking into account the standards at common law in prosecutions for obscene libel.

''(C) BEST PRACTICES.—The Commission, after soliciting comments from the public, shall publish best practices for making publicly available online terms of service or use that state plainly and with particularity the criteria that the provider or user of an interactive computer service employs in its content moderation practices, including by any partially or fully automated processes, in accordance with subparagraph (B)(iii)(I).

''(f) VIOLATIONS.—

''(1) PRIVATE RIGHT OF ACTION.—

''(A) IN GENERAL.—A person aggrieved by a violation of subsection (c) or (d) may bring a civil action against the provider or user of an interactive computer service that committed the violation for any relief permitted under subparagraph (B) of this paragraph.

''(B) RELIEF.—

''(i) IN GENERAL.—The plaintiff may seek the following relief in a civil action brought under subparagraph (A):

''(I) An injunction.

''(II) An award that is the greater of—

''(aa) actual damages; or

''(bb) damages in the amount of $500 for each violation.

''(ii) WILLFUL OR KNOWING VIOLATIONS.—In a civil action brought under subparagraph (A), if the court finds that the defendant willfully or knowingly violated subsection (c) or (d), the court may, in its discretion, increase the amount of the award to not more than 3 times the amount available under clause (i)(II) of this subparagraph.

''(2) ACTIONS BY STATES.—

''(A) AUTHORITY OF STATES.—

''(i) IN GENERAL.—Whenever the attorney general of a State, or an official or agency designated by a State, has reason to believe that any person has engaged or is engaging in a pattern or practice of violating subsection (c) or (d) that has threatened or adversely affected or is threatening or adversely affecting an interest of the residents of that State, the State may bring a civil action against the person on behalf of the residents of the State for any relief permitted under clause (ii) of this subparagraph.

''(ii) RELIEF.—

''(I) IN GENERAL.—The plaintiff may seek the following relief in a civil action brought under clause (i):

''(aa) An injunction.

''(bb) An award that is the greater of—

''(AA) actual damages; or

''(BB) damages in the amount of $500 for each violation.

''(II) WILLFUL OR KNOWING VIOLATIONS.—In a civil action brought under clause (i), if the court finds that the defendant willfully or knowingly violated subsection (c) or (d), the court may, in its discretion, increase the amount of the award to not more than 3 times the amount available under subclause (I)(bb) of this clause.

''(B) INVESTIGATORY POWERS.—For purposes of bringing a civil action under this paragraph, nothing in this section shall prevent the attorney general of a State, or an official or agency designated by a State, from exercising the powers conferred on the attorney general or the official by the laws of the State to—

''(i) conduct investigations;

''(ii) administer oaths or affirmations; or

''(iii) compel the attendance of witnesses or the production of documentary and other evidence.

''(C) EFFECT ON STATE COURT PROCEEDINGS.—Nothing in this paragraph shall be construed to prohibit an authorized State official from proceeding in State court on the basis of an alleged violation of any general civil or criminal statute of the State.

''(D) ATTORNEY GENERAL DEFINED.—For purposes of this paragraph, the term 'attorney general' means the chief legal officer of a State.

''(3) VENUE; SERVICE OF PROCESS.—

''(A) VENUE.—A civil action brought under this subsection may be brought in the location where—

''(i) the defendant—

''(I) is found;

''(II) is an inhabitant; or

''(III) transacts business; or

''(ii) the violation occurred or is occurring.

''(B) SERVICE OF PROCESS.—Process in a civil action brought under this subsection may be served where the defendant—

''(i) is an inhabitant; or

''(ii) may be found.

''(g) OBLIGATIONS OF INTERACTIVE COMPUTER SERVICE.—A provider of an interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify the customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. The notice shall identify, or provide the customer with access to material identifying, current providers of such protections.

''(h) EFFECT ON OTHER LAWS.—

''(1) NO EFFECT ON CRIMINAL LAW.—Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this Act, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute.

''(2) NO EFFECT ON INTELLECTUAL PROPERTY LAW.—Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

''(3) STATE LAW.—Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

''(4) NO EFFECT ON COMMUNICATIONS PRIVACY LAW.—Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

''(5) NO EFFECT ON SEX TRAFFICKING LAW.—Nothing in this section (other than subsection (e)(2)(A)(i)) shall be construed to impair or limit—

''(A) any claim in a civil action brought under section 1595 of title 18, United States Code, if the conduct underlying the claim constitutes a violation of section 1591 of that title;

''(B) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 1591 of title 18, United States Code; or

''(C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18, United States Code, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

''(i) DEFINITIONS.—As used in this section:

''(1) ACCESS SOFTWARE PROVIDER.—The term 'access software provider' means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

''(A) Filter, screen, allow, or disallow material.

''(B) Pick, choose, analyze, or digest material.

''(C) Transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate material.

''(2) BROADBAND INTERNET ACCESS SERVICE.—The term 'broadband internet access service' has the meaning given the term in section 8.1(b) of title 47, Code of Federal Regulations, or any successor regulation.

''(3) COMMON CARRIER TECHNOLOGY COMPANY.—The term 'common carrier technology company' means a provider of an interactive computer service that—

''(A) offers its services to the public; and

''(B) has more than 100,000,000 worldwide active monthly users.

''(4) INFORMATION CONTENT PROVIDER.—

''(A) IN GENERAL.—The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of material provided through the internet or any other interactive computer service.

''(B) RESPONSIBILITY DEFINED.—For purposes of subparagraph (A), the term 'responsible, in whole or in part, for the creation or development of material' includes affirmatively and substantively contributing to,

modifying, altering, presenting with a reasonably discernible viewpoint, commenting upon, or editorializing about material provided by another person or entity.

''(5) INTERACTIVE COMPUTER SERVICE.—The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet and such systems operated or services offered by libraries or educational institutions.

''(6) INTERNET.—The term 'internet' means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

''(7) MATERIAL.—The term 'material' means any data, regardless of physical form or characteristic, including—

''(A) written or printed matter, information, automated information systems storage media, maps, charts, paintings, drawings, films, photographs, images, videos, engravings, sketches, working notes, or papers, or reproductions of any such things by any means or process; and

''(B) sound, voice, magnetic, or electronic recordings.''.

(b) CONFORMING AMENDMENTS.—

(1) COMMUNICATIONS ACT OF 1934.—The Communications Act of 1934 (47 U.S.C. 151 et seq.) is amended—

(A) in section 223(h)(2) (47 U.S.C. 223(h)(2)), by striking ''section 230(f)(2)'' and inserting ''section 232''; and

(B) in section 231(b)(4) (47 U.S.C. 231(b)(4)), by striking ''section 230'' and inserting ''section 232''.

(2) TRADEMARK ACT OF 1946.—Section 45 of the Act entitled ''An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes'', approved July 5, 1946 (commonly known as the ''Trademark Act of 1946'') (15 U.S.C. 1127) is amended by striking the definition relating to the term ''Internet'' and inserting the following:

''The term 'internet' has the meaning given that term in section 232 of the Communications Act of 1934.''.

(3) TITLE 17, UNITED STATES CODE.—Section 1401(g) of title 17, United States Code, is amended—

(A) by striking ''section 230 of the Communications Act of 1934 (47 U.S.C. 230)'' and inserting ''section 232 of the Communications Act of 1934''; and

(B) by striking ''subsection (e)(2) of such section 230'' and inserting ''subsection (h)(2) of such section 232''.

(4) TITLE 18, UNITED STATES CODE.—Part I of title 18, United States Code, is amended—

(A) in section 2257(h)(2)(B)(v), by striking ''section 230(c) of the Communications Act of 1934 (47 U.S.C. 230(c))'' and inserting ''section 232(e) of the Communications Act of 1934''; and

(B) in section 2421A—

(i) in subsection (a), by striking ''(as such term is defined in defined in section 230(f) the Communications Act of 1934 (47 U.S.C. 230(f)))'' and inserting ''(as that term is defined in section 232 of the Communications Act of 1934)''; and

(ii) in subsection (b), by striking ''(as such term is defined in defined in section 230(f) the Communications Act of 1934 (47 U.S.C. 230(f)))'' and inserting ''(as that term is defined in section 232 of the Communications Act of 1934)''.

(5) CONTROLLED SUBSTANCES ACT.—Section 401(h)(3)(A)(iii)(II) of the Controlled Substances Act (21 U.S.C. 841(h)(3)(A)(iii)(II)) is amended by striking ''section 230(c) of the Communications Act of 1934'' and inserting ''section 232(e) of the Communications Act of 1934''.

(6) WEBB-KENYON ACT.—Section 3(b)(1) of the Act entitled ''An Act divesting intoxicating liquors of their interstate character in certain cases'', approved March 1, 1913 (commonly known as the ''Webb-Kenyon Act'') (27 U.S.C. 122b(b)(1)) is amended by striking ''(as defined in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f))'' and inserting ''(as defined in section 232 of the Communications Act of 1934)''.

(7) TITLE 28, UNITED STATES CODE.—Section 4102 of title 28, United States Code, is amended—

(A) in subsection (c)—

(i) by striking ''section 230 of the Communications Act of 1934 (47 U.S.C. 230)'' and inserting ''section 232 of the Communications Act of 1934''; and

(ii) by striking ''section 230 if'' and inserting ''that section if''; and

(B) in subsection (e)(2), by striking ''section 230 of the Communications Act of 1934 (47 U.S.C. 230)'' and inserting ''section 232 of the Communications Act of 1934''.

(8) TITLE 31, UNITED STATES CODE.—Section 5362(6) of title 31, United States Code, is amended by striking ''section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f))'' and inserting ''section 232 of the Communications Act of 1934''.

(9) NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION ORGANIZATION ACT.—Section 157(e)(1) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 941(e)(1)) is amended, in the matter preceding subparagraph (A), by striking ''section 230(c) of the Communications Act of 1934 (47 U.S.C. 230(c))'' and inserting ''section 232(e) of the Communications Act of 1934''.

(c) APPLICABILITY.—Subsections (c) and (d) of section 232 of the Communications Act of 1934, as added by subsection (a), shall apply to a common carrier technology company on and after the date that is 90 days after the date of enactment of this Act.

SA 4703. 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 E of title XII, add the following:

SEC. 1253. STUDY ON THE CREATION OF AN OFFICIAL DIGITAL CURRENCY BY THE PEOPLE'S REPUBLIC OF CHINA.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the President shall submit to the appropriate committees of Congress a report on the short-, medium-, and long-term national security risks associated with the creation and use of the official digital renminbi of the People's Republic of China, including—

(1) risks arising from potential surveillance of transactions;

(2) risks related to security and illicit finance; and

(3) risks related to economic coercion and social control by the People's Republic of China.

(b) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form but may include a classified annex.

(c) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, the Committee on Appropriations, and the Select Committee on Intelligence of the Senate; and

(2) the Committee on Financial Services, the Committee on Foreign Affairs, the Committee on Appropriations, and the Permanent Select Committee on Intelligence of the House of Representatives.

SA 4704. 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 appropriate place, insert the following:

SEC. _____. SUBJECTING THE BUREAU OF CONSUMER FINANCIAL PROTECTION TO THE REGULAR APPROPRIATIONS PROCESS.

(a) IN GENERAL.—Section 1017 of the Consumer Financial Protection Act of 2010 (12 U.S.C. 5497) is amended—

(1) in subsection (a)—

(A) in the subsection heading, by striking ''TRANSFER OF FUNDS FROM BOARD OF GOVERNORS.—'' and inserting ''BUDGET AND FINANCIAL MANAGEMENT.—'';

(B) by striking paragraphs (1) through (3);

(C) by redesignating paragraphs (4) and (5) as paragraphs (1) and (2), respectively; and

(D) in paragraph (1), as so redesignated—

(i) in the paragraph heading, by striking ''BUDGET AND FINANCIAL MANAGEMENT.—'' and inserting ''IN GENERAL.—'';

(ii) by striking subparagraph (E); and

(iii) by redesignating subparagraph (F) as subparagraph (E);

(2) by striking subsections (b) and (c);

(3) by redesignating subsections (d) and (e) as subsections (b) and (c), respectively;

(4) in subsection (b), as so redesignated—

(A) in paragraph (2)—

(i) in the first sentence, by inserting ''direct'' before ''victims''; and

(ii) by striking the second sentence; and

(B) by adding at the end the following:

''(3) TREATMENT OF EXCESS AMOUNTS.—If, after the Bureau obtains a civil penalty in a judicial or administrative action under Federal consumer financial laws, deposits that civil penalty into the Civil Penalty Fund under paragraph (1), and, under paragraph (2), makes payments to all of the direct victims of activities for which that civil penalty was imposed, amounts remain in the Civil Penalty Fund with respect to that civil penalty, the Bureau shall transfer those excess amounts to the general fund of the Treasury.''; and

(5) in subsection (c), as so redesignated—

(A) by striking paragraphs (1) through (3) and inserting the following:

''(1) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such funds as may be necessary to carry out this title for fiscal year 2023.''; and

(B) by redesignating paragraph (4) as paragraph (2).

(b) EFFECTIVE DATE.—The amendments made by this section shall take effect on October 1, 2022.

SA 4705. 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 end of subtitle G of title X, add the following:

SEC. 1064. DECLASSIFICATION OF HISTORICAL FISA DECISIONS, ORDERS, AND OPINIONS OF SIGNIFICANCE.

(a) IN GENERAL.—Section 602 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1872) shall apply with respect to decisions, orders, and opinions by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as such terms are defined in section 601(e) of such Act (50 U.S.C. 1871(e))) that were issued before, on, or after the date of enactment of the USA FREEDOM Act of 2015 (Public Law 114–23; 129 Stat. 268).

(b) DEADLINE.—Not later than 1 year after the date of enactment of this Act, the Director of National Intelligence shall complete the review required under section 602 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1872) with respect to, and make publicly available to the greatest extent practicable in accordance with such section, each decision, order, and opinion described in subsection (a) of this section that was issued before the date of enactment of the USA FREEDOM Act of 2015 (Public Law 114–23; 129 Stat. 268).

SA 4706. Mr. COTTON 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 Defense 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 eliminate their dependence on non-allied countries for critical minerals to the maximum extent practicable.

(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 in detail 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 discontinuing the use of critical minerals from foreign entities of concern (as defined in section 9901(6) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (15 U.S.C. 4651(6))) 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.

SA 4707. Mr. WHITEHOUSE (for himself and Ms. HASSAN) submitted an amendment intended to be proposed by him 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. ____. INCREASING THE CAPACITY OF STATES AND PARTNER COUNTRIES TO COUNTER CORRUPTION AND MONEY LAUNDERING SCHEMES RELATED TO DRUG TRAFFICKING.

(a) SHORT TITLE.—This section may be cited as the ''Not Allowing Revenue for Criminal Organizations Act'' or ''NARCO Act''.

(b) FINDINGS.—Congress finds the following:

(1) Drug trafficking organizations, transnational criminal organizations, and money laundering organizations prey upon individuals suffering from substance use disorders and exploit the financial systems of the United States to sustain their criminal enterprises.

(2) The illicit drug trade in the United States is conservatively valued at $150,000,000,000 annually, making it worth more than the gross domestic product of approximately 150 countries.

(3) More than 93,000 individuals in the United States died from drug overdoses in 2020.

(4) Drug trafficking organizations, transnational criminal organizations, and money laundering organizations perpetuate crime, corruption, and kleptocracy, which undermines the rule of law and erodes democratic institutions in foreign countries while threatening the national security of the United States.

(5) Understanding and attacking the financial networks, both in the United States and abroad, that enable drug trafficking organizations, transnational criminal organizations, and money laundering organizations is critical to disrupting and dismantling those organizations.

(6) As such, the national drug control strategy of the United States should include an explicit focus, goals, and metrics related to mapping, tracking, attacking, and dismantling the financial networks of drug trafficking organizations, transnational criminal organizations, and money laundering organizations.

(7) Uniform application of anti-money laundering laws and information sharing will enhance the ability of the Federal Government and State governments to dismantle drug trafficking organizations, transnational criminal organizations, and money laundering organizations.

(8) The Financial Action Task Force establishes international standards that aim to prevent money laundering associated with the illicit drug trade and other illegal activities, and is supported by more than 200 implementing countries and jurisdictions, including the United States. In its 2016 Mutual Evaluation Report of the United States, the Task Force found that while Federal law enforcement agencies aggressively target money laundering cases, ''State law enforcement authorities can complement Federal efforts, but more typically pursue State-level law enforcement priorities. Among the States, there is no uniform approach and little data is available. Where information was provided, it tended to suggest that [money laundering] is not prioritised by the State authorities.''.

(9) It is in the best national security interest of the United States to increase the capacity of States and partner countries to identify, investigate, and prosecute corruption and money laundering schemes that directly benefit drug trafficking organizations, transnational criminal organizations, and money laundering organizations.

(c) GAO REPORT.—

(1) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, and annually thereafter, the Comptroller General of the United States shall submit to the Committee on the Judiciary of the Senate, the Caucus on International Narcotics Control of the Senate, the Committee on the Judiciary of the House of Representatives, and the Director of National Drug Control Policy an assessment of—

(A) the number and status of investigations and prosecutions across National Drug Control Program agencies (as defined in section 702 of the Office of National Drug Control Policy Reauthorization Act of 1998 (21 U.S.C. 1701)) with a drug trafficking and money laundering and illicit finance nexus, unless the disclosure of such information would reveal information protected by rule 6(e) of the Federal Rules of Criminal Procedure or a court order; and

(B) the amount of money and other things of value in various forms, including tangible and digital assets, and property criminally seized by or forfeited to the Federal Government on an annual basis from individuals associated with drug trafficking, drug trafficking organizations, transnational criminal organizations, or money laundering organizations, which shall be—

(i) adjusted to eliminate duplication in the case of seizures or forfeitures carried out and reported by multiple agencies; and

(ii) disaggregated by agency.

(2) CLASSIFIED ANNEX.—The Comptroller General may provide the assessment under paragraph (1), or a portion thereof, in a classified annex if necessary.

(d) TECHNICAL UPDATES TO OFFICE OF NATIONAL DRUG CONTROL POLICY REAUTHORIZATION ACT OF 1998.—

(1) DEFINITION OF ''SUPPLY REDUCTION''.—Section 702(17) of the Office of National Drug Control Policy Reauthorization Act of 1998 (21 U.S.C. 1701(17)) is amended—

(A) by redesignating subparagraphs (G) and (H) as subparagraphs (H) and (I), respectively; and

(B) by inserting after subparagraph (F) the following:

''(G) activities to map, track, dismantle, and disrupt the financial networks of drug trafficking organizations, transnational criminal organizations, and money laundering organizations involved in the manufacture and trafficking of drugs in the United States and in foreign countries;''.

(2) CONTENTS OF NATIONAL DRUG CONTROL STRATEGY.—Section 706(c)(1)(L) of the Office of National Drug Control Policy Reauthorization Act of 1998 (21 U.S.C. 1705(c)(1)(L)) is amended by inserting before the period at the end the following: '', which statistical data shall include, to the greatest extent practicable, the information submitted to the Director by the Comptroller General of the United States in the 2 most recent annual reports under subsection (c) of the Not Allowing Revenue for Criminal Organizations Act''.

(e) MODEL LAWS.—

(1) IN GENERAL.—The Attorney General shall enter into an agreement with a nongovernmental organization, which may include an institution of higher education, to—

(A) advise States on establishing laws and policies to address money laundering practices related to the manufacture, sale, or trafficking of illicit drugs;

(B) develop model State laws pertaining to money laundering practices related to the sale or trafficking of illicit drugs; and

(C) revise the model State laws described in subparagraph (B) and draft supplementary model State laws that take into consideration changes in the trafficking of illicit drugs and related money laundering schemes in the State involved.

(2) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $300,000 for each of fiscal years 2022 through 2026 to carry out this subsection.

(f) COUNTERING INTERNATIONAL ILLICIT FINANCE TECHNIQUES USED BY CRIMINAL ORGANIZATIONS.—

(1) IN GENERAL.—The Attorney General, in consultation with the Director of the Financial Crimes Enforcement Network of the Department of the Treasury, shall provide training, technical assistance, and mentorship, through the International Criminal Investigative Training Assistance Program and the Office of Overseas Prosecutorial Development, Assistance, and Training, to foreign countries that have been designated as major money laundering countries under section 489 of the Foreign Assistance Act of 1961 (22 U.S.C. 2291h) in order to—

(A) increase the institutional capacity of those countries to prevent corruption and swiftly address corruption when it occurs;

(B) implement justice sector reform to ensure the successful prosecution of drug trafficking organizations, transnational criminal organizations, money laundering organizations, and other entities or individuals involved in the illicit drug trade;

(C) better understand, map, target, and attack the financial networks of drug trafficking organizations, transnational criminal organizations, and other entities or individuals involved in the illicit drug trade;

(D) develop and implement laws and regulations to establish or strengthen asset forfeiture programs; and

(E) develop and implement laws and regulations to counter corruption, money laundering, and illicit finance techniques used by drug trafficking organizations, transnational criminal organizations, money laundering organizations, and other entities or individuals involved in the illicit drug trade.

(2) ANNUAL REPORT.—Not later than 120 days after the end of each fiscal year, beginning with fiscal year 2023, the Attorney General shall submit a report to the Committee on the Judiciary of the Senate, the Caucus on International Narcotics Control of the Senate, and the Committee on the Judiciary of the House of Representatives that includes, with respect to each country that received training, technical assistance, and mentorship under paragraph (1) during that fiscal year—

(A) the type and duration of training, technical assistance, and mentorship provided to the country;

(B) the implementation status of new laws and regulations to counter corruption, money laundering, and illicit finance techniques used by drug trafficking organizations, transnational criminal organizations, money laundering organizations, and other entities or individuals involved in the illicit drug trade in the country;

(C) the number of money laundering and illicit finance investigations, prosecutions, and convictions related to the narcotics trade that were undertaken in the country;

(D) the amount of money and other things of value in various forms, including tangible and digital assets, and property criminally seized by or forfeited to the Federal Government from drug trafficking organizations, transnational criminal organizations, money laundering organizations, and other entities or individuals involved in the illicit drug trade, in the country; and

(E) the number of joint investigations that United States undertook with the country and whether those investigations led to prosecutions or convictions.

(3) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $80,000,000 for each of fiscal years 2022 through 2026 to carry out this subsection.

SA 4708. Mr. WHITEHOUSE (for himself and Mr. GRASSLEY) submitted an amendment intended to be proposed by him 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. ESTABLISHMENT OF AFGHAN WORKING GROUP AND AFGHAN THREAT FINANCE CELL.

(a) AFGHAN WORKING GROUP.—

(1) ESTABLISHMENT.—Not later than 90 days after the date of the enactment of this Act, the President shall establish an interagency organization to be known as the ''Afghan Working Group''.

(2) MISSION.—The mission of the Afghan Working Group shall be—

(A) to reduce the manufacture, sale, and distribution of illicit narcotics from Afghanistan;

(B) to identify, disrupt, and eliminate illicit financial networks in Afghanistan, particularly—

(i) such networks involved in narcotics trafficking, illicit financial transactions (including through the use of domestic and international professional money launderers), and official corruption; and

(ii) terrorist networks; and

(C) to promote the rule of law in Afghanistan.

(3) MEMBERSHIP.—The Afghan Working Group shall be convened by the Assistant to the President for National Security Affairs and consist of representatives from the following agencies:

(A) The Department of the Treasury.

(B) The Department of Justice.

(C) The Drug Enforcement Administration.

(D) The Department of State.

(E) The Department of Defense.

(F) The Federal Bureau of Investigation.

(G) The Internal Revenue Service.

(H) The Department of Homeland Security.

(I) The Defense Intelligence Agency.

(J) The Office of Foreign Assets Control of the Department of the Treasury.

(K) The Central Intelligence Agency.

(L) The Financial Crimes Enforcement Network of the Department of Treasury.

(M) The Bureau of International Narcotics Control and Law Enforcement Affairs.

(N) The Office of National Drug Control Policy.

(O) Any other law enforcement agency or element of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) the Assistant to the President for National Security Affairs considers appropriate.

(4) COORDINATION.—The Afghan Working Group shall regularly coordinate and consult with regional anti-corruption bodies, financial intelligence units, the international Financial Action Task Force, and the Special Inspector General for Afghanistan Reconstruction.

(5) BRIEFINGS.—

(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, and annually thereafter, the Afghan Working Group shall provide to the appropriate committees of Congress a briefing on the activities of the Afghan Working Group.

