(ii) by striking ''subsection (a)'' and inserting ''this subsection''; and

(E) by adding at the end the following:

''(5) GRANTS.—Subject to the availability of appropriations, the Maritime Administrator, may establish and carry out a competitive grant program to award grants to eligible entities for projects in the United States consistent with the goals of this subsection to study, evaluate, test, demonstrate, or apply technologies and practices to improve environmental performance.'';

(8) in subsection (b), as redesignated by paragraph (5) of this section, by striking ''subsection (b)(1)'' and inserting ''this section''; and

(9) by adding at the end the following:

''(c) VESSELS.—Activities carried out under a grant or cooperative agreement made under this section may be conducted on public vessels under the control of the Maritime Administration, upon approval of the Maritime Administrator.

''(d) ELIGIBLE ENTITY DEFINED.—In this section, the term 'eligible entity' means—

''(1) a private entity, including a nonprofit organization;

''(2) a State, regional, local, or Tribal government or entity, including special districts;

''(3) an institution of higher education as defined under section 102 of the Higher Education Act of 1965 (? 20 U.S.C. 1002); or

''(4) a partnership or collaboration of entities described in paragraphs (1) through (3).

''(e) CENTER FOR MARITIME INNOVATION.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Maritime Administration Authorization Act for Fiscal Year 2023, the Secretary of Transportation shall, through a cooperative agreement, establish a United States Center for Maritime Innovation (referred to in this subsection as the 'Center') to support the study, research, development, assessment, and deployment of emerging marine technologies and practices related to the maritime transportation system.

''(2) SELECTION.—The Center shall be—

''(A) selected through a competitive process of eligible entities;

''(B) based in the United States with technical expertise in emerging marine technologies and practices related to the maritime transportation system; and

''(C) located in close proximity to eligible entities with expertise in United States emerging marine technologies and practices, including the use of alternative fuels and the development of both vessel and shoreside infrastructure.

''(3) COORDINATION.—The Secretary of Transportation shall coordinate with other agencies critical for science, research, and regulation of emerging marine technologies for the maritime sector, including the Department of Energy, the Environmental Protection Agency, the National Science Foundation, and the Coast