(B) ELEMENTS.—Each briefing under subparagraph (A) shall include the following:

(i) An assessment of the activities undertaken by, and the effectiveness of, the Afghan Working Group with respect to—

(I) reducing the manufacture, sale, and distribution of illicit narcotics from Afghanistan;

(II) identifying, disrupting, and eliminating illicit financial networks in Afghanistan, particularly—

(aa) such networks involved in narcotics trafficking, illicit financial transactions (including through the use of domestic and international professional money launderers), and official corruption; and

(bb) terrorist networks; and

(III) promoting the rule of law in Afghanistan.

(ii) Recommendations to Congress on legislative or regulatory improvements necessary to support the efforts described in subclauses (I) through (III) of clause (i).

(C) FORM.—A briefing under subparagraph (A) may be provided in classified form.

(b) AFGHAN THREAT FINANCE CELL.—

(1) ESTABLISHMENT.—Not later than 90 days after the date on which the Afghan Working Group is established, the Afghan Working Group shall establish an interagency organization to be known as the ''Afghan Threat Finance Cell''.

(2) MISSION.—The mission of the Afghan Threat Finance Cell shall be to identify, disrupt, and eliminate illicit financial networks in Afghanistan, particularly—

(A) such networks involved in narcotics trafficking, illicit financial transactions (including through the use of domestic and international professional money launderers), and official corruption; and

(B) terrorist networks.

(3) LEAD AGENCIES.—The Department of the Treasury shall serve as the lead agency of the Afghan Threat Finance Cell, and the Drug Enforcement Administration and the Department of Defense shall serve as the co-deputy lead agencies of the Afghan Threat Finance Cell.

(4) COORDINATION.—The Afghan Threat Finance Cell shall regularly coordinate and consult with regional financial intelligence units, the international Financial Action Task Force, and the Special Inspector General for Afghanistan Reconstruction.

(5) BRIEFINGS.—

(A) REQUIREMENT.—Not later than one year after the date of the enactment of this Act, and annually thereafter, the Afghan Threat Finance Cell shall provide to the appropriate committees of Congress a briefing on the activities of the Afghan Threat Finance Cell.

(B) ELEMENTS.—Each briefing under subparagraph (A) shall include the following:

(i) An assessment of the activities undertaken by, and the effectiveness of, the Afghan Threat Finance Cell in identifying, disrupting, and eliminating illicit financial networks in Afghanistan, particularly—

(I) such networks involved in narcotics trafficking, illicit financial transactions, (including through the use of domestic and international professional money launderers), and official corruption; and

(II) terrorist networks.

(ii) Recommendations to Congress on legislative or regulatory improvements necessary to support the identification, disruption, and elimination of illicit financial networks in Afghanistan.

(C) FORM.—A briefing under subparagraph (A) may be provided in classified form.

(c) TERMINATION.—

(1) IN GENERAL.—Subject to paragraph (2), the Afghan Working Group and the Afghan Threat Finance Cell shall terminate on the date that is three years after the date of the enactment of this Act.

(2) EXTENSION.—The President may extend the termination date under paragraph (1) for the Afghan Working Group, the Afghan Threat Finance Cell, or both, as necessary.

(d) APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) The Committee on Banking, Housing, and Urban Affairs, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Committee on Armed Services of the Senate, and the Senate Caucus on International Narcotics Control; and

(2) The Committee on Financial Services, the Committee on Oversight and Reform, the Committee on the Judiciary, and the Committee on Armed Services of the House of Representatives.

SA 4709. Mr. VAN HOLLEN (for himself and Mr. SULLIVAN) 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 X, add the following:

Subtitle H—Foreign Service Families Act of 2021

SECTION 1071. SHORT TITLE.

This subtitle may be cited as the ''Foreign Service Families Act of 2021''.

SEC. 1072. TELECOMMUTING OPPORTUNITIES.

(a) DETO POLICY.—

(1) IN GENERAL.—Each Federal department and agency shall establish a policy enumerating the circumstances under which employees may be permitted to temporarily perform work requirements and duties from approved overseas locations where there is a related Foreign Service assignment pursuant to an approved Domestically Employed Teleworking Overseas (DETO) agreement.

(2) PARTICIPATION.—The policy described under paragraph (1) shall—

(A) ensure that telework does not diminish employee performance or agency operations;

(B) require a written agreement that—

(i) is entered into between an agency manager and an employee authorized to telework, that outlines the specific work arrangement that is agreed to; and

(ii) is mandatory in order for any employee to participate in telework;

(C) provide that an employee may not be authorized to telework if the performance of that employee does not comply with the terms of the written agreement between the agency manager and that employee;

(D) except in emergency situations as determined by the head of an agency, not apply to any employee of the agency whose official duties require on at least a monthly basis—

(i) direct handling of secure materials determined to be inappropriate for telework by the agency head; or

(ii) on-site activity that cannot be handled remotely or at an alternate worksite;

(E) be incorporated as part of the continuity of operations plans of the agency in the event of an emergency; and

(F) enumerate the circumstances under which employees may be permitted to temporarily perform work requirements and duties from approved overseas locations.

(b) ACCESS TO ICASS SYSTEM.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall revise chapter 900 of volume 6 of the Foreign

Affairs Manual, the International Cooperative Administrative Support Services Handbook, the Personnel Operations Handbook, and any other relevant regulations to allow each Federal agency that has enacted a policy under subsection (a) to have access to the International Cooperative Administrative Support Services (ICASS) system.

SEC. 1073. EMPLOYMENT AND EDUCATION PROGRAMS FOR ELIGIBLE FAMILY MEMBERS OF MEMBERS OF THE FOREIGN SERVICE.

Section 706(b) of the Foreign Service Act of 1980 (22 U.S.C. 4026(b)) is amended—

(1) in paragraph (1)—

(A) by striking ''The Secretary may facilitate the employment of spouses of members of the Foreign Service by—'' and inserting ''The Secretary shall implement such measures as the Secretary considers necessary to facilitate the employment of spouses and members of the Service. The measures may include—''; and

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

(C) by amending subparagraph (C) to read as follows:

''(C) establishing a program for assisting eligible family members in accessing employment and education opportunities, as appropriate, including by exercising the authorities, in relevant part, under sections 1784 and 1784a of title 10, United States Code, and subject to such regulations as the Secretary may prescribe modeled after those prescribed pursuant to subsection (b) of such section 1784;'';

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

(3) by inserting after paragraph (1) the following new paragraphs:

''(2) The Secretary may prescribe regulations—

''(A) to provide preference to eligible family members in hiring for any civilian position in the Department, notwithstanding the prohibition on marital discrimination found in 5 U.S.C. 2302(b)(1)(E), if —

''(i) the eligible family member is among persons determined to be best qualified for the position; and

''(ii) the position is located in the overseas country of assignment of their sponsoring employee;

''(B) to ensure that notice of any vacant position in the Department is provided in a manner reasonably designed to reach eligible family members of sponsoring employees whose permanent duty stations are in the same country as that in which the position is located; and

''(C) to ensure that an eligible family member who applies for a vacant position in the Department shall, to the extent practicable, be considered for any such position located in the same country as the permanent duty station of their sponsoring employee.

''(3) Nothing in this section may be construed to provide an eligible family member with entitlement or preference in hiring over an individual who is preference eligible.

''(4) Under regulations prescribed by the Secretary, a chief of mission may, consistent with all applicable laws and regulations pertaining to the ICASS system, make available to an eligible family member and a non-Department entity space in an embassy or consulate for the purpose of the non-Department entity providing employment-related training for eligible family members.

''(5) The Secretary may work with the Director of the Office of Personnel Management and the heads of other Federal departments and agencies to expand and facilitate the use of existing Federal programs and resources in support of eligible family member employment.''; and

(4) by adding after paragraph (6), as redesignated by paragraph (2) of this subsection, the following new paragraph:

''(7) In this subsection, the term 'eligible family member' refers to family members of government employees assigned abroad or hired for service at their post of residence who are appointed by the Secretary of State or the Administrator of the United States Agency for International Development pursuant to sections 102, 202, 303, and 311.''.

SEC. 1074. BRIEFING ON FOREIGN SERVICE FAMILY RESERVE CORPS.

(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary of State shall brief the appropriate congressional committees on the status of implementation of the Foreign Service Family Reserve Corps.

(b) ELEMENTS.—The briefing required under subsection (a) shall include the following elements:

(1) A description of the status of implementation of the Foreign Service Family Reserve Corps (FSFRC).

(2) An assessment of the extent to which implementation was impacted by the Department's hiring freeze and a detailed explanation of the effect of any such impacts.

(3) A description of the status of implementation of a hiring preference for the FSFRC.

(4) A detailed accounting of any individuals eligible for membership in the FSFRC who were unable to begin working at a new location as a result of being unable to transfer their security clearance, including an assessment of whether they would have been able to port their clearance as a member of the FSFRC if the program had been fully implemented.

(5) An estimate of the number of individuals who are eligible to join the FSFRC worldwide and the categories, as detailed in the Under Secretary for Management's guidance dated May 3, 2016, under which those individuals would enroll.

(6) An estimate of the number of individuals who are enrolled in the FSFRC worldwide and the categories, as detailed in the Under Secretary for Management's guidance dated May 3, 2016, under which those individuals enrolled.

(7) An estimate of the number of individuals who were enrolled in each phase of the implementation of the FSFRC as detailed in guidance issued by the Under Secretary for Management.

(8) An estimate of the number of individuals enrolled in the FSFRC who have successfully transferred a security clearance to a new post since implementation of the program began.

(9) An estimate of the number of individuals enrolled in the FSFRC who have been unable to successfully transfer a security clearance to a new post since implementation of the program began.

(10) An estimate of the number of individuals who have declined in writing to apply to the FSFRC.

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on Foreign Relations and the Committee on Appropriations of the Senate; and

(2) the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives.

SEC. 1075. TREATMENT OF FAMILY MEMBERS SEEKING POSITIONS CUSTOMARILY FILLED BY FOREIGN SERVICE OFFICERS OR FOREIGN NATIONAL EMPLOYEES.

Section 311 of the Foreign Service Act of 1980 (22 U.S.C. 3951) is amended by adding at the end the following:

''(e) The Secretary shall hold a family member of a government employee described in subsection (a) seeking employment in a position described in that subsection to the same employment standards as those applicable to Foreign Service officers, Foreign Service personnel, or foreign national employees seeking the same or a substantially similar position.''.

SEC. 1076. IN-STATE TUITION RATES FOR MEMBERS OF QUALIFYING FEDERAL SERVICE.

(a) IN GENERAL.—Section 135 of the Higher Education Act of 1965 (20 U.S.C. 1015d) is amended—

(1) in the section heading, by striking ''**THE ARMED FORCES ON ACTIVE DUTY, SPOUSES, AND DEPENDENT CHILDREN**'' and inserting ''**QUALIFYING FEDERAL SERVICE**'';

(2) in subsection (a), by striking ''member of the armed forces who is on active duty for a period of more than 30 days and'' and inserting ''member of a qualifying Federal service'';

(3) in subsection (b), by striking ''member of the armed forces'' and inserting ''member of a qualifying Federal service''; and

(4) by striking subsection (d) and inserting the following:

''(d) DEFINITIONS.—In this section, the term 'member of a qualifying Federal service' means—

''(1) a member of the armed forces (as defined in section 101 of title 10, United States Code) who is on active duty for a period of more than 30 days (as defined in section 101 of title 10, United States Code); or

''(2) a member of the Foreign Service (as defined in section 103 of the Foreign Service Act of 1980 (22 U.S.C. 3903)) who is on active duty for a period of more than 30 days.''.

(b) EFFECTIVE DATE.—The amendments made under subsection (a) shall take effect at each public institution of higher education in a State that receives assistance under the Higher Education Act of 1965 (20 U.S.C. 1001 et seq.) for the first period of enrollment at such institution that begins after July 1, 2023.

SEC. 1077. TERMINATION OF RESIDENTIAL OR MOTOR VEHICLE LEASES AND TELEPHONE SERVICE CONTRACTS FOR CERTAIN MEMBERS OF THE FOREIGN SERVICE.

(a) IN GENERAL.—Chapter 9 of title I of the Foreign Service Act of 1980 (22 U.S.C. 4081 et seq.) is amended by adding at the end the following new section:

''SEC. 907. TERMINATION OF RESIDENTIAL OR MOTOR VEHICLE LEASES AND TELEPHONE SERVICE CONTRACTS.

''The terms governing the termination of residential or motor vehicle leases and telephone service contracts described in sections 305 and 305A, respectively of the Servicemembers Civil Relief Act (50 U.S.C. 3955 and 3956) with respect to servicemembers who receive military orders described in such Act shall apply in the same manner and to the same extent to members of the Service who are posted abroad at a Foreign Service post in accordance with this Act.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 2 of the Foreign Service Act of 1980 is amended by inserting after the item relating to section 906 the following new item:

''Sec. 907. Termination of residential or motor vehicle leases and telephone service contracts.''.

SA 4710. Mr. CASSIDY (for himself and Mr. SCHATZ) 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. RESEARCH ENDOWMENTS AT BOTH CURRENT AND FORMER CENTERS OF EXCELLENCE.

Paragraph (1) (beginning with ''(1) IN GENERAL'') of section 464z–3(h) of the Public Health Service Act (42 U.S.C. 285t(h)) is amended to read as follows:

''(1) IN GENERAL.—The Director of the Institute may carry out a program to facilitate minority health disparities research and other health disparities research by providing for research endowments—

''(A) at current or former centers of excellence under section 736; and

''(B) at current or former centers of excellence under section 464z–4.''.

SA 4711. Mr. MCCONNELL (for himself, Mr. DURBIN, Mr. YOUNG, Mr. GRASSLEY, Mr. GRAHAM, Mr. HAGERTY, and Mr. CARDIN) 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. SUPPORTING DEMOCRACY IN BURMA.

(a) DEFINED TERM.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on Foreign Relations of the Senate;

(2) the Committee on Foreign Affairs of the House of Representatives;

(3) the Committee on Appropriations of the Senate;

(4) the Committee on Appropriations of the House of Representatives;

(5) the Committee on Armed Services of the Senate;

(6) the Committee on Armed Services of the House of Representatives;

(7) the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(8) the Committee on Financial Services of the House of Representatives.

(b) BRIEFING REQUIRED.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the following officials shall jointly brief the appropriate congressional committees regarding actions taken by the United States Government to further United States policy and security objectives in Burma (officially known as the ''Republic of the Union of Myanmar''):

(A) The Assistant Secretary of State for East Asian and Pacific Affairs.

(B) The Counselor of the Department of State.

(C) The Under Secretary of the Treasury for Terrorism and Financial Intelligence.

(D) The Assistant to the Administrator for the Bureau for Conflict Prevention and Stabilization.

(E) Additional officials from the Department of Defense or the Intelligence Community, as appropriate.

(2) INFORMATION REQUIRED.—The briefing required under paragraph (1) shall include—

(A) a detailed description of the specific United States policy and security objectives in Burma;

(B) information about any actions taken by the United States, either directly or in coordination with other countries—

(i) to support and legitimize the National Unity Government of the Republic of the Union of Myanmar, The Civil Disobedience Movement in Myanmar, and other entities promoting democracy in Burma, while simultaneously denying legitimacy and resources to the Myanmar's military junta;

(ii) to impose costs on Myanmar's military junta, including—

(I) an assessment of the impact of existing United States and international sanctions; and

(II) a description of potential prospects for additional sanctions;

(iii) to secure the restoration of democracy, the establishment of inclusive and representative civilian government, with a reformed military reflecting the diversity of Burma and under civilian control, and the enactment of constitutional, political, and economic reform in Burma;

(iv) to secure the unconditional release of all political prisoners in Burma;

(v) to promote genuine national reconciliation among Burma's diverse ethnic and religious groups;

(vi) to ensure accountability for atrocities, human rights violations, and crimes against humanity committed by Myanmar's military junta; and

(vii) to avert a large-scale humanitarian disaster;

(C) an update on the current status of United States assistance programs in Burma, including—

(i) humanitarian assistance for affected populations, including internally displaced persons and efforts to mitigate humanitarian and health crises in neighboring countries and among refugee populations;

(ii) democracy assistance, including support to the National Unity Government of the Republic of the Union of Myanmar and civil society groups in Burma;

(iii) economic assistance; and

(iv) global health assistance, including COVID–19 relief; and

(D) a description of the strategic interests in Burma of the People's Republic of China and the Russian Federation, including—

(i) access to natural resources and lines of communications to sea routes; and

(ii) actions taken by such countries—

(I) to support Myanmar's military junta in order to preserve or promote such interests;

(II) to undermine the sovereignty and territorial integrity of Burma; and

(III) to promote ethnic conflict within Burma.

(c) CLASSIFICATION AND FORMAT.—The briefing required under subsection (b)—

(1) shall be provided in an unclassified setting; and

(2) may be accompanied by a separate classified briefing, as appropriate.

SA 4712. Mr. WHITEHOUSE (for himself and Mr. PORTMAN) 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. RESEARCH INTO NON-OPIOID PAIN MANAGEMENT.

(a) IN GENERAL.—The Secretary of Health and Human Services shall conduct or support research and surveillance with respect to non-opioid methods of pain management, including non-pharmaceutical remedies for pain and integrative medicine solutions.

(b) AUTHORIZATION OF APPROPRIATIONS.—For purposes of conducting research under this section, there are authorized to be appropriated such sums as may be necessary for each of fiscal years 2022 through 2026.

SA 4713. Mr. PADILLA 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 XII, add the following:

SEC. 1264. REPORT ON NAGORNO KARABAKH CONFLICT.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State, in consultation with the Secretary of Defense, shall submit to the congressional defense committees, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate a report on the 2020 conflict in Nagorno Karabakh.

(b) ELEMENTS.—The report required by subsection (a) shall include the following:

(1) An assessment of the use of weapon systems produced outside either country that was a party to the 2020 conflict in Nagorno Karabakh that were employed in the conflict, including a list of the origins of those weapon systems.

(2) An assessment of the use of white phosphorous or cluster bombs in the conflict.

(3) A description of the involvement of foreign actors in the conflict, including a description of the military activities, influence operations, and diplomatic engagement by foreign countries before, during, and after the conflict, as well as any effort by parties to the conflict or foreign actors to recruit or employ foreign fighters during the conflict.

(4) Any other matter the Secretary of State considers important.

SA 4714. Mr. REED (for himself and Mr. INHOFE) 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 A of title V, add the following:

SEC. 503. AUTHORITY TO VARY NUMBER OF SPACE FORCE OFFICERS CONSIDERED FOR PROMOTION TO MAJOR GENERAL.

(a) IN GENERAL.—Notwithstanding section 616(d) of title 10, United States Code, the number of officers recommended for promotion by a selection board convened by the Secretary of the Air Force under section 611(a) of title 10, United States Code, to consider officers on the Space Force active duty list for promotion to major general may not exceed the number equal to 95 percent of the total number of brigadier generals eligible for consideration by the board.

(b) TERMINATION.—The authority provided under subsection (a) shall terminate on December 31, 2022.

SA 4715. Mr. ROUNDS (for Mr. INHOFE) 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. EXPANSION OF PROPERTY OF DEPARTMENT OF DEFENSE NOT ELIGIBLE FOR SALE OR DONATION FOR LAW ENFORCEMENT ACTIVITIES AND STUDY ON USE OF SUCH AUTHORITY TO SELL OR DONATE PROPERTY.

(a) IN GENERAL.—Section 2576a(e) of title 10, United States Code, is amended by adding at the end the following new paragraphs:

''(5) Explosives.

''(6) Firearms of 50 cal mil or greater and ammunition of 50 cal mil or greater.

''(7) Asphyxiating gases, including those comprised of lachrymatory agents, and analogous liquids, materials, or devices.''.

(b) STUDY.—

(1) IN GENERAL.—The Director of the Defense Logistics Agency shall conduct a study on the use by the Department of Defense of the authority under section 2576a of title 10, United States Code, and the administration of such authority by the Law Enforcement Support Office of the Department.

(2) ELEMENTS.—The study required under paragraph (1) shall include—

(A) an analysis of the degree to which personal property transferred under section 2576a of title 10, United States Code, has been distributed equitably between larger, well-resourced municipalities and units of government and smaller, less well-resourced municipalities and units of government; and

(B) an identification of potential modifications to the authority under such section to ensure that property transferred under such section is transferred in a manner that provides adequate opportunity for participation by smaller, less well-resourced municipalities and units of government.

(3) REPORT.—Not later than December 1, 2022, the Director of the Defense Logistics Agency shall submit to the congressional defense committees a report on the results of the study conducted under paragraph (1).

SA 4716. Mr. HAGERTY (for himself and 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:

At the end of subtitle E of title III, add the following:

SEC. 376. ACCESS TO CATEGORY 3 SUBTERRANEAN TRAINING FACILITIES.

(a) IN GENERAL.—The Secretary of Defense may have access to a covered category 3 subterranean training facility on a continuing basis, subject to the availability of appropriations for such purpose.

(b) AUTHORITY TO ENTER INTO LEASE.—The Secretary may enter into a short-term lease with a provider of a covered category 3 subterranean training facility for purposes of subsection (a).

(c) COVERED CATEGORY 3 SUBTERRANEAN TRAINING FACILITY DEFINED.—In this section, the term ''covered category 3 subterranean training facility'' means a category 3 subterranean training facility that is—

(1) operational as of the date of the enactment of this Act; and

(2) determined by the Secretary to be safe for use as of such date.

SA 4717. Mr. BROWN 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 ____—STEM RESEARCH GAINS

SEC. ___01. SHORT TITLE.

This title may be cited as the ''Strengthening the STEM Research Workforce to Generate American Infrastructure for National Security Act of 2021'' or the ''STEM Research GAINS Act of 2021''.

SEC. ___02. DEFINITIONS.

In this title:

(1) COVERED FIELD.—The term ''covered field'' means a field in science, technology, engineering, or mathematics research or development that is determined to be—

(A) a subject area relating to the national security of the United States;

(B) a subject area relating to the United States' ability to compete in an open, fair, and competitive international market and achieve economic growth; or

(C) a subject area that is in need of expanded and strengthened academic pipelines to ensure a diverse workforce.

(2) DIRECTOR.—The term ''Director'' means the Director of the National Science Foundation.

(3) FEDERAL SCIENCE AGENCY.—The term ''Federal science agency'' has the meaning given the term in section 103(f) of the America COMPETES Reauthorization Act of 2010 (42 U.S.C. 6623(f)).

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

(5) MINORITY.—The term ''minority'' has the meaning given the term in section 365(2) of the Higher Education Act of 1965 (20 U.S.C. 1067k(2)).

(6) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means—

(A) a part B institution (as defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061));

(B) a Hispanic-serving institution (as defined in section 502 of that Act (20 U.S.C. 1101a));

(C) a Tribal College or University (as defined in section 316 of that Act (20 U.S.C. 1059c));

(D) an Alaska Native-serving institution (as defined in section 317(b) of that Act (20 U.S.C. 1059d(b)));

(E) a Native Hawaiian-serving institution (as defined in section 317(b) of that Act (20 U.S.C. 1059d(b)));

(F) a Predominantly Black Institution (as defined in section 318 of that Act (20 U.S.C. 1059e));

(G) an Asian American and Native American Pacific Islander-serving institution (as defined in section 320(b) of that Act (20 U.S.C. 1059g(b))); or

(H) a Native American-serving, nontribal institution (as defined in section 319 of that Act (20 U.S.C. 1059f)).

(7) STEM.—The term ''STEM'' means science, technology, engineering, and mathematics, including computer science.

(8) UNDERREPRESENTED FIELD.—The term ''underrepresented field'' means a field in STEM in which the national rate of representation of women among tenured, tenure-track faculty, or nonfaculty researchers at doctorate-granting institutions of higher education is less than 25 percent, according to the most recent data available from the National Center for Science and Engineering Statistics.

(9) UNDERREPRESENTED IN SCIENCE AND ENGINEERING.—The term ''underrepresented in science and engineering'' means a minority group whose number of scientists and engineers, per 10,000 population of that group, is substantially below the comparable figure for scientists and engineers who are white and not of Hispanic origin, as determined by the Secretary of Education under section 637.4(b) of title 34, Code of Federal Regulations, or similar successor regulations.

Subtitle A—Expanding Pipeline Programs to Research Opportunities

SEC. ___11. RESEARCH AND DEVELOPMENT AREAS CRITICAL TO NATIONAL SECURITY.

(a) COVERED FIELDS.—The President shall conduct a study to identify areas for research and development that are covered fields.

(b) UPDATE.—Not less than once every 5 years, the President shall reassess the covered fields.

SEC. ___12. INCREASING INVESTMENT IN UNDERGRADUATE SCIENCE PIPELINES.

(a) IN GENERAL.—There are authorized to be appropriated to the National Science Foundation for fiscal year 2022 and for each of the following 4 years, $750,000,000, which shall be used by the Director for the following National Science Foundation programs:

(1) The Historically Black Colleges and Universities Undergraduate Program.

(2) The Louis Stokes Alliances for Minority Participation program.

(3) The Research Experiences for Undergraduates program.

(4) The Tribal Colleges and Universities Program.

(5) The Improving Undergraduates STEM Education: Hispanic-Serving Institutions Program.

(6) Other programs to broaden participation in undergraduate STEM programs, as determined by the Director.

(b) SUPPLEMENT NOT SUPPLANT.—The amounts used under subsection (a) shall supplement, and not supplant, any other amounts used by the National Science Foundation for the programs described in such subsection.

SEC. ___14. BOLSTERING STEM PIPELINES STRATEGIC PLAN.

(a) BROADENING PARTICIPATION STRATEGIC PLAN.—Not later than 1 year after the date of enactment of this Act, the Subcommittee on Federal Coordination in Science, Technology, Engineering, and Mathematics Education (FC-STEM) of the Committee on Science, Technology, Engineering, and Mathematics Education (CoSTEM) of the National Science and Technology Council shall submit to Congress a report containing the subcommittee's current strategic plan for Federal science agencies to increase the capacity of STEM programs carried out by Federal science agencies that are in effect as of the date of the report to increase the participation of individuals who are underrepresented in science and engineering, women who are underrepresented in STEM fields, and low-income and first-generation college students, in order to broaden participation in grants and programs carried out by the Federal science agencies. The report shall include—

(1) a description of how the grants and programs that are carried out by the Federal science agencies, as of the time of the report, are carried out in a manner that advances diverse pipelines in STEM fields, and a description of how the Federal science agencies can better advance such diverse pipelines;

(2) an analysis of the data collection that would allow for meaningful goal setting and transparency relating to the Federal science agencies' progress in broadening participation of individuals from groups that are underrepresented in science and engineering with respect to those grants and programs;

(3) an analysis of how the Federal science agencies can meet goals related to broadening the participation of individuals from groups that are underrepresented in science and engineering by—

(A) creating or expanding funding opportunities;

(B) modifying existing research and development programs; and

(C) establishing coordination between existing programs carried out by the Federal science agencies;

(4) a description of the ways that the Federal science agencies work with minority-serving institutions to—

(A) enable those eligible institutions to compete effectively for grants, contracts, or cooperative agreements carried out by the National Science Foundation;

(B) encourage those eligible institutions to participate in programs carried out by the Federal science agencies; and

(C) encourage students and faculty, particularly minority students and faculty and students and faculty in underrepresented fields, at the eligible institution to apply for and successfully earn graduate and professional opportunities from programs supported by the Federal science agencies;

(5) an analysis of the best ways to share best practices for institutions of higher education and Federal science agencies interested in supporting individuals from groups that are underrepresented in science and engineering;

(6) an analysis of how the Federal science agencies can work together to advance goals related to broadening the participation of individuals from groups that are underrepresented in science and engineering; and

(7) an analysis of how to promote relationships between institutions of higher education and high schools to enhance the pipeline for high school students to undergraduate STEM opportunities in covered fields and enhance the quality of high school teachers in STEM fields.

(b) REPORT TO CONGRESS.—Not later than 2 years after the date of enactment of this Act, and every 5 years thereafter, the Subcommittee on Federal Coordination in Science, Technology, Engineering, and Mathematics Education of the Committee on Science, Technology, Engineering, and Mathematics Education of the National Science and Technology Council shall report to Congress on the implementation by Federal science agencies of the strategic plan developed under this section.

SEC. ___15. RESEARCH PROGRAM CLEARINGHOUSE AND TECHNICAL ASSISTANCE CENTER.

(a) OPPORTUNITIES CLEARINGHOUSE.—The Subcommittee on Federal Coordination in Science, Technology, Engineering, and Mathematics Education of the Committee on Science, Technology, Engineering, and Mathematics Education of the National Science and Technology Council shall establish and maintain a public clearinghouse (including by maintaining a publicly available website) of all research programs sponsored by Federal science agencies that are available to individuals as undergraduate and graduate students.

(b) BEST PRACTICES CLEARINGHOUSE.—The Director shall work with the Director of the Institute of Education Sciences of the Department of Education to maintain the What Works Clearinghouse to collect, analyze, identify, disseminate, and make publicly available information about best practices for institutions of higher education to strengthen the pipeline of individuals pursuing careers in covered fields (particularly for minority students pursuing those careers), and particularly information to help address gaps identified in the publication entitled ''Minority Serving Institutions: America's Underutilized Resource for Strengthening the STEM Workforce'', published in 2019 by the National Academies of Sciences, Engineering, and Medicine.

(c) TECHNICAL ASSISTANCE.—The Director shall fund the maintenance of existing (as of the date of the funding) technical resource centers to enable the centers to work with institutions of higher education seeking to implement strategies to—

(1) bolster and diversify the student body at the institution that pursue STEM fields;

(2) support students underrepresented in science and engineering who are pursuing research-based STEM studies to help those students continue and complete those studies; or

(3) support other technical assistance activities determined by the Director to be appropriate.

Subtitle B—Increasing Transparency for Graduate Education

SEC. ___21. STRENGTHENING TRANSPARENCY.

(a) ASSESSMENTS.—The Director shall conduct regular assessments of graduate research fellowship programs carried out by the National Science Foundation and make additional information publicly available about those programs, including for each program—

(1) the number of applications received, disaggregated by undergraduate and graduate institution, race, gender, age, and eligibility for a Federal Pell Grant;

(2) the number of applications approved, disaggregated by undergraduate and graduate institution, race, gender, age, and eligibility for a Federal Pell Grant;

(3) the number of students that are awarded grants to develop a diverse STEM workforce, disaggregated by undergraduate population, public or private institution, and (in the case of a minority-serving institution) type of minority-serving institutions;

(4) an analysis of the recipients of scholarships and fellowships awarded by institutions of higher education through the graduate research fellowship programs, disaggregated by race; and

(5) the ratio of the number of individuals who participated in the assessment from the program to the number of students in the program.

(b) VOLUNTARILY PROVIDED DATA.—For purposes of subsection (a), the Director shall base the assessments on, and make information publicly available on, data voluntarily provided by student applicants for the graduate research fellowship program involved.

(c) REPORTS.—The Director shall prepare and submit to Congress, and make publicly available, annual reports that show trends in how research fellowships and scholarships supported by the National Science Foundation are awarded to individuals from underrepresented groups, institutions of higher education, and entities from different geographic areas, in order to better show trends in the participation of underrepresented groups in such research fellowships and scholarships.

Subtitle C—Strengthening the National Security Research Workforce

SEC. ___31. EARLY CAREER FACULTY SUPPORTS.

(a) RISING FACULTY PROFESSIONAL ADVANCEMENT PROGRAM.—

(1) ESTABLISHMENT OF PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, the Director shall select an organization to establish a 5-year pilot mentorship program to be known as ''Rising Faculty Professional Advancement Program'' (referred to in this section as the ''program'') in order to increase the diversity of faculty in STEM fields.

(2) PURPOSE.—The purpose of the Rising Faculty Professional Advancement Program shall be—

(A) to increase the number of doctoral-level professionals from underrepresented groups in STEM fields who transition into faculty positions at institutions of higher education; and

(B) to improve mentorship and training for researchers who are navigating the transition in the research pipeline to becoming faculty, which is a time when a significant decrease in diversity often occurs.

(b) PROGRAM PARTICIPANTS.—

(1) ELIGIBILITY.—An individual shall be eligible to participate in the program if the individual is a doctoral degree holding researcher in a post-doctoral research position or early-career faculty (defined as a faculty researcher with a title of assistant professor or other non-tenured equivalent).

(2) OUTREACH.—The organization shall conduct outreach to encourage participation in the program by individuals described in paragraph (1) who are from groups underrepresented in STEM fields, including—

(A) individuals from groups who are underrepresented in science and engineering;

(B) individuals holding doctoral degrees in covered fields from or faculty positions at minority-serving institutions;

(C) individuals holding doctoral degrees in covered fields from institutions of higher education in the bottom 90 percent of research and development expenditures, as ranked by the National Center for Science and Engineering Statistics; and

(D) individuals who are women and who hold positions from underrepresented fields.

(c) ACTIVITIES.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the organization shall establish program activities including—

(A) training for Rising Faculty and mentors;

(B) a program curriculum; and

(C) support for existing (as of the date of provision of the support) mentoring programs for mentor engagement.

(2) COLLABORATIVE RESEARCH.—The organization shall encourage program mentors to network and enter into collaboration on research projects with Rising Faculty and other mentors within the program.

(3) SURVEY.—Following the first year of program enrollment, and on an annual basis during the program, the organization shall—

(A) conduct a survey of Rising Faculty and mentors to determine best practices and outcomes achieved;

(B) conduct a survey to collect information about the demographics of the Rising Faculty and mentors; and

(C) conduct additional surveys or other analyses of Rising Faculty who completed the program to assess career progression for not more than 5 years following the completion of the program by Rising Faculty.

(d) ASSESSMENT OF THE PILOT PROGRAM AND RECOMMENDATIONS.—Not later than 180 days after the conclusion of the pilot program, the Director shall provide a report to the appropriate committees of Congress with respect to the pilot program, which shall include—

(1) a description and evaluation of the status and effectiveness of the program, including a summary of survey data collected;

(2) an assessment of the success and utility of the pilot program in meeting the purposes of this section;

(3) a summary and analysis of the types and frequency of activities and policies developed and carried out under the pilot program; and

(4) a recommendation about continuing the program on a pilot or permanent basis.

SA 4718. 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, insert the following:

SEC. _____. MINORITY INSTITUTE FOR DEFENSE RESEARCH.

(a) PLAN TO ESTABLISH MINORITY INSTITUTE FOR DEFENSE RESEARCH.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this section, the Secretary shall submit to the congressional defense committees a plan (in this section referred to as the ''Plan'') 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) Information relating to the projected needs of the Department for the next twenty years with respect to essential engineering, research, or development capability.

(B) An assessment relating to the engineering, research, and development capability of each minority institution to identify each leading minority institution.

(C) Information relating to the advancements and investments necessary to elevate a minority institution or a consortium of minority institutions to the research capacity of a University Affiliated Research Center.

(D) Recommendations relating to actions that may be taken by the Department, Congress, and minority institutions to establish the Consortium within 10 years.

(3) PUBLICLY AVAILABLE.—The Plan shall be posted on a publicly available website of the Department.

(b) NAMING OF THE CONSORTIUM.—With respect to the naming of the Consortium, the Secretary shall—

(1) establish a process to solicit and review proposals of names from—

(A) minority institutions;

(B) nonprofit institutions that advocate on behalf of minority institutions; and

(C) members of the public;

(2) develop a list of all names received pursuant to paragraph (1);

(3) provide opportunity for public comment on the names included on such list; and

(4) choose a name from such list to name the Consortium.

(c) GRANT PROGRAM FOR LEADING MINORITY INSTITUTIONS.—

(1) IN GENERAL.—The Secretary may establish a program to award grants, on a competitive basis, to leading minority institutions for the purposes described in paragraph (2).

(2) PURPOSES.—The purposes described in this paragraph are the following:

(A) Establishing a legal entity for the purpose of entering into research contracts or agreements with the Federal Government or the Consortium.

(B) Developing the capability to bid on Federal Government or Consortium contracts.

(C) Requesting technical assistance from the Federal Government or a private entity with respect to contracting with the Federal Government or the Consortium.

(D) Recruiting and retaining research faculty.

(E) Advancing research capabilities relating to the national security of the United States.

(F) Any other matter determined appropriate by the Secretary.

(3) APPLICATION.—To be eligible to receive a grant under this section, a leading minority institution shall submit to the Secretary an application therefor in such form, and containing such information, as the Secretary may require.

(4) PREFERENCE.—In awarding grants pursuant to paragraph (1), the Secretary shall give preference to a leading minority institution with a R1 or R2 status on the Carnegie Classification of Institutions of Higher Education.

(d) DEFINITIONS.—In this section:

(1) The term ''Department'' means the Department of Defense.

(2) The term ''leading minority institution'' means a minority institution identified (pursuant to the assessment required under subsection (a)(2)(B)) as being in the top 20 percent of all such institutions with respect to providing essential engineering, research, or development capability.

(3) 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).

(4) 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) any institution of higher education at which not less than 50 percent of the total student enrollment consists of students from ethnic groups that are underrepresented in the fields of science and engineering.

(5) The term ''Secretary'' means the Secretary of Defense.

(6) The term ''University Affiliated Research Center'' means a research organization within an institution of higher education 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 title 10, United States Code.

SEC. _____. SUBCONTRACT REQUIREMENTS FOR MINORITY INSTITUTIONS.

(a) IN GENERAL.—Section 2304 of title 10, United States Code, is amended by adding at the end the following new subsection:

''(m)(1) The head of an agency shall require that a contract awarded to an educational institution pursuant to subsection (c)(3)(B) includes a requirement to subcontract with one or more minority institutions for a total amount of not less than 5 percent of the amount awarded in the contract.

''(2) For the purposes of this subsection, a minority institution means—

''(A) a part B institution (as that term is defined in section 322(2) of the Higher Education Act of 1965 (20 U.S.C. 1061(2))); or

''(B) any other institution of higher education (as that term is defined in section 101 of such Act (20 U.S.C. 1001)) at which not less than 50 percent of the total student enrollment consists of students from ethnic groups that are underrepresented in the fields of science and engineering.''.

(b) EFFECTIVE DATE.—The amendments made by subsection (a) shall—

(1) take effect on October 1, 2026; and

(2) apply with respect to funds that are awarded by the Department of Defense on or after such date.

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 $30,000,000, 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 $15,000,000, with the amount of the increase to be available for Advanced Research High speed flight experiment testing (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 $45,000,000, 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) DEFINITION OF MINORITY INSTITUTION.—In this section, 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) any institution of higher education at which not less than 50 percent of the total

student enrollment consists of students from ethnic groups that are underrepresented in the fields of science and engineering.

SA 4719. Mr. BROWN (for himself and Mr. CASEY) 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. _____. PROTECTIONS FOR OBLIGORS AND COSIGNERS IN CASE OF DEATH OR TOTAL AND PERMANENT DISABILITY.

(a) IN GENERAL.—Section 140(g) of the Truth in Lending Act (15 U.S.C. 1650(g)) is amended—

(1) in paragraph (2)—

(A) in the heading, by striking ''IN CASE OF DEATH OF BORROWER''; an

(B) by striking ''death'' each place the term appears and inserting ''death or total and permanent disability'';

(2) by adding at the end the following:

''(3) DISCHARGE IN CASE OF DEATH OR TOTAL AND PERMANENT DISABILITY OF BORROWER.—The holder of a private education loan shall, when notified of the death or total and permanent disability of a student obligor, discharge the liability of the student obligor on the loan and may not, after such notification—

''(A) attempt to collect on the outstanding liability of the student obligor; and

''(B) in the case of total and permanent disability, monitor the disability status of the student obligor at any point after the date of discharge.

''(4) PRIVATE DISCHARGE IN CASES OF CERTAIN DISCHARGE FOR DEATH OR DISABILITY.—The holder of a private education loan shall, when notified of the discharge of liability of a student obligor on a loan described under section 108(f)(5)(A) of the Internal Revenue Code of 1986, discharge any liability of the student obligor (and any cosigner) on any private education loan which the private education loan holder holds and may not, after such notification—

''(A) attempt to collect on the outstanding liability of the student obligor; and

''(B) in the case of total and permanent disability, monitor the disability status of the student obligor at any point after the date of discharge.

''(5) DEFINITION.—In this subsection, the term 'total and permanent disability' has the meaning given the term 'totally and permanently disabled' in section 685.102(b) of title 34, Code of Federal Regulations.''.

(b) RULEMAKING.—The Director of the Bureau of Consumer Financial Protection may promulgate regulations to implement the amendments made by subsection (a) as the Director determines appropriate.

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

SA 4720. Mr. ROUNDS (for Mr. INHOFE) submitted an amendment intended to be proposed to amendment SA 4431 submitted by Mr. INHOFE and intended to be proposed to the amendment SA 3867 proposed by Mr. REED 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 lieu of the matter proposed to be inserted, insert the following:

SEC. 1516. MODIFICATION TO ESTIMATE OF DAMAGES FROM FEDERAL COMMUNICATIONS COMMISSION ORDER 20–48.

Section 1664 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283) is amended—

(1) in subsection (a), in the matter preceding paragraph (1), by inserting ''or any subsequent fiscal year'' after ''fiscal year 2021''; and

(2) by adding at the end the following new subsections:

''(d) DISTRIBUTION OF ESTIMATE.—As soon as practicable after submitting an estimate as described in paragraph (1) of subsection (a) and making the certification described in paragraph (2) of such subsection, the Secretary shall make such estimate available to any licensee operating under the Order and Authorization described in such subsection.

''(e) AUTHORITY OF SECRETARY OF DEFENSE TO SEEK RECOVERY OF COSTS.—The Secretary may work directly with any licensee (or any future assignee, successor, or purchaser) affected by the Order and Authorization described in subsection (a) to seek recovery of costs incurred by the Department as a result of the effect of such order and authorization.

''(f) REIMBURSEMENT.—

''(1) IN GENERAL.—The Secretary shall establish and facilitate a process for any licensee (or any future assignee, successor, or purchaser) subject to the Order and Authorization described in subsection (a) to provide reimbursement to the Department, only to the extent provided in appropriation Acts, for the covered costs and eligible reimbursable costs submitted and certified to the congressional defense committees under such subsection.

''(2) USE OF FUNDS.—The Secretary shall use any funds received under this subsection, to the extent and in such amounts as are provided in advance in appropriation Acts, for covered costs described in subsection (b) and the range of eligible reimbursable costs identified under subsection (a)(1).

''(3) REPORT.—Not later than 90 days after the date on which the Secretary establishes the process required by paragraph (1), the Secretary shall submit to the congressional defense committees a report on such process.''.

SA 4721. Mr. WARNOCK 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 X, add the following:

Subtitle H—Maternal Health

SEC. 1071. INNOVATION FOR MATERNAL HEALTH.

Title III of the Public Health Service Act (42 U.S.C. 241 et seq.) is amended by inserting after section 330N of such Act, the following:

''SEC. 330O. INNOVATION FOR MATERNAL HEALTH.

''(a) IN GENERAL.—The Secretary, in consultation with experts representing a variety of clinical specialties, State, Tribal, or local public health officials, researchers, epidemiologists, statisticians, and community organizations, shall establish or continue a program to award competitive grants to eligible entities for the purpose of—

''(1) identifying, developing, or disseminating best practices to improve maternal health care quality and outcomes, improve maternal and infant health, and eliminate preventable maternal mortality and severe maternal morbidity, which may include—

''(A) information on evidence-based practices to improve the quality and safety of maternal health care in hospitals and other health care settings of a State or health care system by addressing topics commonly associated with health complications or risks related to prenatal care, labor care, birthing, and postpartum care;

''(B) best practices for improving maternal health care based on data findings and reviews conducted by a State maternal mortality review committee that address topics of relevance to common complications or health risks related to prenatal care, labor care, birthing, and postpartum care; and

''(C) information on addressing determinants of health that impact maternal health outcomes for women before, during, and after pregnancy;

''(2) collaborating with State maternal mortality review committees to identify issues for the development and implementation of evidence-based practices to improve maternal health outcomes and reduce preventable maternal mortality and severe maternal morbidity, consistent with section 317K;

''(3) providing technical assistance and supporting the implementation of best practices identified in paragraph (1) to entities providing health care services to pregnant and postpartum women; and

''(4) identifying, developing, and evaluating new models of care that improve maternal and infant health outcomes, which may include the integration of community-based services and clinical care.

''(b) ELIGIBLE ENTITIES.—To be eligible for a grant under subsection (a), an entity shall—

''(1) submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require; and

''(2) demonstrate in such application that the entity is capable of carrying out data-driven maternal safety and quality improvement initiatives in the areas of obstetrics and gynecology or maternal health.

''(c) REPORT.—Not later than September 30, 2024, and every 2 years thereafter, the Secretary shall submit a report to Congress on the practices described in paragraphs (1) and (2) of subsection (a). Such report shall include a description of the extent to which such practices reduced preventable maternal mortality and severe maternal morbidity, and whether such practices improved maternal and infant health. The Secretary shall disseminate information on such practices, as appropriate.

''(d) AUTHORIZATION OF APPROPRIATIONS.—To carry out this section, there are authorized to be appropriated $9,000,000 for each of fiscal years 2022 through 2026.''.

SEC. 1072. TRAINING FOR HEALTH CARE PROVIDERS.

Title VII of the Public Health Service Act is amended by striking section 763 (42 U.S.C. 294p) and inserting the following:

"SEC. 763. TRAINING FOR HEALTH CARE PROVIDERS.

''(a) GRANT PROGRAM.—The Secretary shall establish a program to award grants to accredited schools of allopathic medicine, osteopathic medicine, and nursing, and other health professional training programs for the training of health care professionals to improve the provision of prenatal care, labor care, birthing, and postpartum care for racial and ethnic minority populations, including with respect to perceptions and biases that may affect the approach to, and provision of, care.

''(b) ELIGIBILITY.—To be eligible for a grant under subsection (a), an entity described in such subsection shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

''(c) REPORTING REQUIREMENTS.—

''(1) PERIODIC GRANTEE REPORTS.—Each entity awarded a grant under this section shall periodically submit to the Secretary a report on the status of activities conducted using the grant, including a description of the impact of such training on patient outcomes, as applicable.

''(2) REPORT TO CONGRESS.—Not later than September 30, 2025, the Secretary shall submit a report to Congress on the activities conducted using grants under subsection (a) and any best practices identified and disseminated under subsection (d).

''(d) BEST PRACTICES.—The Secretary may identify and disseminate best practices for the training described in subsection (a).

''(e) AUTHORIZATION OF APPROPRIATIONS.—To carry out this section, there are authorized to be appropriated $5,000,000 for each of fiscal years 2022 through 2026.''.

SEC. 1073. STUDY ON IMPROVING TRAINING FOR HEALTH CARE PROVIDERS.

Not later than 2 years after date of enactment of this Act, the Secretary of Health and Human Services shall, through a contract with an independent research organization, conduct a study and make recommendations for accredited schools of allopathic medicine, osteopathic medicine, and nursing, and other health professional training programs on best practices related to training to improve the provision of prenatal care, labor care, birthing, and postpartum care for racial and ethnic minority populations, including with respect to perceptions and biases that may affect the approach to, and provision of, care.

SEC. 1074. PERINATAL QUALITY COLLABORATIVES.

(a) IN GENERAL.—Section 317K(a)(2) of the Public Health Service Act (42 U.S.C. 247b–12(a)(2)) is amended by adding at the end the following:

''(E)(i) The Secretary, acting through the Director of the Centers for Disease Control and Prevention and in coordination with other offices and agencies, as appropriate, shall establish or continue a competitive grant program for the establishment or support of perinatal quality collaboratives to improve perinatal care and perinatal health outcomes for pregnant and postpartum women and their infants. A State, Indian Tribe, or Tribal organization may use funds received through such grant to—

''(I) support the use of evidence-based or evidence-informed practices to improve outcomes for maternal and infant health;

''(II) work with clinical teams; experts; State, local, and, as appropriate, Tribal public health officials; and stakeholders, including patients and families, to identify, develop, or disseminate best practices to improve perinatal care and outcomes; and

''(III) employ strategies that provide opportunities for health care professionals and clinical teams to collaborate across health care settings and disciplines, including primary care and mental health, as appropriate, to improve maternal and infant health outcomes, which may include the use of data to provide timely feedback across hospital and clinical teams to inform responses, and to provide support and training to hospital and clinical teams for quality improvement, as appropriate.

''(ii) To be eligible for a grant under clause (i), an entity shall submit to the Secretary an application in such form and manner and containing such information as the Secretary may require.''.

(b) REPORT TO CONGRESS.—Not later than September 30, 2025, the Secretary of Health and Human Services shall submit to Congress a report regarding the activities conducted by recipients of grants under subsection (a)(2)(E) of section 317K of the Public Health Service Act (42 U.S.C. 247b–12).

SEC. 1075. INTEGRATED SERVICES FOR PREGNANT AND POSTPARTUM WOMEN.

(a) GRANTS.—Title III of the Public Health Service Act (42 U.S.C. 241 et seq.) is amended by inserting after section 330O of such Act, as added by section 1071, the following:

"SEC. 330P. INTEGRATED SERVICES FOR PREGNANT AND POSTPARTUM WOMEN.

''(a) IN GENERAL.—The Secretary may award grants for the purpose of establishing or operating evidence-based or innovative, evidence-informed programs to deliver integrated health care services to pregnant and postpartum women to optimize the health of women and their infants, including to reduce adverse maternal health outcomes, pregnancy-related deaths, and related health disparities (including such disparities associated with racial and ethnic minority populations), and, as appropriate, by addressing issues researched under subsection (b)(2) of section 317K.

''(b) INTEGRATED SERVICES FOR PREGNANT AND POSTPARTUM WOMEN.—

''(1) ELIGIBILITY.—To be eligible to receive a grant under subsection (a), a State, Indian Tribe, or Tribal organization (as such terms are defined in section 4 of the Indian Self-Determination and Education Assistance Act) shall work with relevant stakeholders that coordinate care to develop and carry out the program, including—

''(A) State, Tribal, and local agencies responsible for Medicaid, public health, social services, mental health, and substance use disorder treatment and services;

''(B) health care providers who serve pregnant and postpartum women; and

''(C) community-based health organizations and health workers, including providers of home visiting services and individuals representing communities with disproportionately high rates of maternal mortality and severe maternal morbidity, and including those representing racial and ethnic minority populations.

''(2) TERMS.—

''(A) PERIOD.—A grant awarded under subsection (a) shall be made for a period of 5 years. Any supplemental award made to a grantee under subsection (a) may be made for a period of less than 5 years.

''(B) PRIORITIES.—In awarding grants under subsection (a), the Secretary shall—

''(i) give priority to States, Indian Tribes, and Tribal organizations that have the highest rates of maternal mortality and severe maternal morbidity relative to other such States, Indian Tribes, or Tribal organizations, respectively; and

''(ii) shall consider health disparities related to maternal mortality and severe maternal morbidity, including such disparities associated with racial and ethnic minority populations.

''(C) EVALUATION.—The Secretary shall require grantees to evaluate the outcomes of the programs supported under the grant.

''(c) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $10,000,000 for each of fiscal years 2022 through 2026.''.

(b) REPORT ON GRANT OUTCOMES AND DISSEMINATION OF BEST PRACTICES.—

(1) REPORT.—Not later than February 1, 2026, the Secretary of Health and Human Services shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report that describes—

(A) the outcomes of the activities supported by the grants awarded under the amendments made by this section on maternal and child health;

(B) best practices and models of care used by recipients of grants under such amendments; and

(C) obstacles identified by recipients of grants under such amendments, and strategies used by such recipients to deliver care, improve maternal and child health, and reduce health disparities.

(2) DISSEMINATION OF BEST PRACTICES.—Not later than August 1, 2026, the Secretary of Health and Human Services shall disseminate information on best practices and models of care used by recipients of grants under the amendments made by this section (including best practices and models of care relating to the reduction of health disparities, including such disparities associated with racial and ethnic minority populations, in rates of maternal mortality and severe maternal morbidity) to relevant stakeholders, which may include health providers, medical schools, nursing schools, relevant State, Tribal, and local agencies, and the general public.

SEC. 1076. MATERNAL VACCINATION AWARENESS.

In carrying out the public awareness initiative related to vaccinations pursuant to section 313 of the Public Health Service Act (42 U.S.C. 245), the Secretary of Health and Human Services shall take into consideration the importance of increasing awareness and knowledge of the safety and effectiveness of vaccines to prevent disease in pregnant and postpartum women and in infants and the need to improve vaccination rates in communities and populations with low rates of vaccination.

SA 4722. 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 appropriate place, insert the following:

SEC. _____. IMPROVEMENTS TO CHIPS.

Section 9902 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (15 U.S.C. 4652) is amended—

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

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

''(c) CONDITIONS OF RECEIPT.—

''(1) REQUIRED AGREEMENT.—A covered entity to which the Secretary awards Federal financial assistance under this section shall enter into an agreement that specifies that, during the 5-year period immediately following the award of the Federal financial assistance—

''(A) the covered entity will not—

''(i) repurchase an equity security that is listed on a national securities exchange of the covered entity or any parent company of the covered entity, except to the extent required under a contractual obligation that is in effect as of the date of enactment of this subsection;

''(ii) outsource or offshore jobs to a location outside of the United States; or

''(iii) abrogate existing collective bargaining agreements; and

''(B) the covered entity will remain neutral in any union organizing effort.

''(2) FINANCIAL PROTECTION OF GOVERNMENT.—

''(A) IN GENERAL.—The Secretary may not award Federal financial assistance to a covered entity under this section, unless—

''(i)(I) the covered entity has issued securities that are traded on a national securities exchange; and

''(II) the Secretary of the Treasury receives a warrant or equity interest in the covered entity; or

''(ii) in the case of any covered entity other than a covered entity described in clause (i), the Secretary of the Treasury receives, in the discretion of the Secretary of the Treasury—

''(I) a warrant or equity interest in the covered entity; or

''(II) a senior debt instrument issued by the covered entity.

''(B) TERMS AND CONDITIONS.—The terms and conditions of any warrant, equity interest, or senior debt instrument received under subparagraph (A) shall be set by the Secretary and shall meet the following requirements:

''(i) PURPOSES.—Such terms and conditions shall be designed to provide for a reasonable participation by the Secretary of Commerce, for the benefit of taxpayers, in equity appreciation in the case of a warrant or other equity interest, or a reasonable interest rate premium, in the case of a debt instrument.

''(ii) AUTHORITY TO SELL, EXERCISE, OR SURRENDER.—For the primary benefit of taxpayers, the Secretary may sell, exercise, or surrender a warrant or any senior debt instrument received under this subparagraph. The Secretary shall not exercise voting power with respect to any shares of common stock acquired under this subparagraph.

''(iii) SUFFICIENCY.—If the Secretary determines that a covered entity cannot feasibly issue warrants or other equity interests as required by this subparagraph, the Secretary may accept a senior debt instrument in an amount and on such terms as the Secretary determines appropriate.''.

SA 4723. Mr. DAINES (for himself 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 appropriate place, insert the following:

SEC. _____. CONGRESSIONAL GOLD MEDAL.

(a) FINDINGS.—Congress finds the following:

(1) At 9:44 a.m., on August 26, 2021, the Pentagon confirmed that one explosion occurred at the Hamid Karzai International Airport.

(2) The explosion was confirmed to be a suicide bombing by ISIS–K terrorist group.

(3) Estimates as high as 200 deaths were reported, including 13 service members of the United States, as well as hundreds more wounded.

(4) The attack on Thursday, August 26, 2021 at the Hamid Karzai International Airport in Kabul, Afghanistan, killed 13 United States service members, making it the deadliest single day of the war for the United States in more than a decade.

(5) The American service members went above and beyond the call of duty to protect citizens of the United States and our allies to ensure they are brought to safety in an extremely dangerous situation as the Taliban regained control over Afghanistan.

(6) The American service members exemplified extreme bravery and valor against armed enemy combatants.

(7) The American service members dedicated their lives and their heroism deserves great honor.

(8) Maxton Soviak, Kareem Nikoui, David Espinoza, Rylee McCollum, Jared Schmitz, Hunter Lopez, Taylor Hoover, Daegan William-Tyeler Page, Nicole Gee, Humberto Sanchez, Dylan Merola, Johanny Rosario Pichardo, and Ryan Knauss have been identified as the 13 service members who died from the blast while stationed at Hamid Karzai International Airport.

(b) CONGRESSIONAL GOLD MEDAL.—

(1) PRESENTATIONS AUTHORIZED.—The Speaker of the House of Representatives and the President pro tempore of the Senate shall make appropriate arrangements for the posthumous presentation, on behalf of Congress, of a single gold medal of appropriate design in commemoration of the 13 service members who perished as a result of the attack in Afghanistan, on August 26, 2021.

(2) DESIGN AND STRIKING.—For purposes of the presentation referred to in paragraph (1), the Secretary of the Treasury (referred to in this section as the ''Secretary'') shall strike a gold medal with suitable emblems, devices, and inscriptions, to be determined by the Secretary.

(3) SMITHSONIAN INSTITUTION.—

(A) IN GENERAL.—Following the award of the gold medal under paragraph (1), the gold medal shall be given to the Smithsonian Institution, where it shall be available for display as appropriate and made available for research.

(B) SENSE OF CONGRESS.—It is the sense of Congress that the Smithsonian Institution shall make the gold medal received under paragraph (1) available for display outside of the District of Columbia at times, particularly at other locations associated with the 13 service members who perished in Afghanistan on August 26, 2021.

(c) DUPLICATE MEDALS.—The Secretary may strike and sell duplicates in bronze of the gold medal struck pursuant to subsection (b) at a price sufficient to cover the cost thereof, including labor, materials, dies, use of machinery, and overhead expenses.

(d) STATUS OF MEDALS.—

(1) NATIONAL MEDALS.—The medal struck pursuant to this section is a national medal for purposes of chapter 51 of title 31, United States Code.

(2) NUMISMATIC ITEMS.—For purposes of section 5134 of title 31, United States Code, all medals struck under this section shall be considered to be numismatic items.

(e) AUTHORITY TO USE FUND AMOUNTS; PROCEEDS OF SALE.—

(1) AUTHORITY TO USE FUND AMOUNTS.—There is authorized to be charged against the United States Mint Public Enterprise Fund such amounts as may be necessary to pay for the costs of the medals struck pursuant to this section.

(2) PROCEEDS OF SALE.—The amounts received from the sale of duplicate bronze medals authorized under subsection (c) shall be deposited into the United States Mint Public Enterprise Fund.

SA 4724. 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 of subtitle G of title X, add the following:

SEC. 1064. REPORT ON CYBERSECURITY CERTIFICATIONS AND LABELING.

Not later than October 1, 2022, the National Cyber Director, in consultation with the Director of the National Institute of Standards and Technology, the Chairman of the Federal Trade Commission, and the Director of the Cybersecurity and Infrastructure Security Agency, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives a report that—

(1) identifies and assesses existing efforts by the Federal Government to create, administer, or otherwise support the use of certifications or labels to communicate the security or security characteristics of information technology or operational technology products and services; and

(2) assesses the viability of and need for a new program at the Department of Homeland Security, or at other Federal agencies as appropriate, to better address information technology and operational technology product and service security certification and labeling efforts across the Federal Government and between the Federal Government and the private sector.

SA 4725. Ms. CORTEZ MASTO (for herself and Mr. KAINE) 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. _____. IMPROVING IRAQ & AFGHANISTAN SERVICE GRANT AND CHILDREN OF FALLEN HEROES GRANT.

(a) TECHNICAL AMENDMENT RELATING TO IRAQ AND AFGHANISTAN SERVICE GRANT AND

CHILDREN OF FALLEN HEROES GRANT.—Part A of title IV of the Higher Education Act of 1965 (20 U.S.C. 1070 et seq.), as amended by section 703 of the FAFSA Simplification Act (title VII of division FF of Public Law 116–260), is amended—

(1) in section 401—

(A) in subsection (c)—

(i) in paragraph (2)—

(I) by striking subparagraph (A); and

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

(ii) in paragraph (3)(A), by striking ''(2)(B)(i)'' and inserting ''(2)(A)(i)'';

(iii) by redesignating paragraph (5) as paragraph (7); and

(iv) by inserting after paragraph (4) the following:

''(5) PREVENTION OF DOUBLE BENEFITS.—No eligible student described in paragraph (2) may concurrently receive a grant under both this subsection and subsection (b).

''(6) TERMS AND CONDITIONS.—The Secretary shall award grants under this subsection in the same manner and with the same terms and conditions, including the length of the period of eligibility, as the Secretary awards Federal Pell Grants under subsection (b), except that—

''(A) the award rules and determination of need applicable to the calculation of Federal Pell Grants under subsection (b)(1) shall not apply to grants made under this subsection; and

''(B) the maximum period determined under subsection (d)(5) shall be determined by including all grants made under this section received by the eligible student and all grants so received under subpart 10 before the effective date of this subsection.''; and

(2) by striking section 420R (20 U.S.C. 1070h).

(b) EFFECTIVE DATE.—The amendments made by subsection (a) shall take effect as if included in section 703 of the FAFSA Simplification Act (title VII of division FF of Public Law 116–260) and subject to the effective date of section 701(b) of such Act.

(c) TRANSITION.—The Secretary shall take such steps as are necessary to transition from the Iraq and Afghanistan Service Grant program under subpart 10 of part A of title IV of the Higher Education Act of 1965 (20 U.S.C. 1070h), as in effect on the day before the effective date of this section, and the provision of Federal Pell Grants under section 401(c) of the Higher Education Act of 1965 (20 U.S.C. 1070a(c)), as amended by the FAFSA Simplification Act and this Act.

SA 4726. 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, 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 4727. Mr. SULLIVAN 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. DISCLOSURES REQUIRED BY UNITED STATES FINANCIAL INSTITUTIONS INVESTING IN PEOPLE'S REPUBLIC OF CHINA.

(a) IN GENERAL.—The Secretary of Defense shall—

(1) require any United States financial institution that makes an investment described subsection (b) to disclose the amount and purpose, and potential impacts on the national defense, of such investments to the Secretary on an annual basis; and

(2) make such disclosures available to the public.

(b) INVESTMENTS DESCRIBED.—An investment described in this subsection is a monetary investment, in an amount that exceeds a threshold to be determined by the Secretary, directly or indirectly—

(1) to—

(A) the People's Republic of China;

(B) an entity owned or controlled by the Chinese Communist Party; or

(C) the People's Liberation Army; or

(2) for the benefit of any key industrial sector sponsored by the Chinese Communist Party.

(c) CONSOLIDATED REPORT.—Not less frequently than annually, the Secretary shall compile the disclosures submitted under subsection (a) and submit that compilation and a summary of those disclosures to the congressional defense committees.

(d) REGULATIONS.—The Secretary shall prescribe such regulations as are necessary to carry out this section, which may include—

(1) requirements for documents and information to be submitted with disclosures required under subsection (a); and

(2) procedures for the determining the amount under subsection (b).

(e) DEFINITIONS.—In this section:

(1) FINANCIAL INSTITUTION.—The term ''financial institution''—

(A) has the meaning given that term in section 5312 of title 31, United States Code; and

(B) includes a private equity company, venture capital company, or hedge fund.

(2) UNITED STATES FINANCIAL INSTITUTION.—The term ''United States financial institution'' means a financial institution organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such an institution.

SA 4728. 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) COUNTERING EXTREMISM.—

(1) IN GENERAL.—Title 10, United States Code, is amended—

(A) in Part II of subtitle A, by adding at the end the following new chapter:

''CHAPTER 89—COUNTERING EXTREMISM

''1801. Senior Official for Countering Extremism.
''1802. Training and education.
''1803. Data collection and analysis.
''1804. Reporting requirements.
''1805. Definitions.

''§ 1801. Senior Official for Countering Extremism

''(a) DESIGNATION.—The Secretary of Defense shall designate an Under Secretary of Defense as the Senior Official for Countering Extremism.

''(b) DUTIES.—The Senior Official shall—

''(1) coordinate and facilitate programs, resources, and activities within the Department of Defense to counter extremist activities, to include screening of publicly available information and Insider Threat Programs;

''(2) coordinate with Federal, State, and local enforcement organizations to counter extremism within the Department of Defense;

''(3) coordinate with the Secretary of Veterans Affairs on addressing and preventing extremist activities following an individual's separation from the armed forces;

''(4) engage and interact with, and solicit recommendations from, outside experts on extremist activities; and

''(5) perform any additional duties prescribed by the Secretary of Defense, in consultation with the Secretary of Homeland Security.

''§ 1802. Training and education

''(a) 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.

''(b) CONTENT.—The training and education described in subsection (a) 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.

''(c) REQUIREMENTS.—The Secretary of Defense, in consultation with the Secretary of Homeland Security, shall provide the training and education described in subsection (a)—

''(1) to a member of the armed forces, civilian employee of the Department of Defense, cadet at a military service academy, or an individual in a pre-commissioning program no less than once a year;

''(2) 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 this title;

''(3) to a member of the armed forces performing recruitment activities within the 30 days prior to commencing such activities; and

''(4) additionally as determined by the Secretary of Defense.

''§ 1803. Data collection and analysis

''(a) IN GENERAL.—The Senior Official for Countering Extremism shall establish and maintain a database on extremist activities in the Department of Defense.

''(b) CONTENT.—The database established under subsection (a) shall—

''(1) include records on each allegation, investigation, disciplinary action, and separation related to extremist activities within the Department of Defense;

''(2) include, as appropriate, information related to extremist activities in the armed forces provided by or generated from information from a Federal law enforcement agency; and

''(3) any other requirements prescribed by the Secretary of Defense, in consultation with the Secretary of Homeland Security.

''§ 1804. Reporting requirements

''(a) ANNUAL REPORT.—Not later than December 1 of each year, the Senior Official for Countering Extremism shall submit to Congress a report on the prevalence of extremist activities within the Department of Defense.

''(b) ELEMENTS.—The report required by subsection (a) shall include each of the following elements:

''(1) The number of extremist activity allegations, investigations, disciplinary actions, and separations disaggregated data by the armed force, race, gender, ethnicity, grade, and rank of the principal.

''(2) An analysis and assessment of trends in the incidence and disposition of extremist activities during the year covered by the report.

''(3) Any other matters as determined by the Senior Official for Countering Extremism.

''(c) PUBLICATION.—The Secretary of Defense shall—

''(1) publish on an appropriate publicly available website of the Department of Defense the reports required by subsection (a); and

''(2) ensure that any data included with each such report is made available in a machine-readable format that is downloadable, searchable, and sortable.

''§ 1805. Definitions

''The following definitions apply in this chapter:

''(1) The term 'extremist activities' shall—

''(A) have the meaning prescribed by the Secretary of Defense; and

''(B) include membership in an extremist organization.

''(2) The term 'extremist insider threat' means a member of the armed forces or civilian employee of the Department of Defense with access to government information, systems, or facilities, who—

''(A) can use such access to do harm to the security of the United States; and

''(B) engages in extremist activities.

''(3) The term 'extremist organization' shall have the meaning prescribed by the Secretary of Defense.

''(4) The term 'principal' means a member of the armed forces or civilian employee of the Department of Defense who engages in an extremist activity, or aids, abets, counsels, commands, or procures its commission.''; and

(B) in chapter 39, by inserting after section 985 the following new section:

''§ 986. Prohibition on extremist activities

''(a) PROHIBITION.—An individual who engages in extremist activities may not serve as a member of the armed forces.

''(b) REGULATIONS.—The Secretary of Defense shall prescribe regulations regarding the separation of a member of the armed forces who engages in extremist activities.

''(c) DISSEMINATION OF EXTREMIST CONTENT.—The Secretary of Defense may use extremist content knowingly shared, disseminated, or otherwise made available online (including on social media platforms and accounts) by an individual who serves in an armed force as cause for involuntary separation of such individual from an armed force.

''(d) DEFINITIONS.—In this section:

''(1) The term 'extremist activities' has the meaning given such term in section 1805 of this title.

''(2) The term 'extremist content' means content that expresses support for extremist activities (as that term is defined in section 1805 of this title).''.

(2) CLERICAL AMENDMENTS.—

(A) PART II OF SUBTITLE A.—The table of chapters for part II of subtitle A of title 10, United States Code, is amended by inserting after the item relating to chapter 88 the following new item:

''CHAPTER 89—COUNTERING EXTREMISM''.

(B) CHAPTER 39.—The table of sections at the beginning of chapter 39 is amended by inserting after the item relating to section 985 the following new item:

''986. Prohibition on extremist activities.''.

(b) COORDINATION OF EFFORTS WITH INSPECTOR GENERAL.—Section 554(a)(3) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283) is amended by adding at the end the following new subparagraph:

''(E) The Senior Official for Countering Extremism.''.

(c) REGULATIONS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall prescribe regulations under chapter 89 of title 10, United States Code (including definitions under section 1805 of such title), as added by subsection (a).

(d) EFFECTIVE DATE.—The amendments made by this section shall take effect on the day that the Secretary of Defense prescribes regulations under subsection (c).

(e) PROGRESS REPORT.—Not later than 240 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 chapter 89 of title 10, United States Code, as added by subsection (a)(1)(A), and the implementation of section 986 of such title, as added by subsection (a)(1)(B).

SA 4729. 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 XII, add the following:

SEC. 1253. ELIGIBILITY FOR FOREIGN MILITARY SALES AND EXPORT STATUS UNDER ARMS EXPORT CONTROL ACT.

The Arms Export Control Act (22 U.S.C. 2751 et seq.) is amended—

(1) in sections 3(d)(2)(B), 3(d)(3)(A)(i), 3(d)(5), 21(e)(2)(A), 36(b)(1), 36(b)(2), 36(b)(6), 36(c)(2)(A), 36(c)(5), 36(d)(2)(A), 62(c)(1), and 63(a)(2), by inserting ''India,'' before ''or New Zealand'' each place it appears;

(2) in section 3(b)(2), by inserting ''the Government of India,'' before ''or the Government of New Zealand''; and

(3) in sections 21(h)(1)(A) and 21(h)(2), by inserting ''India,'' before ''or Israel'' each place it appears.

SA 4730. Mr. MENENDEZ (for himself and Mr. RISCH) 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—DEPARTMENT OF STATE AUTHORIZATION ACT OF 2021

SEC. 5001. SHORT TITLE.

This division may be cited as the ''Department of State Authorization Act of 2021''.

SEC. 5002. DEFINITIONS.

In this division:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term '' 'appropriate congressional committees' '' means the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(2) DEPARTMENT.—If not otherwise specified, the term '' 'Department' '' means the Department of State.

(3) SECRETARY.—If not otherwise specified, the term '' 'Secretary' '' means the Secretary of State.

TITLE I—ORGANIZATION AND OPERATIONS OF THE DEPARTMENT OF STATE

SEC. 5101. SENSE OF CONGRESS ON IMPORTANCE OF DEPARTMENT OF STATE'S WORK.

It is the sense of Congress that—

(1) United States global engagement is key to a stable and prosperous world;

(2) United States leadership is indispensable in light of the many complex and interconnected threats facing the United States and the world;

(3) diplomacy and development are critical tools of national power, and full deployment of these tools is vital to United States national security;

(4) challenges such as the global refugee and migration crises, terrorism, historic famine and food insecurity, and fragile or repressive societies cannot be addressed without sustained and robust United States diplomatic and development leadership;

(5) the United States Government must use all of the instruments of national security and foreign policy at its disposal to protect United States citizens, promote United States interests and values, and support global stability and prosperity;

(6) United States security and prosperity depend on having partners and allies that share our interests and values, and these partnerships are nurtured and our shared interests and values are promoted through United States diplomatic engagement, security cooperation, economic statecraft, and assistance that helps further economic development, good governance, including the rule of law and democratic institutions, and the development of shared responses to natural and humanitarian disasters;

(7) as the United States Government agencies primarily charged with conducting diplomacy and development, the Department

and the United States Agency for International Development (USAID) require sustained and robust funding to carry out this important work, which is essential to our ability to project United States leadership and values and to advance United States interests around the world;

(8) the work of the Department and USAID makes the United States and the world safer and more prosperous by alleviating global poverty and hunger, fighting HIV/AIDS and other infectious diseases, strengthening alliances, expanding educational opportunities for women and girls, promoting good governance and democracy, supporting anti-corruption efforts, driving economic development and trade, preventing armed conflicts and humanitarian crises, and creating American jobs and export opportunities;

(9) the Department and USAID are vital national security agencies, whose work is critical to the projection of United States power and leadership worldwide, and without which Americans would be less safe, United States economic power would be diminished, and global stability and prosperity would suffer;

(10) investing in diplomacy and development before conflicts break out saves American lives while also being cost-effective; and

(11) the contributions of personnel working at the Department and USAID are extraordinarily valuable and allow the United States to maintain its leadership around the world.

SEC. 5102. ASSISTANT SECRETARY FOR INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS.

(a) IN GENERAL.—Section 1(c) of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a(c)) is amended—

(1) by redesignating paragraphs (3) and (4) as paragraphs (4) and (5); and

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

''(3) ASSISTANT SECRETARY FOR INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS.—

''(A) IN GENERAL.—There is authorized to be in the Department of State an Assistant Secretary for International Narcotics and Law Enforcement Affairs, who shall be responsible to the Secretary of State for all matters, programs, and related activities pertaining to international narcotics, anti-crime, and law enforcement affairs in the conduct of foreign policy by the Department, including, as appropriate, leading the coordination of programs carried out by United States Government agencies abroad, and such other related duties as the Secretary may from time to time designate.

''(B) AREAS OF RESPONSIBILITY.—The Assistant Secretary for International Narcotics and Law Enforcement Affairs shall maintain continuous observation and coordination of all matters pertaining to international narcotics, anti-crime, and law enforcement affairs in the conduct of foreign policy, including programs carried out by other United States Government agencies when such programs pertain to the following matters:

''(i) Combating international narcotics production and trafficking.

''(ii) Strengthening foreign justice systems, including judicial and prosecutorial capacity, appeals systems, law enforcement agencies, prison systems, and the sharing of recovered assets.

''(iii) Training and equipping foreign police, border control, other government officials, and other civilian law enforcement authorities for anti-crime purposes, including ensuring that no foreign security unit or member of such unit shall receive such assistance from the United States Government absent appropriate vetting.

''(iv) Ensuring the inclusion of human rights and women's participation issues in law enforcement programs, in consultation with the Assistant Secretary for Democracy, Human Rights, and Labor, and other senior officials in regional and thematic bureaus and offices.

''(v) Combating, in conjunction with other relevant bureaus of the Department of State and other United States Government agencies, all forms of transnational organized crime, including human trafficking, illicit trafficking in arms, wildlife, and cultural property, migrant smuggling, corruption, money laundering, the illicit smuggling of bulk cash, the licit use of financial systems for malign purposes, and other new and emerging forms of crime.

''(vi) Identifying and responding to global corruption, including strengthening the capacity of foreign government institutions responsible for addressing financial crimes and engaging with multilateral organizations responsible for monitoring and supporting foreign governments' anti-corruption efforts.

''(C) ADDITIONAL DUTIES.—In addition to the responsibilities specified in subparagraph (B), the Assistant Secretary for International Narcotics and Law Enforcement Affairs shall also—

''(i) carry out timely and substantive consultation with chiefs of mission and, as appropriate, the heads of other United States Government agencies to ensure effective coordination of all international narcotics and law enforcement programs carried out overseas by the Department and such other agencies;

''(ii) coordinate with the Office of National Drug Control Policy to ensure lessons learned from other United States Government agencies are available to the Bureau of International Narcotics and Law Enforcement Affairs of the Department;

''(iii) develop standard requirements for monitoring and evaluation of Bureau programs, including metrics for success that do not rely solely on the amounts of illegal drugs that are produced or seized;

''(iv) in coordination with the Secretary of State, annually certify in writing to the Committee on Foreign Relations of the Senate that United States and the Committee on Foreign Affairs of the House of Representatives enforcement personnel posted abroad whose activities are funded to any extent by the Bureau of International Narcotics and Law Enforcement Affairs are complying with section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927); and

''(v) carry out such other relevant duties as the Secretary may assign.

''(D) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to limit or impair the authority or responsibility of any other Federal agency with respect to law enforcement, domestic security operations, or intelligence activities as defined in Executive Order 12333.''.

(b) MODIFICATION OF ANNUAL INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT.—Subsection (a) of section 489 of the Foreign Assistance Act of 1961 (22 U.S.C. 2291h) is amended by inserting after paragraph (9) the following new paragraph:

''(10) A separate section that contains an identification of all United States Government-supported units funded by the Bureau of International Narcotics and Law Enforcement Affairs and any Bureau-funded operations by such units in which United States law enforcement personnel have been physically present.''.

SEC. 5103. BUREAU OF CONSULAR AFFAIRS; BUREAU OF POPULATION, REFUGEES, AND MIGRATION.

Section 1 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a) is amended—

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

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

''(g) BUREAU OF CONSULAR AFFAIRS.—There is in the Department of State the Bureau of Consular Affairs, which shall be headed by the Assistant Secretary of State for Consular Affairs.

''(h) BUREAU OF POPULATION, REFUGEES, AND MIGRATION.—There is in the Department of State the Bureau of Population, Refugees, and Migration, which shall be headed by the Assistant Secretary of State for Population, Refugees, and Migration.''.

SEC. 5104. OFFICE OF INTERNATIONAL DISABILITY RIGHTS.

(a) ESTABLISHMENT.—There should be established in the Department of State an Office of International Disability Rights (referred to in this section as the ''Office'').

(b) DUTIES.—The Office should—

(1) seek to ensure that all United States foreign operations are accessible to, and inclusive of, persons with disabilities;

(2) promote the human rights and full participation in international development activities of all persons with disabilities;

(3) promote disability inclusive practices and the training of Department of State staff on soliciting quality programs that are fully inclusive of people with disabilities;

(4) represent the United States in diplomatic and multilateral fora on matters relevant to the rights of persons with disabilities, and work to raise the profile of disability across a broader range of organizations contributing to international development efforts;

(5) conduct regular consultation with civil society organizations working to advance international disability rights and empower persons with disabilities internationally;

(6) consult with other relevant offices at the Department that are responsible for drafting annual reports documenting progress on human rights, including, wherever applicable, references to instances of discrimination, prejudice, or abuses of persons with disabilities;

(7) advise the Bureau of Human Resources or its equivalent within the Department regarding the hiring and recruitment and overseas practices of civil service employees and Foreign Service officers with disabilities and their family members with chronic medical conditions or disabilities; and

(8) carry out such other relevant duties as the Secretary of State may assign.

(c) SUPERVISION.—The Office may be headed by—

(1) a senior advisor to the appropriate Assistant Secretary of State; or

(2) an officer exercising significant authority who reports to the President or Secretary of State, appointed by and with the advice and consent of the Senate.

(d) CONSULTATION.—The Secretary of State should direct Ambassadors at Large, Representatives, Special Envoys, and coordinators working on human rights to consult with the Office to promote the human rights and full participation in international development activities of all persons with disabilities.

SEC. 5105. SPECIAL APPOINTMENT AUTHORITY.

Section 1 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a), as amended by section 5103 of this Act, is further amended by inserting after subsection (h) the following new subsection:

''(i) SPECIAL APPOINTMENTS.—

''(1) POSITIONS EXERCISING SIGNIFICANT AUTHORITY.—The President may, by and with the advice and consent of the Senate, appoint an individual as a Special Envoy, Special Representative, Special Coordinator, Special Negotiator, Envoy, Representative, Coordinator, Special Advisor, or other position performing a similar function, regardless of title, at the Department of State exercising significant authority pursuant to the laws of the United States. Except as provided in paragraph (3) or in clause 3, section 2, article II of the Constitution (relating to recess appointments), an individual may not be designated as a Special Envoy, Special Representative, Special Coordinator, Special Negotiator, Envoy, Representative, Coordinator, Special Advisor, or other position performing a similar function, regardless of title, at the Department exercising significant authority pursuant to the laws of the United States without the advice and consent of the Senate.

''(2) POSITIONS NOT EXERCISING SIGNIFICANT AUTHORITY.—The President or Secretary of State may appoint any Special Envoy, Special Representative, Special Coordinator, Special Negotiator, Special Envoy, Representative, Coordinator, Special Advisor, or other position performing a similar function, regardless of title, at the Department of State not exercising significant authority pursuant to the laws of the United States without the advice and consent of the Senate, if the President or Secretary, not later than 15 days before the appointment of a person to such a position, submits to the appropriate congressional committees a notification that includes the following:

''(A) A certification that the position does not require the exercise of significant authority pursuant to the laws of the United States.

''(B) A description of the duties and purpose of the position.

''(C) The rationale for giving the specific title and function to the position.

''(3) LIMITED EXCEPTION FOR TEMPORARY APPOINTMENTS EXERCISING SIGNIFICANT AUTHORITY.—The President may maintain or establish a position with the title of Special Envoy, Special Representative, Special Coordinator, Special Negotiator, Envoy, Representative, Coordinator, Special Advisor, or other position performing a similar function, regardless of title, at the Department of State exercising significant authority pursuant to the laws of the United States for not longer than 180 days if the Secretary of State, not later than 15 days after the appointment of a person to such a position, or 30 days after the date of the enactment of this subsection, whichever is earlier, submits to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a notification that includes the following:

''(A) The necessity for conferring such title and function.

''(B) The dates during which such title and function will be held.

''(C) The justification for not submitting the proposed conferral of such title and function to the Senate as a nomination for advice and consent to appointment.

''(D) All relevant information concerning any potential conflict of interest which the proposed recipient of such title and function may have with regard to the appointment.

''(4) RENEWAL OF TEMPORARY APPOINTMENT.—The President may renew for one period not to exceed 180 days any position maintained or established under paragraph (3) if the President, not later than 15 days before issuing such renewal, submits to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a detailed justification on the necessity of such extension, including the dates with respect to which such title will continue to be held and the justification for not submitting such title to the Senate as a nomination for advice and consent.

''(5) EXEMPTION.—Paragraphs (1) through (4) shall not apply to a Special Envoy, Special Representative, Special Coordinator, Special Negotiator, Envoy, Representative, Coordinator, Special Advisor, or other person performing a similar function, regardless of title, at the Department of State if the position is expressly mandated by statute.

''(6) EFFECTIVE DATE.—This subsection shall apply to appointments made on or after January 3, 2023.''.

SEC. 5106. REPEAL OF AUTHORITY FOR SPECIAL REPRESENTATIVE AND POLICY COORDINATOR FOR BURMA.

Section 7 of the Tom Lantos Block Burmese Jade (Junta's Anti-Democratic Efforts) Act of 2008 (Public Law 110–286; 50 U.S.C. 1701 note) relating to the establishment of a Special Representative and Policy Coordinator for Burma) is hereby repealed.

SEC. 5107. ANTI-PIRACY INFORMATION SHARING.

The Secretary is authorized to provide for the participation by the United States in the Information Sharing Centre located in Singapore, as established by the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP).

SEC. 5108. IMPORTANCE OF FOREIGN AFFAIRS TRAINING TO NATIONAL SECURITY.

It is the sense of Congress that—

(1) the Department is a crucial national security agency, whose employees, both Foreign and Civil Service, require the best possible training at every stage of their careers to prepare them to promote and defend United States national interests and the health and safety of United States citizens abroad;

(2) the Secretary should explore establishing a ''training float'' requiring that a certain percentage of the Foreign Service shall be in long-term training at any given time;

(3) the Department's Foreign Service Institute should seek to substantially increase its educational and training offerings to Department personnel, including developing new and innovative educational and training courses, methods, programs, and opportunities; and

(4) consistent with existing Department gift acceptance authority and other applicable laws, the Department and Foreign Service Institute may accept funds and other resources from foundations, not-for-profit corporations, and other appropriate sources to help the Department and the Institute accomplish the goals specified in paragraph (3).

SEC. 5109. CLASSIFICATION AND ASSIGNMENT OF FOREIGN SERVICE OFFICERS.

The Foreign Service Act of 1980 is amended—

(1) in section 501 (22 U.S.C. 3981), by inserting ''If a position designated under this section is unfilled for more than 365 calendar days, such position may be filled, as appropriate, on a temporary basis, in accordance with section 309.'' after ''Positions designated under this section are excepted from the competitive service.''; and

(2) in paragraph (2) of section 502(a) (22 U.S.C. 3982(a)), by inserting '', or domestically, in a position working on issues relating to a particular country or geographic area,'' after ''geographic area''.

SEC. 5110. REPORTING ON IMPLEMENTATION OF GAO RECOMMENDATIONS.

(a) INITIAL REPORT.—Not later than 120 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report that lists all of the Government Accountability Office's recommendations relating to the Department that have not been fully implemented.

(b) COMPTROLLER GENERAL REPORT.—Not later than 30 days after the Secretary submits the report under subsection (a), the Comptroller General of the United States shall submit to the appropriate congressional committees a report that identifies any discrepancies between the list of recommendations included in such report and the Government Accountability Office's list of outstanding recommendations for the Department.

(c) IMPLEMENTATION REPORT.—

(1) IN GENERAL.—Not later than 120 days after the date of the submission of the Comptroller General's report under subsection (b), the Secretary shall submit to the appropriate congressional committees a report that describes the implementation status of each recommendation from the Government Accountability Office included in the report submitted under subsection (a).

(2) JUSTIFICATION.—The report under paragraph (1) shall include—

(A) a detailed justification for each decision not to fully implement a recommendation or to implement a recommendation in a different manner than specified by the Government Accountability Office;

(B) a timeline for the full implementation of any recommendation the Secretary has decided to adopt, but has not yet fully implemented; and

(C) an explanation for any discrepancies included in the Comptroller General report submitted under subsection (b).

(d) FORM.—The information required in each report under this section shall be submitted in unclassified form, to the maximum extent practicable, but may be included in a classified annex to the extent necessary.

SEC. 5111. EXTENSION OF PERIOD FOR REIMBURSEMENT OF FISHERMEN FOR COSTS INCURRED FROM THE ILLEGAL SEIZURE AND DETENTION OF U.S.-FLAG FISHING VESSELS BY FOREIGN GOVERNMENTS.

(a) IN GENERAL.—Subsection (e) of section 7 of the Fishermen's Protective Act of 1967 (22 U.S.C. 1977) is amended to read as follows:

''(e) AMOUNTS.—Payments may be made under this section only to such extent and in such amounts as are provided in advance in appropriation Acts.''.

(b) RETROACTIVE APPLICABILITY.—

(1) EFFECTIVE DATE.—The amendment made by subsection (a) shall take effect on the date of the enactment of this Act and apply as if the date specified in subsection (e) of section 7 of the Fishermen's Protective Act of 1967, as in effect on the day before the date of the enactment of this Act, were the day after such date of enactment.

(2) AGREEMENTS AND PAYMENTS.—The Secretary is authorized to—

(A) enter into agreements pursuant to section 7 of the Fishermen's Protective Act of 1967 for any claims to which such section would otherwise apply but for the date specified in subsection (e) of such section, as in effect on the day before the date of the enactment of this Act; and

(B) make payments in accordance with agreements entered into pursuant to such section if any such payments have not been made as a result of the expiration of the date specified in such section, as in effect on the day before the date of the enactment of this Act.

SEC. 5112. ART IN EMBASSIES.

(a) IN GENERAL.—No funds are authorized to be appropriated for the purchase of any piece of art for the purposes of installation or display in any embassy, consulate, or

other foreign mission of the United States if the purchase price of such piece of art is in excess of $50,000, unless such purchase is subject to prior consultation with, and the regular notification procedures of, the appropriate congressional committees.

(b) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees and the Committees on Appropriations of the Senate and the House of Representatives a report on the costs of the Art in Embassies Program for each of fiscal years 2012, 2013, and 2014.

(c) SUNSET.—This section shall terminate on the date that is 2 years after the date of the enactment of this Act.

(d) DEFINITION.—In this section, the term ''art'' includes paintings, sculptures, photographs, industrial design, and craft art.

SEC. 5113. AMENDMENT OR REPEAL OF REPORTING REQUIREMENTS.

(a) BURMA.—

(1) IN GENERAL.—Section 570 of Public Law 104–208 is amended—

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

''(c) MULTILATERAL STRATEGY.—The President shall develop, in coordination with likeminded countries, a comprehensive, multilateral strategy to—

''(1) assist Burma in addressing corrosive malign influence of the People's Republic of China; and

''(2) support a return to democratic governance, and support constitutional, economic, and security sector reforms in Burma designed to—

''(A) advance democratic development and improve human rights practices and the quality of life; and

''(B) promote genuine national reconciliation.''; and

(B) in subsection (d)—

(i) in the matter preceding paragraph (1), by striking ''six months'' and inserting ''year'';

(ii) by redesignating paragraph (3) as paragraph (7); and

(iii) by inserting after paragraph (2) the following new paragraphs:

''(3) improvements in human rights practices;

''(4) progress toward broad-based and inclusive economic growth; and

''(5) progress toward genuine national reconciliation.''.

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall take effect on the date of the enactment of this Act and apply with respect to the first report required under subsection (d) of section 570 of Public Law 104–208 that is required after the date of the enactment of this Act.

(b) REPEALS.—The following provisions of law are hereby repealed:

(1) Subsection (b) of section 804 of Public Law 101–246.

(2) Section 6 of Public Law 104–45.

(3) Subsection (c) of section 702 of Public Law 96–465 (22 U.S.C. 4022).

(4) Section 404 of the Arms Control and Disarmament Act (22 U.S.C. 2593b).

(5) Section 5 of Public Law 94–304 (22 U.S.C. 3005).

(6) Subsection (b) of section 502 of the International Security and Development Cooperation Act of 1985 (22 U.S.C. 2349aa–7).

(c) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State and the Administrator of the United States Agency for International Development shall submit to the appropriate congressional committees a report that includes each of the following:

(1) A list of all reports described in subsection (d) required to be submitted by their respective agency.

(2) For each such report, a citation to the provision of law under which the report is required to be submitted.

(3) The reporting frequency of each such report.

(4) The estimated cost of each report, to include personnel time costs.

(d) COVERED REPORTS.—A report described in this subsection is a recurring report that is required to be submitted to Congress by the Department of State or the United States Agency for International Development, or by any officer, official, component, or element of each entity.

(e) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives and the Committees on Appropriations of the Senate and the House of Representatives.

TITLE II—EMBASSY CONSTRUCTION

SEC. 5201. EMBASSY SECURITY, CONSTRUCTION, AND MAINTENANCE.

For ''Embassy Security, Construction, and Maintenance'', there is authorized to be appropriated $1,975,449,000 for fiscal year 2022.

SEC. 5202. STANDARD DESIGN IN CAPITAL CONSTRUCTION.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the Department's Bureau of Overseas Building Operations (OBO) or successor office should give appropriate consideration to standardization in construction, in which each new United States embassy and consulate starts with a standard design and keeps customization to a minimum.

(b) CONSULTATION.—The Secretary shall carry out any new United States embassy compound or new consulate compound project that utilizes a non-standard design, including those projects that are in the design or pre-design phase as of the date of the enactment of this Act, only in consultation with the appropriate congressional committees. The Secretary shall provide the appropriate congressional committees, for each such project, the following documentation:

(1) A comparison of the estimated full lifecycle costs of the project to the estimated full lifecycle costs of such project if it were to use a standard design.

(2) A comparison of the estimated completion date of such project to the estimated completion date of such project if it were to use a standard design.

(3) A comparison of the security of the completed project to the security of such completed project if it were to use a standard design.

(4) A justification for the Secretary's selection of a non-standard design over a standard design for such project.

(5) A written explanation if any of the documentation necessary to support the comparisons and justification, as the case may be, described in paragraphs (1) through (4) cannot be provided.

(c) SUNSET.—The consultation requirement under subsection (b) shall expire on the date that is 4 years after the date of the enactment of this Act.

SEC. 5203. CAPITAL CONSTRUCTION TRANSPARENCY.

Section 118 of the Department of State Authorities Act, Fiscal Year 2017 (22 U.S.C. 304) is amended—

(1) in the section heading , by striking ''**ANNUAL REPORT ON EMBASSY CONSTRUCTION COSTS**'' and inserting ''**BIANNUAL REPORT ON OVERSEAS CAPITAL CONSTRUCTION PROJECTS**''; and

(2) by striking subsections (a) and (b) and inserting the following new subsections:

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection and every 180 days thereafter until the date that is 4 years after such date of enactment, the Secretary shall submit to the appropriate congressional committees and the Committees on Appropriations of the Senate and the House of Representatives a comprehensive report regarding all ongoing overseas capital construction projects and major embassy security upgrade projects.

''(b) CONTENTS.—Each report required under subsection (a) shall include the following with respect to each ongoing overseas capital construction project and major embassy security upgrade project:

''(1) The initial cost estimate as specified in the proposed allocation of capital construction and maintenance funds required by the Committees on Appropriations for Acts making appropriations for the Department of State, foreign operations, and related programs.

''(2) The current cost estimate.

''(3) The value of each request for equitable adjustment received by the Department to date.

''(4) The value of each certified claim received by the Department to date.

''(5) The value of any usage of the project's contingency fund to date and the value of the remainder of the project's contingency fund.

''(6) An enumerated list of each request for adjustment and certified claim that remains outstanding or unresolved.

''(7) An enumerated list of each request for equitable adjustment and certified claim that has been fully adjudicated or that the Department has settled, and the final dollar amount of each adjudication or settlement.

''(8) The date of estimated completion specified in the proposed allocation of capital construction and maintenance funds required by the Committees on Appropriations not later than 45 days after the date of the enactment of an Act making appropriations for the Department of State, foreign operations, and related programs.

''(9) The current date of estimated completion.''.

SEC. 5204. CONTRACTOR PERFORMANCE INFORMATION.

(a) DEADLINE FOR COMPLETION.—The Secretary shall complete all contractor performance evaluations outstanding as of the date of the enactment of this Act required by subpart 42.15 of the Federal Acquisition Regulation for those contractors engaged in construction of new embassy or new consulate compounds by April 1, 2022.

(b) PRIORITIZATION SYSTEM.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall develop a prioritization system for clearing the current backlog of required evaluations referred to in subsection (a).

(2) ELEMENTS.—The system required under paragraph (1) should prioritize the evaluations as follows:

(A) Project completion evaluations should be prioritized over annual evaluations.

(B) Evaluations for relatively large contracts should have priority.

(C) Evaluations that would be particularly informative for the awarding of government contracts should have priority.

(c) BRIEFING.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall brief the appropriate congressional committees on the Department's plan for completing all evaluations by April 1, 2022, in accordance with subsection (a) and the prioritization system developed pursuant to subsection (b).

(d) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) contractors deciding whether to bid on Department contracts would benefit from

greater understanding of the Department as a client; and

(2) the Department should develop a forum where contractors can comment on the Department's project management performance.

SEC. 5205. GROWTH PROJECTIONS FOR NEW EMBASSIES AND CONSULATES.

(a) IN GENERAL.—For each new United States embassy compound (NEC) and new consulate compound project (NCC) in or not yet in the design phase as of the date of the enactment of this Act, the Department shall project growth over the estimated life of the facility using all available and relevant data, including the following:

(1) Relevant historical trends for Department personnel and personnel from other agencies represented at the NEC or NCC that is to be constructed.

(2) An analysis of the tradeoffs between risk and the needs of United States Government policy conducted as part of the most recent Vital Presence Validation Process, if applicable.

(3) Reasonable assumptions about the strategic importance of the NEC or NCC, as the case may be, over the life of the building at issue.

(4) Any other data that would be helpful in projecting the future growth of NEC or NCC.

(b) OTHER FEDERAL AGENCIES.—The head of each Federal agency represented at a United States embassy or consulate shall provide to the Secretary, upon request, growth projections for the personnel of each such agency over the estimated life of each embassy or consulate, as the case may be.

(c) BASIS FOR ESTIMATES.—The Department shall base its growth assumption for all NECs and NCCs on the estimates required under subsections (a) and (b).

(d) CONGRESSIONAL NOTIFICATION.—Any congressional notification of site selection for a NEC or NCC submitted after the date of the enactment of this Act shall include the growth assumption used pursuant to subsection (c).

SEC. 5206. LONG-RANGE PLANNING PROCESS.

(a) PLANS REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter for the next five years as the Secretary of State considers appropriate, the Secretary shall develop—

(A) a comprehensive 6-year plan documenting the Department's overseas building program for the replacement of overseas diplomatic posts taking into account security factors under the Secure Embassy Construction and Counterterrorism Act of 1999 and other relevant statutes and regulations, as well as occupational safety and health factors pursuant to the Occupational Safety and Health Act of 1970 and other relevant statutes and regulations, including environmental factors such as indoor air quality that impact employee health and safety; and

(B) a comprehensive 6-year plan detailing the Department's long-term planning for the maintenance and sustainment of completed diplomatic posts, which takes into account security factors under the Secure Embassy Construction and Counterterrorism Act of 1999 and other relevant statutes and regulations, as well as occupational safety and health factors pursuant to the Occupational Safety and Health Act of 1970 and other relevant statutes and regulations, including environmental factors such as indoor air quality that impact employee health and safety.

(2) INITIAL REPORT.—The first plan developed pursuant to paragraph (1)(A) shall also include a one-time status report on existing small diplomatic posts and a strategy for establishing a physical diplomatic presence in countries in which there is no current physical diplomatic presence and with which the United States maintains diplomatic relations. Such report, which may include a classified annex, shall include the following:

(A) A description of the extent to which each small diplomatic post furthers the national interest of the United States.

(B) A description of how each small diplomatic post provides American Citizen Services, including data on specific services provided and the number of Americans receiving services over the previous year.

(C) A description of whether each small diplomatic post meets current security requirements.

(D) A description of the full financial cost of maintaining each small diplomatic post.

(E) Input from the relevant chiefs of mission on any unique operational or policy value the small diplomatic post provides.

(F) A recommendation of whether any small diplomatic posts should be closed.

(3) UPDATED INFORMATION.—The annual updates of each of the plans developed pursuant to paragraph (1) shall highlight any changes from the previous year's plan to the ordering of construction and maintenance projects.

(b) REPORTING REQUIREMENTS.—

(1) SUBMISSION OF PLANS TO CONGRESS.—Not later than 60 days after the completion of each plan required under subsection (a), the Secretary shall submit the plans to the appropriate congressional committees and the Committees on Appropriations of the Senate and the House of Representatives.

(2) REFERENCE IN BUDGET JUSTIFICATION MATERIALS.—In the budget justification materials submitted to the appropriate congressional committees in support of the Department's budget for any fiscal year (as submitted with the budget of the President under section 1105(a) of title 31, United States Code), the plans required under subsection (a) shall be referenced to justify funding requested for building and maintenance projects overseas.

(3) FORM OF REPORT.—Each report required under paragraph (1) shall be submitted in unclassified form but may include a classified annex.

(c) SMALL DIPLOMATIC POST DEFINED.—In this section, the term ''small diplomatic post'' means any United States embassy or consulate that has employed five or fewer United States Government employees or contractors on average over the 36 months prior to the date of the enactment of this Act.

SEC. 5207. VALUE ENGINEERING AND RISK ASSESSMENT.

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

(1) Federal departments and agencies are required to use value engineering (VE) as a management tool, where appropriate, to reduce program and acquisition costs pursuant to OMB Circular A–131, Value Engineering, dated December 31, 2013.

(2) OBO has a Policy Directive and Standard Operation Procedure, dated May 24, 2017, on conducting risk management studies on all international construction projects.

(b) NOTIFICATION REQUIREMENTS.—

(1) SUBMISSION TO AUTHORIZING COMMITTEES.—Any operating plan that includes the allocation of capital construction and maintenance funds shall be submitted to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(2) REQUIREMENT TO CONFIRM COMPLETION OF VALUE ENGINEERING AND RISK ASSESSMENT STUDIES.—The notifications required under paragraph (1) shall include confirmation that the Department has completed the requisite VE and risk management process described in subsection (a), or applicable successor process.

(c) REPORTING AND BRIEFING REQUIREMENTS.—The Secretary shall provide to the appropriate congressional committees upon request—

(1) a description of each risk management study referred to in subsection (a)(2) and a table detailing which recommendations related to each such study were accepted and which were rejected; and

(2) a report or briefing detailing the rationale for not implementing any such recommendations that may otherwise yield significant cost savings to the Department if implemented.

SEC. 5208. BUSINESS VOLUME.

Section 402(c)(2)(E) of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (22 U.S.C. 4852(c)(2)(E)) is amended by striking ''in 3 years'' and inserting ''cumulatively over 3 years''.

SEC. 5209. EMBASSY SECURITY REQUESTS AND DEFICIENCIES.

The Secretary of State shall provide to the appropriate congressional committees, the Committee on Armed Services of the House of Representatives, and the Committee on Armed Services of the Senate upon request information on physical security deficiencies at United States diplomatic posts, including relating to the following:

(1) Requests made over the previous year by United States diplomatic posts for security upgrades.

(2) Significant security deficiencies at United States diplomatic posts that are not operating out of a new embassy compound or new consulate compound.

SEC. 5210. OVERSEAS SECURITY BRIEFINGS.

Not later than one year after the date of the enactment of this Act, the Secretary of State shall revise the Foreign Affairs Manual to stipulate that information on the current threat environment shall be provided to all United States Government employees under chief of mission authority traveling to a foreign country on official business. To the extent practicable, such material shall be provided to such employees prior to their arrival at a United States diplomatic post or as soon as possible thereafter.

SEC. 5211. CONTRACTING METHODS IN CAPITAL CONSTRUCTION.

(a) DELIVERY.—Unless the Secretary of State notifies the appropriate congressional committees that the use of the design-build project delivery method would not be appropriate, the Secretary shall make use of such method at United States diplomatic posts that have not yet received design or capital construction contracts as of the date of the enactment of this Act.

(b) NOTIFICATION.—Before executing a contract for a delivery method other than design-build in accordance with subsection (a), the Secretary of State shall notify the appropriate congressional committees in writing of the decision, including the reasons therefor. The notification required by this subsection may be included in any other report regarding a new United States diplomatic post that is required to be submitted to the appropriate congressional committees.

(c) PERFORMANCE EVALUATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State shall report to the appropriate congressional committees regarding performance evaluation measures in accordance with GAO's ''Standards for Internal Control in the Federal Government'' that will be applicable to design and construction, lifecycle cost, and building maintenance programs of the Bureau of Overseas Building Operations of the Department.

SEC. 5212. COMPETITION IN EMBASSY CONSTRUCTION.

Not later than 45 days after the date of the enactment of this Act, the Secretary of

State shall submit to the appropriate congressional committee and the Committees on Appropriations of the Senate and the House of Representatives a report detailing steps the Department of State is taking to expand the embassy construction contractor base in order to increase competition and maximize value.

SEC. 5213. STATEMENT OF POLICY.

It is the policy of the United States that the Bureau of Overseas Building Operations of the Department or its successor office shall continue to balance functionality and security with accessibility, as defined by guidelines established by the United States Access Board in constructing embassies and consulates, and shall ensure compliance with the Architectural Barriers Act of 1968 (42 U.S.C. 4151 et seq.) to the fullest extent possible.

SEC. 5214. DEFINITIONS.

In this title:

(1) DESIGN-BUILD.—The term ''design-build'' means a method of project delivery in which one entity works under a single contract with the Department to provide design and construction services.

(2) NON-STANDARD DESIGN.—The term ''non-standard design'' means a design for a new embassy compound project or new consulate compound project that does not utilize a standardized design for the structural, spatial, or security requirements of such embassy compound or consulate compound, as the case may be.

TITLE III—PERSONNEL ISSUES

SEC. 5301. DEFENSE BASE ACT INSURANCE WAIVERS.

(a) APPLICATION FOR WAIVERS.—Not later than 30 days after the date of the enactment of this Act, the Secretary shall apply to the Department of Labor for a waiver from insurance requirements under the Defense Base Act (42 U.S.C. 1651 et seq.) for all countries with respect to which the requirement was waived prior to January 2017, and for which there is not currently a waiver.

(b) CERTIFICATION REQUIREMENT.—Not later than 45 days after the date of the enactment of this Act, the Secretary shall certify to the appropriate congressional committees that the requirement in subsection (a) has been met.

SEC. 5302. STUDY ON FOREIGN SERVICE ALLOWANCES.

(a) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than one year after date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report detailing an empirical analysis on the effect of overseas allowances on the foreign assignment of Foreign Service officers (FSOs), to be conducted by a federally-funded research and development center with appropriate expertise in labor economics and military compensation.

(2) CONTENTS.—The analysis required under paragraph (1) shall—

(A) identify all allowances paid to FSOs assigned permanently or on temporary duty to foreign areas;

(B) examine the efficiency of the Foreign Service bidding system in determining foreign assignments;

(C) examine the factors that incentivize FSOs to bid on particular assignments, including danger levels and hardship conditions;

(D) examine the Department's strategy and process for incentivizing FSOs to bid on assignments that are historically in lower demand, including with monetary compensation, and whether monetary compensation is necessary for assignments in higher demand;

(E) make any relevant comparisons to military compensation and allowances, noting which allowances are shared or based on the same regulations;

(F) recommend options for restructuring allowances to improve the efficiency of the assignments system and better align FSO incentives with the needs of the Foreign Service, including any cost savings associated with such restructuring;

(G) recommend any statutory changes necessary to implement subparagraph (F), such as consolidating existing legal authorities for the provision of hardship and danger pay; and

(H) detail any effects of recommendations made pursuant to subparagraphs (F) and (G) on other United States Government departments and agencies with civilian employees permanently assigned or on temporary duty in foreign areas, following consultation with such departments and agencies.

(b) BRIEFING REQUIREMENT.—Before initiating the analysis required under subsection (a)(1), and not later than 60 days after the date of the enactment of this Act, the Secretary shall provide to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs in the House of Representatives a briefing on the implementation of this section that includes the following:

(1) The name of the federally funded research and development center that will conduct such analysis.

(2) The scope of such analysis and terms of reference for such analysis as specified between the Department and such federally funded research and development center.

(c) AVAILABILITY OF INFORMATION.—

(1) IN GENERAL.—The Secretary shall make available to the federally-funded research and development center carrying out the analysis required under subsection (a)(1) all necessary and relevant information to allow such center to conduct such analysis in a quantitative and analytical manner, including historical data on the number of bids for each foreign assignment and any survey data collected by the Department from eligible bidders on their bid decision-making.

(2) COOPERATION.—The Secretary shall work with the heads of other relevant United States Government departments and agencies to ensure such departments and agencies provide all necessary and relevant information to the federally-funded research and development center carrying out the analysis required under subsection (a)(1).

(d) INTERIM REPORT TO CONGRESS.—The Secretary shall require that the chief executive officer of the federally-funded research and development center that carries out the analysis required under subsection (a)(1) submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives an interim report on such analysis not later than 180 days after the date of the enactment of this Act.

SEC. 5303. SCIENCE AND TECHNOLOGY FELLOWSHIPS.

Section 504 of the Foreign Relations Authorization Act, Fiscal Year 1979 (22 U.S.C. 2656d) is amended by adding at the end the following new subsection:

''(e) GRANTS AND COOPERATIVE AGREEMENTS RELATED TO SCIENCE AND TECHNOLOGY FELLOWSHIP PROGRAMS.—

''(1) IN GENERAL.—The Secretary is authorized to make grants or enter into cooperative agreements related to Department of State science and technology fellowship programs, including for assistance in recruiting fellows and the payment of stipends, travel, and other appropriate expenses to fellows.

''(2) EXCLUSION FROM CONSIDERATION AS COMPENSATION.—Stipends under paragraph (1) shall not be considered compensation for purposes of section 209 of title 18, United States Code.

''(3) MAXIMUM ANNUAL AMOUNT.—The total amount of grants made pursuant to this subsection may not exceed $500,000 in any fiscal year.''.

SEC. 5304. TRAVEL FOR SEPARATED FAMILIES.

Section 901(15) of the Foreign Service Act of 1980 (22 U.S.C. 4081(15)) is amended—

(1) in the matter preceding subparagraph (A), by striking ''1 round-trip per year for each child below age 21 of a member of the Service assigned abroad'' and inserting ''in the case of one or more children below age 21 of a member of the Service assigned abroad, 1 round-trip per year'';

(2) in subparagraph (A)—

(A) by inserting ''for each child'' before ''to visit the member abroad''; and

(B) by striking ''; or'' and inserting a comma;

(3) in subparagraph (B)—

(A) by inserting ''for each child'' before ''to visit the other parent''; and

(B) by inserting ''or'' after ''resides,'';

(4) by inserting after subparagraph (B) the following new subparagraph:

''(C) for one of the child's parents to visit the child or children abroad if the child or children do not regularly reside with that parent and that parent is not receiving an education allowance or educational travel allowance for the child or children under section 5924(4) of title 5, United States Code,''; and

(5) in the matter following subparagraph (C), as added by paragraph (4) of this section, by striking ''a payment'' and inserting ''the cost of round-trip travel''.

SEC. 5305. HOME LEAVE TRAVEL FOR SEPARATED FAMILIES.

Section 903(b) of the Foreign Service Act of 1980 (22 U.S.C. 4083(b)) is amended by adding at the end the following new sentence: ''In cases in which a member of the Service has official orders to an unaccompanied post and in which the family members of the member reside apart from the member at authorized locations outside the United States, the member may take the leave ordered under this section where that member's family members reside, notwithstanding section 6305 of title 5, United States Code.''.

SEC. 5306. SENSE OF CONGRESS REGARDING CERTAIN FELLOWSHIP PROGRAMS.

It is the sense of Congress that Department fellowships that promote the employment of candidates belonging to under-represented groups, including the Charles B. Rangel International Affairs Graduate Fellowship Program, the Thomas R. Pickering Foreign Affairs Fellowship Program, and the Donald M. Payne International Development Fellowship Program, represent smart investments vital for building a strong, capable, and representative national security workforce.

SEC. 5307. TECHNICAL CORRECTION.

Subparagraph (A) of section 601(c)(6) of the Foreign Service Act of 1980 (22 U.S.C. 4001(c)(6)) is amended, in the matter preceding clause (i), by—

(1) striking ''promotion'' and inserting ''promotion, on or after January 1, 2017,''; and

(2) striking ''individual joining the Service on or after January 1, 2017,'' and inserting ''Foreign Service officer, appointed under section 302(a)(1), who has general responsibility for carrying out the functions of the Service''.

SEC. 5308. FOREIGN SERVICE AWARDS.

(a) IN GENERAL.—Section 614 of the Foreign Service Act of 1980 (22 U.S.C. 4013) is amended—

(1) by amending the section heading to read as follows: ''DEPARTMENT AWARDS''; and

(2) in the first sentence, by inserting ''or Civil Service'' after ''the Service''.

(b) CONFORMING AMENDMENT.—The item relating to section 614 in the table of contents of the Foreign Service Act of 1980 is amended to read as follows:

''Sec. 614. Department awards.''.

SEC. 5309. DIPLOMATIC PROGRAMS.

(a) SENSE OF CONGRESS ON WORKFORCE RECRUITMENT.—It is the sense of Congress that the Secretary should continue to hold entry-level classes for Foreign Service officers and specialists and continue to recruit civil servants through programs such as the Presidential Management Fellows Program and Pathways Internship Programs in a manner and at a frequency consistent with prior years and consistent with the need to maintain a pool of experienced personnel effectively distributed across skill codes and ranks. It is further the sense of Congress that absent continuous recruitment and training of Foreign Service officers and civil servants, the Department will lack experienced, qualified personnel in the short, medium, and long terms.

(b) LIMITATION.—The Secretary should not implement any reduction-in-force action under section 3502 or 3595 of title 5, United States Code, or for any incentive payments for early separation or retirement under any other provision of law unless—

(1) the appropriate congressional committees are notified not less than 15 days in advance of such obligation or expenditure; and

(2) the Secretary has provided to the appropriate congressional committees a detailed report that describes the Department's strategic staffing goals, including—

(A) a justification that describes how any proposed workforce reduction enhances the effectiveness of the Department;

(B) a certification that such workforce reduction is in the national interest of the United States;

(C) a comprehensive strategic staffing plan for the Department, including 5-year workforce forecasting and a description of the anticipated impact of any proposed workforce reduction; and

(D) a dataset displaying comprehensive workforce data for all current and planned employees of the Department, disaggregated by—

(i) Foreign Service officer and Foreign Service specialist rank;

(ii) civil service job skill code, grade level, and bureau of assignment;

(iii) contracted employees, including the equivalent job skill code and bureau of assignment; and

(iv) employees hired under schedule C of subpart C of part 213 of title 5, Code of Federal Regulations, including their equivalent grade and job skill code and bureau of assignment.

SEC. 5310. SENSE OF CONGRESS REGARDING VETERANS EMPLOYMENT AT THE DEPARTMENT OF STATE.

It is the sense of Congress that—

(1) the Department should continue to promote the employment of veterans, in accordance with section 301 of the Foreign Service Act of 1980 (22 U.S.C. 3941), as amended by section 5406 of this Act, including those veterans belonging to traditionally underrepresented groups at the Department;

(2) veterans employed by the Department have made significant contributions to United States foreign policy in a variety of regional and global affairs bureaus and diplomatic posts overseas; and

(3) the Department should continue to encourage veteran employment and facilitate their participation in the workforce.

SEC. 5311. EMPLOYEE ASSIGNMENT RESTRICTIONS AND PRECLUSIONS.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the Department should expand the appeal process it makes available to employees related to assignment preclusions and restrictions.

(b) APPEAL OF ASSIGNMENT RESTRICTION OR PRECLUSION.—Subsection (a) of section 414 of the Department of State Authorities Act, Fiscal Year 2017 (22 U.S.C. 2734c(a)) is amended by adding at the end the following new sentences: ''Such right and process shall ensure that any employee subjected to an assignment restriction or preclusion shall have the same appeal rights as provided by the Department regarding denial or revocation of a security clearance. Any such appeal shall be resolved not later than 60 days after such appeal is filed.''.

(c) NOTICE AND CERTIFICATION.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall revise, and certify to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives regarding such revision, the Foreign Affairs Manual guidance regarding denial or revocation of a security clearance to expressly state that all review and appeal rights relating thereto shall also apply to any recommendation or decision to impose an assignment restriction or preclusion to an employee.

SEC. 5312. RECALL AND REEMPLOYMENT OF CAREER MEMBERS.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) career Department employees provide invaluable service to the United States as nonpartisan professionals who contribute subject matter expertise and professional skills to the successful development and execution of United States foreign policy; and

(2) reemployment of skilled former members of the Foreign and civil service who have voluntarily separated from the Foreign or civil service due to family reasons or to obtain professional skills outside government is of benefit to the Department.

(b) NOTICE OF EMPLOYMENT OPPORTUNITIES.—Title 5, United States Code, is amended by inserting after chapter 102 the following new chapter:

''CHAPTER 103—DEPARTMENT OF STATE

''Sec.

''10301. Notice of employment opportunities for Department of State and USAID positions.

''10302. Consulting services for the Department of State.

''§ 10301. Notice of employment opportunities for Department of State and USAID positions

''To ensure that individuals who have separated from the Department of State or the United States Agency for International Development and who are eligible for reappointment are aware of such opportunities, the Department of State and the United States Agency for International Development shall publicize notice of all employment opportunities, including positions for which the relevant agency is accepting applications from individuals within the agency's workforce under merit promotion procedures, on publicly accessible sites, including www.usajobs.gov. If using merit promotion procedures, the notice shall expressly state that former employees eligible for reinstatement may apply.''.

(c) CLERICAL AMENDMENT.—The table of chapters at the beginning of title 5, United States Code, is amended by inserting after the item relating to chapter 102 the following:

''103. Department of State .....10301.''.

SEC. 5313. STRATEGIC STAFFING PLAN FOR THE DEPARTMENT OF STATE.

(a) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees and the Committees on Appropriations of the Senate and the House of Representatives a comprehensive 5-year strategic staffing plan for the Department that is aligned with and furthers the objectives of the National Security Strategy of the United States of America issued in December 2017, or any subsequent strategy issued not later than 18 months after the date of the enactment of this Act, which shall include the following:

(1) A dataset displaying comprehensive workforce data, including all shortages in bureaus described in GAO report GAO–19–220, for all current and planned employees of the Department, disaggregated by—

(A) Foreign Service officer and Foreign Service specialist rank;

(B) civil service job skill code, grade level, and bureau of assignment;

(C) contracted employees, including the equivalent job skill code and bureau of assignment; and

(D) employees hired under schedule C of subpart C of part 213 of title 5, Code of Federal Regulations, including the equivalent grade and job skill code and bureau of assignment of such employee.

(2) Recommendations on the number of Foreign Service officers disaggregated by service cone that should be posted at each United States diplomatic post and in the District of Columbia, with a detailed basis for such recommendations.

(3) Recommendations on the number of civil service officers that should be employed by the Department, with a detailed basis for such recommendations.

(b) MAINTENANCE.—The dataset required under subsection (a)(1) shall be maintained and updated on a regular basis.

(c) CONSULTATION.—The Secretary shall lead the development of the plan required under subsection (a) but may consult or partner with private sector entities with expertise in labor economics, management, or human resources, as well as organizations familiar with the demands and needs of the Department's workforce.

(d) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Secretary of State shall submit to the appropriate congressional committees a report regarding root causes of Foreign Service and civil service shortages, the effect of such shortages on national security objectives, and the Department's plan to implement recommendations described in GAO–19–220.

SEC. 5314. CONSULTING SERVICES.

Chapter 103 of title 5, United States Code, as added by section 5312, is amended by adding at the end the following:

''§ 10302. Consulting services for the Department of State

''Any consulting service obtained by the Department of State through procurement contract pursuant to section 3109 of title 5, United States Code, shall be limited to those contracts with respect to which expenditures are a matter of public record and available for public inspection, except if otherwise provided under existing law, or under existing Executive order issued pursuant to existing law.''.

SEC. 5315. INCENTIVES FOR CRITICAL POSTS.

Section 1115(d) of the Supplemental Appropriations Act, 2009 (Public Law 111–32) is amended by striking the last sentence.

SEC. 5316. EXTENSION OF AUTHORITY FOR CERTAIN ACCOUNTABILITY REVIEW BOARDS.

Section 301(a)(3) of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (22 U.S.C. 4831(a)(3)) is amended—

(1) in the heading, by striking ''AFGHANISTAN AND'' and inserting ''AFGHANISTAN, YEMEN, SYRIA, AND''; and

(2) in subparagraph (A)—

(A) in clause (i), by striking ''Afghanistan or'' and inserting ''Afghanistan, Yemen, Syria, or''; and

(B) in clause (ii), by striking ''beginning on October 1, 2005, and ending on September 30, 2009'' and inserting ''beginning on October 1, 2020, and ending on September 30, 2022''.

SEC. 5317. FOREIGN SERVICE SUSPENSION WITHOUT PAY.

Subsection (c) of section 610 of the Foreign Service Act of 1980 (22 U.S.C. 4010) is amended—

(1) in paragraph (1), in the matter preceding subparagraph (A), by striking ''suspend'' and inserting ''indefinitely suspend without duties'';

(2) by redesignating paragraph (5) as paragraph (7);

(3) by inserting after paragraph (4) the following new paragraphs:

''(5) Any member of the Service suspended from duties under this subsection may be suspended without pay only after a final written decision is provided to such member under paragraph (2).

''(6) If no final written decision under paragraph (2) has been provided within 1 calendar year of the date the suspension at issue was proposed, not later than 30 days thereafter the Secretary of State shall report to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate in writing regarding the specific reasons for such delay.''; and

(4) in paragraph (7), as so redesignated—

(A) by striking ''(7) In this subsection:'';

(B) in subparagraph (A), by striking ''(A) The term'' and inserting the following:

''(7) In this subsection, the term'';

(C) by striking subparagraph (B) (relating to the definition of ''suspend'' and ''suspension''); and

(D) by redesignating clauses (i) and (ii) as subparagraphs (A) and (B), respectively; and moving such subparagraphs 2 ems to the left.

SEC. 5318. FOREIGN AFFAIRS MANUAL AND FOREIGN AFFAIRS HANDBOOK CHANGES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter for 5 years, the Secretary shall submit to the appropriate congressional committees a report detailing all changes made to the Foreign Affairs Manual or the Foreign Affairs Handbook.

(b) COVERED PERIODS.—The first report required under subsection (a) shall cover the 5-year period preceding the submission of such report. Each subsequent report shall cover the 180-day period preceding submission.

(c) CONTENTS.—Each report required under subsection (a) shall contain the following:

(1) The location within the Foreign Affairs Manual or the Foreign Affairs Handbook where a change has been made.

(2) The statutory basis for each such change.

(3) A side-by-side comparison of the Foreign Affairs Manual or Foreign Affairs Handbook before and after such change.

(4) A summary of such changes displayed in spreadsheet form.

SEC. 5319. WAIVER AUTHORITY FOR INDIVIDUAL OCCUPATIONAL REQUIREMENTS OF CERTAIN POSITIONS.

The Secretary of State may waive any or all of the individual occupational requirements with respect to an employee or prospective employee of the Department of State for a civilian position categorized under the GS–0130 occupational series if the Secretary determines that the individual possesses significant scientific, technological, engineering, or mathematical expertise that is integral to performing the duties of the applicable position, based on demonstrated job performance and qualifying experience. With respect to each waiver granted under this subsection, the Secretary shall set forth in a written document that is transmitted to the Director of the Office of Personnel Management the rationale for the decision of the Secretary to waive such requirements.

SEC. 5320. APPOINTMENT OF EMPLOYEES TO THE GLOBAL ENGAGEMENT CENTER.

The Secretary may appoint, for a 3-year period that may be extended for up to an additional 2 years, solely to carry out the functions of the Global Engagement Center, employees of the Department without regard to the provisions of title 5, United States Code, governing appointment in the competitive service, and may fix the basic compensation of such employees without regard to chapter 51 and subchapter III of chapter 53 of such title.

SEC. 5321. EDUCATION ALLOWANCES DUE TO CORONAVIRUS.

(a) IN GENERAL.—The authority under section 5924 of title 5, United States Code, may be exercised by the Secretary of State and the heads of other Federal agencies for education allowances to employees who are in the United States with assignment orders to a foreign area and for whom service abroad has been interrupted or delayed because of the coronavirus pandemic without regard to the foreign area limitations referenced therein.

(b) TERMINATION.—The authority under subsection shall expire on September 30, 2022.

SEC. 5322. COMPETITIVE STATUS FOR CERTAIN EMPLOYEES HIRED BY INSPECTORS GENERAL TO SUPPORT THE LEAD IG MISSION.

Subparagraph (A) of section 8L(d)(5)(A) of the Inspector General Act of 1978 (5 U.S.C. App.) is amended by striking ''a lead Inspector General for'' and inserting ''any of the Inspectors General specified in subsection (c) for oversight of''.

SEC. 5323. REPORT RELATING TO FOREIGN SERVICE OFFICER TRAINING AND DEVELOPMENT.

(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of State shall submit to the appropriate committees of Congress a report certain fellowship or detail opportunities for Department of State Foreign Service personnel.

(b) ELEMENTS.—The report required by subsection (a) shall include the following elements:

(1) The number of Senior Foreign Service Officer generalists who, as of the date of the enactment of this Act, have done a tour of at least one year in any of the agencies or congressional committees described in subsection (a).

(2) The total number of senior Foreign Service Officer generalists as of the date of the enactment of this Act.

(3) The average number of Senior Foreign Service Officer generalists inducted annually during the 10 years preceding the date of the enactment of this Act.

(4) The total number of Department advisors stationed in any of the agencies or congressional offices described in subsection (a), including the agencies or offices in which such advisors serve.

(5) The total number of advisors from other United States Government agencies stationed in the Department of State (excluding defense attaches, senior defense officials, and other Department of Defense personnel stationed in United States missions abroad), the home agency of the advisor, and the offices in which such advisors serve.

TITLE IV—A DIVERSE WORKFORCE: RECRUITMENT, RETENTION, AND PROMOTION

SEC. 5401. DEFINITIONS.

In this title:

(1) APPLICANT FLOW DATA.—The term ''applicant flow data'' means data that tracks the rate of applications for job positions among demographic categories.

(2) DEMOGRAPHIC DATA.—The term ''demographic data'' means facts or statistics relating to the demographic categories specified in the Office of Management and Budget statistical policy directive entitled ''Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity'' (81 Fed. Reg. 67398).

(3) DIVERSITY.—The term ''diversity'' means those classes of persons protected under the Civil Rights Act of 1964 (42 U.S.C. 2000a et seq.) and the Americans with Disabilities Act of 1990 (42 U.S.C. 12101 et seq.).

(4) WORKFORCE.—The term ''workforce'' means—

(A) individuals serving in a position in the civil service (as defined in section 2101 of title 5, United States Code);

(B) individuals who are members of the Foreign Service (as defined in section 103 of the Foreign Service Act of 1980 (22 U.S.C. 3902));

(C) all individuals serving under a personal services contract;

(D) all individuals serving under a Foreign Service Limited appointment under section 309 of the Foreign Service Act of 1980; or

(E) individuals other than Locally Employed Staff working in the Department of State under any other authority.

SEC. 5402. EXIT INTERVIEWS FOR WORKFORCE.

(a) RETAINED MEMBERS.—The Director General of the Foreign Service and the Director of the Bureau of Human Resources or its equivalent shall conduct periodic interviews with a representative and diverse cross-section of the workforce of the Department—

(1) to understand the reasons of individuals in such workforce for remaining in a position in the Department; and

(2) to receive feedback on workplace policies, professional development opportunities, and other issues affecting the decision of individuals in the workforce to remain in the Department.

(b) DEPARTING MEMBERS.—The Director General of the Foreign Service and the Director of the Bureau of Human Resources or its equivalent shall provide an opportunity for an exit interview to each individual in the workforce of the Department who separates from service with the Department to better understand the reasons of such individual for leaving such service.

(c) USE OF ANALYSIS FROM INTERVIEWS.—The Director General of the Foreign Service and the Director of the Bureau of Human Resources or its equivalent shall analyze demographic data and other information obtained through interviews under subsections (a) and (b) to determine to what extent, if any, the diversity of those participating in such interviews impacts the results.

(d) TRACKING DATA.—The Department shall—

(1) track demographic data relating to participants in professional development programs and the rate of placement into senior positions for participants in such programs;

(2) annually evaluate such data—

(A) to identify ways to improve outreach and recruitment for such programs, consistent with merit system principles; and

(B) to understand the extent to which participation in any professional development program offered or sponsored by the Department differs among the demographic categories of the workforce; and

(3) actively encourage participation from a range of demographic categories, especially from categories with consistently low participation, in such professional development programs.

SEC. 5403. RECRUITMENT AND RETENTION.

(a) IN GENERAL.—The Secretary shall—

(1) continue to seek a diverse and talented pool of applicants; and

(2) instruct the Director General of the Foreign Service and the Director of the Bureau of Human Resources of the Department to have a recruitment plan of action for the recruitment of people belonging to traditionally under-represented groups, which should include outreach at appropriate colleges, universities, affinity groups, and professional associations.

(b) SCOPE.—The diversity recruitment initiatives described in subsection (a) shall include—

(1) recruiting at women's colleges, historically Black colleges and universities, minority-serving institutions, and other institutions serving a significant percentage of minority students;

(2) placing job advertisements in newspapers, magazines, and job sites oriented toward diverse groups;

(3) sponsoring and recruiting at job fairs in urban and rural communities and land-grant colleges or universities;

(4) providing opportunities through highly respected, international leadership programs, that focus on diversity recruitment and retention;

(5) expanding the use of paid internships; and

(6) cultivating partnerships with organizations dedicated to the advancement of the profession of international affairs and national security to advance shared diversity goals.

(c) EXPAND TRAINING ON ANTI-HARASSMENT AND ANTI-DISCRIMINATION.—

(1) IN GENERAL.—The Secretary shall, through the Foreign Service Institute and other educational and training opportunities—

(A) ensure the provision to all individuals in the workforce of training on anti-harassment and anti-discrimination information and policies, including in existing Foreign Service Institute courses or modules prioritized in the Department's Diversity and Inclusion Strategic Plan for 2016–2020 to promote diversity in Bureau awards or mitigate unconscious bias;

(B) expand the provision of training on workplace rights and responsibilities to focus on anti-harassment and anti-discrimination information and policies, including policies relating to sexual assault prevention and response; and

(C) make such expanded training mandatory for—

(i) individuals in senior and supervisory positions;

(ii) individuals having responsibilities related to recruitment, retention, or promotion of employees; and

(iii) any other individual determined by the Department who needs such training based on analysis by the Department or OPM analysis.

(2) BEST PRACTICES.—The Department shall give special attention to ensuring the continuous incorporation of research-based best practices in training provided under this subsection.

SEC. 5404. LEADERSHIP ENGAGEMENT AND ACCOUNTABILITY.

(a) REWARD AND RECOGNIZE EFFORTS TO PROMOTE DIVERSITY AND INCLUSION.—

(1) IN GENERAL.—The Secretary shall implement performance and advancement requirements that reward and recognize the efforts of individuals in senior positions and supervisors in the Department in fostering an inclusive environment and cultivating talent consistent with merit system principles, such as through participation in mentoring programs or sponsorship initiatives, recruitment events, and other similar opportunities.

(2) OUTREACH EVENTS.—The Secretary shall create opportunities for individuals in senior positions and supervisors in the Department to participate in outreach events and to discuss issues relating to diversity and inclusion with the workforce on a regular basis, including with employee resource groups.

(b) EXTERNAL ADVISORY COMMITTEES AND BOARDS.—For each external advisory committee or board to which individuals in senior positions in the Department appoint members, the Secretary is strongly encouraged by Congress to ensure such external advisory committee or board is developed, reviewed, and carried out by qualified teams that represent the diversity of the organization.

SEC. 5405. PROFESSIONAL DEVELOPMENT OPPORTUNITIES AND TOOLS.

(a) EXPAND PROVISION OF PROFESSIONAL DEVELOPMENT AND CAREER ADVANCEMENT OPPORTUNITIES.—

(1) IN GENERAL.—The Secretary is authorized to expand professional development opportunities that support the mission needs of the Department, such as—

(A) academic programs;

(B) private-public exchanges; and

(C) detail assignments to relevant positions in—

(i) private or international organizations;

(ii) State, local, and Tribal governments;

(iii) other branches of the Federal Government; or

(iv) professional schools of international affairs.

(2) TRAINING FOR SENIOR POSITIONS.—

(A) IN GENERAL.—The Secretary shall offer, or sponsor members of the workforce to participate in, a Senior Executive Service candidate development program or other program that trains members on the skills required for appointment to senior positions in the Department.

(B) REQUIREMENTS.—In determining which members of the workforce are granted professional development or career advancement opportunities under subparagraph (A), the Secretary shall—

(i) ensure any program offered or sponsored by the Department under such subparagraph comports with the requirements of subpart C of part 412 of title 5, Code of Federal Regulations, or any successor thereto, including merit staffing and assessment requirements;

(ii) consider the number of expected vacancies in senior positions as a factor in determining the number of candidates to select for such programs;

(iii) understand how participation in any program offered or sponsored by the Department under such subparagraph differs by gender, race, national origin, disability status, or other demographic categories; and

(iv) actively encourage participation from a range of demographic categories, especially from categories with consistently low participation.

SEC. 5406. EXAMINATION AND ORAL ASSESSMENT FOR THE FOREIGN SERVICE.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the Department should offer both the Foreign Service written examination and oral assessment in more locations throughout the United States. Doing so would ease the financial burden on potential candidates who do not currently reside in and must travel at their own expense to one of the few locations where these assessments are offered.

(b) FOREIGN SERVICE EXAMINATIONS.—Section 301(b) of the Foreign Service Act of 1980 (22 U.S.C. 3941) is amended—

(1) by striking ''The Secretary'' and inserting: ''(1) The Secretary''; and

(2) by adding at the end the following new paragraph:

''(2) The Secretary shall ensure that the Board of Examiners for the Foreign Service annually offers the oral assessment examinations described in paragraph (1) in cities, chosen on a rotating basis, located in at least five cities in three different time zones across the United States.''.

SEC. 5407. PAYNE FELLOWSHIP AUTHORIZATION.

(a) IN GENERAL.—Undergraduate and graduate components of the Donald M. Payne International Development Fellowship Program may conduct outreach to attract outstanding students with an interest in pursuing a Foreign Service career who represent diverse ethnic and socioeconomic backgrounds.

(b) REVIEW OF PAST PROGRAMS.—The Secretary shall review past programs designed to increase minority representation in international affairs positions.

SEC. 5408. VOLUNTARY PARTICIPATION.

(a) IN GENERAL.—Nothing in this title should be construed so as to compel any employee to participate in the collection of the data or divulge any personal information. Department employees shall be informed that their participation in the data collection contemplated by this title is voluntary.

(b) PRIVACY PROTECTION.—Any data collected under this title shall be subject to the relevant privacy protection statutes and regulations applicable to Federal employees.

TITLE V—INFORMATION SECURITY

SEC. 5501. DEFINITIONS.

In this title:

(1) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(2) RELEVANT CONGRESSIONAL COMMITTEES.—The term ''relevant congressional committees'' means—

(A) the appropriate congressional committees;

(B) the Select Committee on Intelligence of the Senate; and

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

SEC. 5502. LIST OF CERTAIN TELECOMMUNICATIONS PROVIDERS.

(a) LIST OF COVERED CONTRACTORS.—Not later than 30 days after the date of the enactment of this Act, the Secretary, in consultation with the Director of National Intelligence and other appropriate Federal agencies as determined jointly by the Secretary and the Director of National Intelligence, shall develop or maintain, as the case may be, and update as frequently as the Secretary determines appropriate, a list of covered contractors with respect to which the Department should seek to avoid entering into contracts. Not later than 30 days after the initial development of the list under this subsection, any update thereto, and annually thereafter for 5 years after such initial 30 day period, the Secretary shall submit to the appropriate congressional committees a copy of such list.

(b) COVERED CONTRACTOR DEFINED.—In this section, the term ''covered contractor'' means a provider of telecommunications, telecommunications equipment, or information technology equipment, including hardware, software, or services, that has knowingly assisted or facilitated a cyber attack or conducted surveillance, including passive or active monitoring, carried out against—

(1) the United States by, or on behalf of, any government, or persons associated with

such government, listed as a cyber threat actor in the intelligence community's 2017 assessment of worldwide threats to United States national security or any subsequent worldwide threat assessment of the intelligence community; or

(2) individuals, including activists, journalists, opposition politicians, or other individuals for the purposes of suppressing dissent or intimidating critics, on behalf of a country included in the annual country reports on human rights practices of the Department for systematic acts of political repression, including arbitrary arrest or detention, torture, extrajudicial or politically motivated killing, or other gross violations of human rights.

SEC. 5503. FOREIGN RELATIONS OF THE UNITED STATES (FRUS) SERIES AND DECLASSIFICATION.

The State Department Basic Authorities Act of 1956 is amended—

(1) in section 402(a)(2) (22 U.S.C. 4352(a)(2)), by striking ''26'' and inserting ''20''; and

(2) in section 404 (22 U.S.C. 4354)—

(A) in subsection (a)(1), by striking ''30''and inserting ''25''; and

(B) in subsection (c)(1)(C), by striking ''30'' and inserting ''25''.

TITLE VI—PUBLIC DIPLOMACY

SEC. 5601. SHORT TITLE.

This title may be cited as the ''Public Diplomacy Modernization Act of 2021''.

SEC. 5602. AVOIDING DUPLICATION OF PROGRAMS AND EFFORTS.

The Secretary shall—

(1) identify opportunities for greater efficiency of operations, including through improved coordination of efforts across public diplomacy bureaus and offices of the Department; and

(2) maximize shared use of resources between, and within, such public diplomacy bureaus and offices in cases in which programs, facilities, or administrative functions are duplicative or substantially overlapping.

SEC. 5603. IMPROVING RESEARCH AND EVALUATION OF PUBLIC DIPLOMACY.

(a) RESEARCH AND EVALUATION ACTIVITIES.—The Secretary, acting through the Director of Research and Evaluation appointed pursuant to subsection (b), shall—

(1) conduct regular research and evaluation of public diplomacy programs and activities of the Department, including through the routine use of audience research, digital analytics, and impact evaluations, to plan and execute such programs and activities; and

(2) make available to Congress the findings of the research and evaluations conducted under paragraph (1).

(b) DIRECTOR OF RESEARCH AND EVALUATION.—

(1) APPOINTMENT.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall appoint a Director of Research and Evaluation (referred to in this subsection as the ''Director'') in the Office of Policy, Planning, and Resources for Public Diplomacy and Public Affairs of the Department.

(2) LIMITATION ON APPOINTMENT.—The appointment of the Director pursuant to paragraph (1) shall not result in an increase in the overall full-time equivalent positions within the Department.

(3) RESPONSIBILITIES.—The Director shall—

(A) coordinate and oversee the research and evaluation of public diplomacy programs and activities of the Department in order to—

(i) improve public diplomacy strategies and tactics; and

(ii) ensure that such programs and activities are increasing the knowledge, understanding, and trust of the United States by relevant target audiences;

(B) routinely organize and oversee audience research, digital analytics, and impact evaluations across all public diplomacy bureaus and offices of the Department;

(C) support United States diplomatic posts' public affairs sections;

(D) share appropriate public diplomacy research and evaluation information within the Department and with other appropriate Federal departments and agencies;

(E) regularly design and coordinate standardized research questions, methodologies, and procedures to ensure that public diplomacy programs and activities across all public diplomacy bureaus and offices are designed to meet appropriate foreign policy objectives; and

(F) report biannually to the United States Advisory Commission on Public Diplomacy, through the Subcommittee on Research and Evaluation established pursuant to subsection (f), regarding the research and evaluation of all public diplomacy bureaus and offices.

(4) GUIDANCE AND TRAINING.—Not later than 1 year after the appointment of the Director pursuant to paragraph (1), the Director shall develop guidance and training, including curriculum for use by the Foreign Service Institute, for all public diplomacy officers of the Department regarding the reading and interpretation of public diplomacy program and activity evaluation findings to ensure that such findings and related lessons learned are implemented in the planning and evaluation of all public diplomacy programs and activities of the Department.

(c) PRIORITIZING RESEARCH AND EVALUATION.—

(1) IN GENERAL.—The head of the Office of Policy, Planning, and Resources for Public Diplomacy and Public Affairs of the Department shall ensure that research and evaluation of public diplomacy and activities of the Department, as coordinated and overseen by the Director pursuant to subsection (b), supports strategic planning and resource allocation across all public diplomacy bureaus and offices of the Department.

(2) ALLOCATION OF RESOURCES.—Amounts allocated for the purpose of research and evaluation of public diplomacy programs and activities of the Department pursuant to subsection (b) shall be made available to be disbursed at the direction of the Director of Research and Evaluation among the research and evaluation staff across all public diplomacy bureaus and offices of the Department.

(3) SENSE OF CONGRESS.—It is the sense of Congress that the Department should gradually increase its allocation of funds made available under the headings ''Educational and Cultural Exchange Programs'' and ''Diplomatic Programs'' for research and evaluation of public diplomacy programs and activities of the Department pursuant to subsection (b) to a percentage of program funds that is commensurate with Federal Government best practices.

(d) LIMITED EXEMPTION RELATING TO THE PAPERWORK REDUCTION ACT.—Chapter 35 of title 44, United States Code (commonly known as the ''Paperwork Reduction Act'') shall not apply to the collection of information directed at any individuals conducted by, or on behalf of, the Department of State for the purpose of audience research, monitoring, and evaluations, and in connection with the Department's activities conducted pursuant to any of the following:

(1) The Mutual Educational and Cultural Exchange Act of 1961 (22 U.S.C. 2451 et seq.).

(2) Section 1287 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 22 U.S.C. 2656 note).

(3) The Foreign Assistance Act of 1961 (22 U.S.C. 2151 et seq.).

(e) LIMITED EXEMPTION RELATING TO THE PRIVACY ACT.—

(1) IN GENERAL.—The Department shall maintain, collect, use, and disseminate records (as such term is defined in section 552a(a)(4) of title 5, United States Code) for audience research, digital analytics, and impact evaluation of communications related to public diplomacy efforts intended for foreign audiences.

(2) CONDITIONS.—Audience research, digital analytics, and impact evaluations under paragraph (1) shall be—

(A) reasonably tailored to meet the purposes of this subsection; and

(B) carried out with due regard for privacy and civil liberties guidance and oversight.

(f) UNITED STATES ADVISORY COMMISSION ON PUBLIC DIPLOMACY.—

(1) SUBCOMMITTEE FOR RESEARCH AND EVALUATION.—The United States Advisory Commission on Public Diplomacy shall establish a Subcommittee on Research and Evaluation to monitor and advise regarding audience research, digital analytics, and impact evaluations carried out by the Department and the United States Agency for Global Media.

(2) ANNUAL REPORT.—The Subcommittee on Research and Evaluation established pursuant to paragraph (1) shall submit to the appropriate congressional committees an annual report, in conjunction with the United States Advisory Commission on Public Diplomacy's Comprehensive Annual Report on the performance of the Department and the United States Agency for Global Media, describing all actions taken by the Subcommittee pursuant to paragraph (1) and any findings made as a result of such actions.

SEC. 5604. PERMANENT REAUTHORIZATION OF THE UNITED STATES ADVISORY COMMISSION ON PUBLIC DIPLOMACY.

Section 1334 of the Foreign Affairs Reform and Restructuring Act of 1998 (22 U.S.C. 6553) is amended—

(1) in the section heading, by striking ''**SUNSET**'' and inserting ''**CONTINUATION**''; and

(2) by striking ''until October 1, 2021''.

SEC. 5605. STREAMLINING OF SUPPORT FUNCTIONS.

(a) WORKING GROUP ESTABLISHED.—Not later than 60 days after the date of the enactment of this Act, the Secretary shall establish a working group to explore the possibilities and cost-benefit analysis of transitioning to a shared services model as such pertains to human resources, travel, purchasing, budgetary planning, and all other executive support functions for all bureaus of the Department that report to the Under Secretary for Public Diplomacy of the Department.

(b) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a plan to implement any such findings of the working group established under subsection (a).

SEC. 5606. GUIDANCE FOR CLOSURE OF PUBLIC DIPLOMACY FACILITIES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State shall adopt, and include in the Foreign Affairs Manual, guidelines to collect and utilize information from each diplomatic post at which the construction of a new embassy compound or new consulate compound would result in the closure or co-location of an American Space, American Center, American Corner, or any other public diplomacy facility under the Secure Embassy Construction and Counterterrorism Act of 1999 (22 U.S.C. 4865 et seq.).

(b) REQUIREMENTS.—The guidelines required by subsection (a) shall include the following:

(1) Standardized notification to each chief of mission at a diplomatic post describing the requirements of the Secure Embassy Construction and Counterterrorism Act of 1999 and the impact on the mission footprint of such requirements.

(2) An assessment and recommendations from each chief of mission of potential impacts to public diplomacy programming at such diplomatic post if any public diplomacy facility referred to in subsection (a) is closed or staff is co-located in accordance with such Act.

(3) A process by which assessments and recommendations under paragraph (2) are considered by the Secretary and the appropriate Under Secretaries and Assistant Secretaries of the Department.

(4) Notification to the appropriate congressional committees, prior to the initiation of a new embassy compound or new consulate compound design, of the intent to close any such public diplomacy facility or co-locate public diplomacy staff in accordance with such Act.

(c) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report containing the guidelines required under subsection (a) and any recommendations for any modifications to such guidelines.

SEC. 5607. DEFINITIONS.

In this title:

(1) AUDIENCE RESEARCH.—The term ''audience research'' means research conducted at the outset of a public diplomacy program or the outset of campaign planning and design regarding specific audience segments to understand the attitudes, interests, knowledge, and behaviors of such audience segments.

(2) DIGITAL ANALYTICS.—The term ''digital analytics'' means the analysis of qualitative and quantitative data, accumulated in digital format, to indicate the outputs and outcomes of a public diplomacy program or campaign.

(3) IMPACT EVALUATION.—The term ''impact evaluation'' means an assessment of the changes in the audience targeted by a public diplomacy program or campaign that can be attributed to such program or campaign.

(4) PUBLIC DIPLOMACY BUREAUS AND OFFICES.—The term ''public diplomacy bureaus and offices'' means, with respect to the Department, the following:

(A) The Bureau of Educational and Cultural Affairs.

(B) The Bureau of Global Public Affairs.

(C) The Office of Policy, Planning, and Resources for Public Diplomacy and Public Affairs.

(D) The Global Engagement Center.

(E) The public diplomacy functions within the regional and functional bureaus.

TITLE VII—COMBATING PUBLIC CORRUPTION

SEC. 5701. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) it is in the foreign policy interest of the United States to help foreign countries promote good governance and combat public corruption;

(2) multiple Federal departments and agencies operate programs that promote good governance in foreign countries and enhance such countries' ability to combat public corruption; and

(3) the Department of State should—

(A) promote coordination among the Federal departments and agencies implementing programs to promote good governance and combat public corruption in foreign countries in order to improve effectiveness and efficiency; and

(B) identify areas in which United States efforts to help other countries promote good governance and combat public corruption could be enhanced.

SEC. 5702. DEFINITIONS.

In this title:

(1) CORRUPT ACTOR.—The term ''corrupt actor'' means—

(A) any foreign person or entity that is a government official or government entity responsible for, or complicit in, an act of corruption; and

(B) any company, in which a person or entity described in subparagraph (A) has a significant stake, which is responsible for, or complicit in, an act of corruption.

(2) CORRUPTION.—The term ''corruption'' means the unlawful exercise of entrusted public power for private gain, including by bribery, nepotism, fraud, or embezzlement.

(3) SIGNIFICANT CORRUPTION.—The term ''significant corruption'' means corruption committed at a high level of government that has some or all of the following characteristics:

(A) Illegitimately distorts major decision-making, such as policy or resource determinations, or other fundamental functions of governance.

(B) Involves economically or socially large-scale government activities.

SEC. 5703. PUBLICATION OF TIERED RANKING LIST.

(a) IN GENERAL.—The Secretary of State shall annually publish, on a publicly accessible website, a tiered ranking of all foreign countries.

(b) TIER 1 COUNTRIES.—A country shall be ranked as a tier 1 country in the ranking published under subsection (a) if the government of such country is complying with the minimum standards set forth in section 5704.

(c) TIER 2 COUNTRIES.—A country shall be ranked as a tier 2 country in the ranking published under subsection (a) if the government of such country is making efforts to comply with the minimum standards set forth in section 5704, but is not achieving the requisite level of compliance to be ranked as a tier 1 country.

(d) TIER 3 COUNTRIES.—A country shall be ranked as a tier 3 country in the ranking published under subsection (a) if the government of such country is making de minimis or no efforts to comply with the minimum standards set forth in section 5704.

SEC. 5704. MINIMUM STANDARDS FOR THE ELIMINATION OF CORRUPTION AND ASSESSMENT OF EFFORTS TO COMBAT CORRUPTION.

(a) IN GENERAL.—The government of a country is complying with the minimum standards for the elimination of corruption if the government—

(1) has enacted and implemented laws and established government structures, policies, and practices that prohibit corruption, including significant corruption;

(2) enforces the laws described in paragraph (1) by punishing any person who is found, through a fair judicial process, to have violated such laws;

(3) prescribes punishment for significant corruption that is commensurate with the punishment prescribed for serious crimes; and

(4) is making serious and sustained efforts to address corruption, including through prevention.

(b) FACTORS FOR ASSESSING GOVERNMENT EFFORTS TO COMBAT CORRUPTION.—In determining whether a government is making serious and sustained efforts to address corruption, the Secretary of State shall consider, to the extent relevant or appropriate, factors such as—

(1) whether the government of the country has criminalized corruption, investigates and prosecutes acts of corruption, and convicts and sentences persons responsible for such acts over which it has jurisdiction, including, as appropriate, incarcerating individuals convicted of such acts;

(2) whether the government of the country vigorously investigates, prosecutes, convicts, and sentences public officials who participate in or facilitate corruption, including nationals of the country who are deployed in foreign military assignments, trade delegations abroad, or other similar missions, who engage in or facilitate significant corruption;

(3) whether the government of the country has adopted measures to prevent corruption, such as measures to inform and educate the public, including potential victims, about the causes and consequences of corruption;

(4) what steps the government of the country has taken to prohibit government officials from participating in, facilitating, or condoning corruption, including the investigation, prosecution, and conviction of such officials;

(5) the extent to which the country provides access, or, as appropriate, makes adequate resources available, to civil society organizations and other institutions to combat corruption, including reporting, investigating, and monitoring;

(6) whether an independent judiciary or judicial body in the country is responsible for, and effectively capable of, deciding corruption cases impartially, on the basis of facts and in accordance with the law, without any improper restrictions, influences, inducements, pressures, threats, or interferences (direct or indirect);

(7) whether the government of the country is assisting in international investigations of transnational corruption networks and in other cooperative efforts to combat significant corruption, including, as appropriate, cooperating with the governments of other countries to extradite corrupt actors;

(8) whether the government of the country recognizes the rights of victims of corruption, ensures their access to justice, and takes steps to prevent victims from being further victimized or persecuted by corrupt actors, government officials, or others;

(9) whether the government of the country protects victims of corruption or whistleblowers from reprisal due to such persons having assisted in exposing corruption, and refrains from other discriminatory treatment of such persons;

(10) whether the government of the country is willing and able to recover and, as appropriate, return the proceeds of corruption;

(11) whether the government of the country is taking steps to implement financial transparency measures in line with the Financial Action Task Force recommendations, including due diligence and beneficial ownership transparency requirements;

(12) whether the government of the country is facilitating corruption in other countries in connection with state-directed investment, loans or grants for major infrastructure, or other initiatives; and

(13) such other information relating to corruption as the Secretary of State considers appropriate.

(c) ASSESSING GOVERNMENT EFFORTS TO COMBAT CORRUPTION IN RELATION TO RELEVANT INTERNATIONAL COMMITMENTS.—In determining whether a government is making serious and sustained efforts to address corruption, the Secretary of State shall consider the government of a country's compliance with the following, as relevant:

(1) The Inter-American Convention against Corruption of the Organization of American States, done at Caracas March 29, 1996.

(2) The Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of the Organisation of

Economic Co-operation and Development, done at Paris December 21, 1997 (commonly referred to as the ''Anti-Bribery Convention'').

(3) The United Nations Convention against Transnational Organized Crime, done at New York November 15, 2000.

(4) The United Nations Convention against Corruption, done at New York October 31, 2003.

(5) Such other treaties, agreements, and international standards as the Secretary of State considers appropriate.

SEC. 5705. IMPOSITION OF SANCTIONS UNDER GLOBAL MAGNITSKY HUMAN RIGHTS ACCOUNTABILITY ACT.

(a) IN GENERAL.—The Secretary of State, in coordination with the Secretary of the Treasury, should evaluate whether there are foreign persons engaged in significant corruption for the purposes of potential imposition of sanctions under the Global Magnitsky Human Rights Accountability Act (subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note)—

(1) in all countries identified as tier 3 countries under section 5703; or

(2) in relation to the planning or construction or any operation of the Nord Stream 2 pipeline.

(b) REPORT REQUIRED.—Not later than 180 days after publishing the list required by section 5703(a) and annually thereafter, the Secretary of State shall submit to the committees specified in subsection (f) a report that includes—

(1) a list of foreign persons with respect to which the President imposed sanctions pursuant to the evaluation under subsection (a);

(2) the dates on which such sanctions were imposed;

(3) the reasons for imposing such sanctions; and

(4) a list of all foreign persons found to have been engaged in significant corruption in relation to the planning, construction, or operation of the Nord Stream 2 pipeline.

(c) FORM OF REPORT.—Each report required by subsection (b) shall be submitted in unclassified form but may include a classified annex.

(d) BRIEFING IN LIEU OF REPORT.—The Secretary of State, in coordination with the Secretary of the Treasury, may (except with respect to the list required by subsection (b)(4)) provide a briefing to the committees specified in subsection (f) instead of submitting a written report required under subsection (b), if doing so would better serve existing United States anti-corruption efforts or the national interests of the Untied States.

(e) TERMINATION OF REQUIREMENTS RELATING TO NORD STREAM 2.—The requirements under subsections (a)(2) and (b)(4) shall terminate on the date that is 5 years after the date of the enactment of this Act.

(f) COMMITTEES SPECIFIED.—The committees specified in this subsection are—

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

(2) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Financial Services, and the Committee on the Judiciary of the House of Representatives.

SEC. 5706. DESIGNATION OF EMBASSY ANTI-CORRUPTION POINTS OF CONTACT.

(a) IN GENERAL.—The Secretary of State shall annually designate an anti-corruption point of contact at the United States diplomatic post to each country identified as tier 2 or tier 3 under section 5703, or which the Secretary otherwise determines is in need of such a point of contact. The point of contact shall be the chief of mission or the chief of mission's designee.

(b) RESPONSIBILITIES.—Each anti-corruption point of contact designated under subsection (a) shall be responsible for enhancing coordination and promoting the implementation of a whole-of-government approach among the relevant Federal departments and agencies undertaking efforts to—

(1) promote good governance in foreign countries; and

(2) enhance the ability of such countries—

(A) to combat public corruption; and

(B) to develop and implement corruption risk assessment tools and mitigation strategies.

(c) TRAINING.—The Secretary of State shall implement appropriate training for anti-corruption points of contact designated under subsection (a).

TITLE VIII—GLOBAL MAGNITSKY HUMAN RIGHTS ACCOUNTABILITY REAUTHORIZATION ACT

SEC. 5801. SHORT TITLE.

This title may be cited as the ''Global Magnitsky Human Rights Accountability Reauthorization Act''.

SEC. 5802. MODIFICATIONS TO AND REAUTHORIZATION OF SANCTIONS WITH RESPECT TO HUMAN RIGHTS VIOLATIONS.

(a) DEFINITIONS.—Section 1262 of the Global Magnitsky Human Rights Accountability Act (Subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note) is amended by striking paragraph (2) and inserting the following:

''(2) IMMEDIATE FAMILY MEMBER.—The term 'immediate family member', with respect to a foreign person, means the spouse, parent, sibling, or adult child of the person.''.

(b) SENSE OF CONGRESS.—The Global Magnitsky Human Rights Accountability Act (Subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note) is amended by inserting after section 1262 the following new section:

''SEC. 1262A. SENSE OF CONGRESS.

''It is the sense of Congress that the President should establish and regularize information sharing and sanctions-related decision making with like-minded governments possessing human rights and anti-corruption sanctions programs similar in nature to those authorized under this subtitle.''.

(c) IMPOSITION OF SANCTIONS.—

(1) IN GENERAL.—Subsection (a) of section 1263 of the Global Magnitsky Human Rights Accountability Act (Subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note) is amended to read as follows:

''(a) IN GENERAL.—The President may impose the sanctions described in subsection (b) with respect to—

''(1) any foreign person that the President determines, based on credible information—

''(A) is responsible for or complicit in, or has directly or indirectly engaged in, serious human rights abuse;

''(B) is a current or former government official, or a person acting for or on behalf of such an official, who is responsible for or complicit in, or has directly or indirectly engaged in—

''(i) corruption, including—

''(I) the misappropriation of state assets;

''(II) the expropriation of private assets for personal gain;

''(III) corruption related to government contracts or the extraction of natural resources; or

''(IV) bribery; or

''(ii) the transfer or facilitation of the transfer of the proceeds of corruption;

''(C) is or has been a leader or official of—

''(i) an entity, including a government entity, that has engaged in, or whose members have engaged in, any of the activities described in subparagraph (A) or (B) related to the tenure of the leader or official; or

''(ii) an entity whose property and interests in property are blocked pursuant to this section as a result of activities related to the tenure of the leader or official;

''(D) has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of—

''(i) an activity described in subparagraph (A) or (B) that is conducted by a foreign person;

''(ii) a person whose property and interests in property are blocked pursuant to this section; or

''(iii) an entity, including a government entity, that has engaged in, or whose members have engaged in, an activity described in subparagraph (A) or (B) conducted by a foreign person; or

''(E) is owned or controlled by, or has acted or been purported to act for or on behalf of, directly or indirectly, a person whose property and interests in property are blocked pursuant to this section; and

''(2) any immediate family member of a person described in paragraph (1).''.

(2) CONSIDERATION OF CERTAIN INFORMATION.—Subsection (c)(2) of such section is amended by inserting ''corruption and'' after ''monitor''.

(3) REQUESTS BY CONGRESS.—Subsection (d) of such section is amended—

(A) in paragraph (1)—

(i) in the matter preceding subparagraph (A), by striking ''subsection (a)'' and inserting ''subsection (a)(1)''; and

(ii) in subparagraph (B)(i), by inserting ''or an immediate family member of the person''; and

(B) in paragraph (2)—

(i) in subparagraph (A)—

(I) in the subparagraph heading, by striking ''HUMAN RIGHTS VIOLATIONS'' and inserting ''SERIOUS HUMAN RIGHTS ABUSE''; and

(II) by striking ''described in paragraph (1) or (2) of subsection (a)'' and inserting ''described in subsection (a)(1) relating to serious human rights abuse''; and

(ii) in subparagraph (B)—

(I) in the matter preceding clause (i), by striking ''described in paragraph (3) or (4) of subsection (a)'' and inserting ''described in subsection (a)(1) relating to corruption or the transfer or facilitation of the transfer of the proceeds of corruption''; and

(II) by striking ''ranking member of'' and all that follows through the period at the end and inserting ''ranking member of one of the appropriate congressional committees''.

(4) TERMINATION OF SANCTIONS.—Subsection (g) of such section is amended, in the matter preceding paragraph (1), by inserting ''and the immediate family members of that person'' after ''a person''.

(d) REPORTS TO CONGRESS.—Section 1264(a) of the Global Magnitsky Human Rights Accountability Act (Subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note) is amended—

(1) in paragraph (5), by striking ''; and'' and inserting a semicolon;

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

(3) by adding at the end the following:

''(7) A description of additional steps taken by the President through diplomacy, international engagement, and assistance to foreign or security sectors to address persistent underlying causes of serious human rights abuse and corruption in each country in which foreign persons with respect to which sanctions have been imposed under section 1263 are located.''.

(e) REPEAL OF SUNSET.—Section 1265 of the Global Magnitsky Human Rights Accountability Act (Subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note) is repealed.

TITLE IX—OTHER MATTERS

SEC. 5901. LIMITATION ON ASSISTANCE TO COUNTRIES IN DEFAULT.

Section 620(q) of the Foreign Assistance Act of 1961 (22 U.S.C. 2370(q)) is amended—

(1) by striking ''No assistance'' and inserting the following:

''(1) No assistance'';

(2) by inserting ''the government of'' before ''any country'';

(3) by inserting ''the government of'' before ''such country'' each place it appears;

(4) by striking ''determines'' and all that follows and inserting ''determines, after consultation with the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives and the Committee on Foreign Relations and the Committee on Appropriations of the Senate, that assistance for such country is in the national interest of the United States.''; and

(5) by adding at the end the following new paragraph:

''(2) No assistance shall be furnished under this Act, the Peace Corps Act, the Millennium Challenge Act of 2003, the African Development Foundation Act, the BUILD Act of 2018, section 504 of the FREEDOM Support Act, or section 23 of the Arms Export Control Act to the government of any country which is in default during a period in excess of 1 calendar year in payment to the United States of principal or interest or any loan made to the government of such country by the United States unless the President determines, following consultation with the congressional committees specified in paragraph (1), that assistance for such country is in the national interest of the United States.''.

SEC. 5902. SEAN AND DAVID GOLDMAN CHILD ABDUCTION PREVENTION AND RETURN ACT OF 2014 AMENDMENT.

Subsection (b) of section 101 of the Sean and David Goldman International Child Abduction Prevention and Return Act of 2014 (22 U.S.C. 9111; Public Law 113–150) is amended—

(1) in paragraph (2)—

(A) in subparagraph (A)—

(i) by inserting '', respectively,'' after ''access cases''; and

(ii) by inserting ''and the number of children involved'' before the semicolon at the end; and

(B) in subparagraph (D), by inserting ''respectively, the number of children involved,'' after ''access cases,'';

(2) in paragraph (7), by inserting '', and number of children involved in such cases'' before the semicolon at the end;

(3) in paragraph (8), by striking ''and'' after the semicolon at the end;

(4) in paragraph (9), by striking the period at the end and inserting ''; and''; and

(5) by adding at the end the following new paragraph:

''(10) the total number of pending cases the Department of State has assigned to case officers and number of children involved for each country and as a total for all countries.''.

SEC. 5903. CONGRESSIONAL OVERSIGHT, QUARTERLY REVIEW, AND AUTHORITY RELATING TO CONCURRENCE PROVIDED BY CHIEFS OF MISSION FOR THE PROVISION OF SUPPORT RELATING TO CERTAIN UNITED STATES GOVERNMENT OPERATIONS.

(a) NOTIFICATION REQUIRED.—Not later than 30 days after the date on which a chief of mission provides concurrence for the provision of United States Government support to entities or individuals engaged in facilitating or supporting United States Government operations within the area of responsibility of the chief of mission, the Secretary of State shall notify the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives of the provision of such concurrence.

(b) QUARTERLY REVIEW, DETERMINATION, AND BRIEFING REQUIRED.—Not less frequently than every 90 days, the Secretary of State shall, in order to ensure support described in subsection (a) continues to align with United States foreign policy objectives and the objectives of the Department of State—

(1) conduct a review of any concurrence described in subsection (a) in effect as of the date of the review;

(2) based on the review, determine whether to revoke any such concurrence pending further study and review; and

(3) brief the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives on the results of the review.

(c) REVOCATION OF CONCURRENCE.—Based on the review conducted pursuant to subsection (b), the Secretary may revoke any such concurrence.

(d) ANNUAL REPORT REQUIRED.—Not later than January 31 of each year, the Secretary of State shall submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report that includes the following:

(1) A description of any support described in subsection (a) that was provided with the concurrence of a chief of mission during the calendar year preceding the calendar year in which the report is submitted.

(2) An analysis of the effects of the support described in paragraph (1) on diplomatic lines of effort, including with respect to—

(A) Nonproliferation, Anti-terrorism, Demining, and Related Programs (NADR) and associated Anti-Terrorism Assistance (ATA) programs;

(B) International Narcotics Control and Law Enforcement (INCLE) programs; and

(C) Foreign Military Sales (FMS), Foreign Military Financing (FMF), and associated training programs.

SEC. 5904. REPORT ON EFFORTS OF THE CORONAVIRUS REPATRIATION TASK FORCE.

Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall submit to the appropriate congressional committees, the Committee on Armed Services of the House of Representatives, and the Committee on Armed Services of the Senate a report evaluating the efforts of the Coronavirus Repatriation Task Force of the Department of State to repatriate United States citizens and legal permanent residents in response to the 2020 coronavirus outbreak. The report shall identify—

(1) the most significant impediments to repatriating such persons;

(2) the lessons learned from such repatriations; and

(3) any changes planned to future repatriation efforts of the Department of State to incorporate such lessons learned.

SA 4731. Mr. THUNE submitted an amendment intended to be proposed by him 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:

SEC. _____. DEVELOPMENT AND TESTING OF DYNAMIC SCHEDULING AND MANAGEMENT OF SPECIAL ACTIVITY AIRSPACE.

(a) SENSE OF CONGRESS ON SPECIAL ACTIVITY AIRSPACE SCHEDULING AND MANAGEMENT.—It is the sense of Congress that—

(1) where it does not conflict with safety, dynamic scheduling and management of special activity airspace (also referred to as ''dynamic airspace'') is expected to optimize the use of the national airspace system for all stakeholders; and

(2) the Administrator of the Federal Aviation Administration and the Secretary of Defense should take such actions as may be necessary to support ongoing efforts to develop dynamic scheduling and management of special activity airspace, including—

(A) the continuation of formal partnerships between the Federal Aviation Administration and the Department of Defense that focus on special activity airspace, future airspace needs, and joint solutions; and

(B) maturing research within their federally funded research and development centers, Federal partner agencies, and the aviation community.

(b) PILOT PROGRAM.—

(1) PILOT PROGRAM REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Federal Aviation Administration, in coordination with the Secretary of Defense, shall establish a pilot program on developing and testing dynamic management of special activity airspace in order to accommodate emerging military training requirements through flexible scheduling, along with increasing access to existing special activity airspace used by the Department of Defense for test and training.

(2) TESTING OF SPECIAL ACTIVITY AIRSPACE SCHEDULING AND MANAGEMENT.—Under the pilot program established under paragraph (1), the Administrator and the Secretary shall jointly test not fewer than three areas of episodic or permanent special activity airspace designated by the Federal Aviation Administration for use by the Department of Defense, of which—

(A) at least one shall be over coastal waters of the United States;

(B) at least two shall be over land of the United States;

(C) access to airspace available for test and training is increased to accommodate dynamic scheduling of existing airspace to more efficiently and realistically provide test and training capabilities to Department of Defense aircrews; and

(D) any increase in access to airspace made available for test and training shall not conflict with the safe management of the national airspace system or the safety of all stakeholders of the national airspace system.

(c) REPORT BY THE ADMINISTRATOR.—

(1) IN GENERAL.—Not less than two years after the date of the establishment of the pilot program under subsection (b)(1), the Administrator shall submit to the appropriate committees of Congress a report on the interim findings of the Administrator with respect to the pilot program.

(2) ELEMENTS.—The report submitted under paragraph (1) shall include the following:

(A) An analysis of how the pilot program established under subsection (b)(1) affected access to special activity airspace by nonmilitary users of the national airspace system.

(B) An analysis of whether the dynamic management of special activity airspace conducted for the pilot program established under subsection (b)(1) contributed to more

efficient use of the national airspace system by all stakeholders.

(d) REPORT BY THE SECRETARY.—Not less than two years after the date of the establishment of the pilot program under subsection (b)(1), the Secretary shall submit to the appropriate committees of Congress a report on the interim findings of the Secretary with respect to the pilot program. Such report shall include an analysis of how the pilot program affected military test and training.

(e) DEFINITIONS.—In this section:

(1) The term ''appropriate committees of Congress'' means—

(A) the Committee on Commerce, Science, and Transportation and the Committee on Armed Services of the Senate; and

(B) the Committee on Transportation and Infrastructure, the Committee on Science, Space, and Technology, and the Committee on Armed Services of the House of Representatives.

(2) The term ''special activity airspace'' means the following airspace with defined dimensions within the National Airspace System wherein limitations may be imposed upon aircraft operations:

(A) Restricted areas.

(B) Military operations areas.

(C) Air Traffic Control assigned airspace.

(D) Warning areas.

SA 4732. Mr. REED 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. _____. CYBERSECURITY TRANSPARENCY.

The Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.) is amended by inserting after section 14B (15 U.S.C. 78n–2) the following:

''SEC. 14C. CYBERSECURITY TRANSPARENCY.

''(a) DEFINITIONS.—In this section—

''(1) the term 'cybersecurity' means any action, step, or measure to detect, prevent, deter, mitigate, or address any cybersecurity threat or any potential cybersecurity threat;

''(2) the term 'cybersecurity threat'—

''(A) 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; and

''(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

''(3) the term 'information system'—

''(A) has the meaning given the term in section 3502 of title 44, United States Code; and

''(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers;

''(4) the term 'NIST' means the National Institute of Standards and Technology; and

''(5) the term 'reporting company' means any company that is an issuer—

''(A) the securities of which are registered under section 12; or

''(B) that is required to file reports under section 15(d).

''(b) REQUIREMENT TO ISSUE RULES.—Not later than 360 days after the date of enactment of this section, the Commission shall issue final rules to require each reporting company, in the annual report of the reporting company submitted under section 13 or section 15(d) or in the annual proxy statement of the reporting company submitted under section 14(a)—

''(1) to disclose whether any member of the governing body, such as the board of directors or general partner, of the reporting company has expertise or experience in cybersecurity and in such detail as necessary to fully describe the nature of the expertise or experience; and

''(2) if no member of the governing body of the reporting company has expertise or experience in cybersecurity, to describe what other aspects of the reporting company's cybersecurity were taken into account by any person, such as an official serving on a nominating committee, that is responsible for identifying and evaluating nominees for membership to the governing body.

''(c) CYBERSECURITY EXPERTISE OR EXPERIENCE.—For purposes of subsection (b), the Commission, in consultation with NIST, shall define what constitutes expertise or experience in cybersecurity using commonly defined roles, specialties, knowledge, skills, and abilities, such as those provided in NIST Special Publication 800–181, entitled 'National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework', or any successor thereto.''.

AUTHORITY FOR COMMITTEES TO MEET

Mrs. MURRAY. Mr. President, I have 5 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:

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Committee on Energy and Natural Resources is authorized to meet during the session of the Senate on Tuesday, November 16, 2021, at 10:00 a.m., to conduct a hearing.

COMMITTEE ON ENERGY AND NATURAL RESOURCES

The Committee on Energy and Natural Resources is authorized to meet during the session of the Senate on Tuesday, November 16, 2021, at 10:00 a.m., to conduct a business meeting.

COMMITTEE ON FINANCE

The Committee on Finance is authorized to meet during the session of the Senate on Tuesday, November 16, 2021, at 10:15 a.m., to conduct a hearing on nominations.

COMMITTEE ON THE JUDICIARY

The Committee on the Judiciary is authorized to meet during the session of the Senate on Tuesday, November 16, 2021, at 10:00 a.m., to conduct a hearing.

SELECT COMMITTEE ON INTELLIGENCE

The Select Committee on Intelligence is authorized to meet during the session of the Senate on Tuesday, November 16, 2021, at 2:30 p.m., to conduct a closed briefing.

U.S. SUPREME COURT

Mr. WHITEHOUSE. Mr. President, I rise today for now the ninth time to unmask the rightwing, dark money scheme to capture our Supreme Court. I say ''capture'' in the sense of regulatory capture, an Agency capture—a well-known phenomenon.

Today, I turn to an important tool of the scheme's apparatus: the orchestrated amicus curiae brief.

So, first things first, amicus—or friend of the court—briefs are an important instrument in our judicial system. They help those who aren't parties to a case to share their expertise, insight, or advocacy with the Court. I file them myself. ''Friend of the court'' briefs are necessary and useful, usually.

However, in recent years, the Court has had a lot more friends than it used to. Amici filed 781 briefs in the 2014 Supreme Court term—a more than 800-percent increase from the 1950s and a 95-percent increase just from 1995. In the 2010 term, 715 amicus briefs were filed in 78 cases. By 2019, that number had swelled to 911 briefs in just 57 cases. The average number of briefs per argued case almost doubled—from 9 in 2010 to 16 in 2019.

There is another odd feature to this uptick of amicus briefs. Most of the time, you file an amicus brief when the Justices have taken a case and are poised to actually decide the outcome of that case, at the so-called merits stage of the case, which makes sense because this is when the rulings actually become law. But these days, more and more amici arrive when the Court considers whether to take up the case, when the Justices are deciding whether to grant certiorari, or cert. Between 1982 and 2014, the percentage of petitions with at least one cert-stage amicus more than doubled.

Justices pay attention to amicus briefs. The Court cited amicus briefs 606 times in 417 opinions from 2008 to 2013—far more than in the past. These briefs don't always add value, and top appellate judges are beginning to sound that alarm.

Seventh Circuit Judge Michael Scudder said in 2020: ''Too many amicus briefs do not even pretend to offer value and instead merely repeat . . . a party's position'' and ''serve only as a show of hands on what interest groups are rooting for what outcome.''

OK. So what does this have to do with the scheme?

Well, what happens if the Justices whom dark money forces ushered onto the Court are looking for that show of hands?

I doubt it is just a coincidence that the rightwing donor machine that set out to capture the Court has also kicked into gear flotillas of amici that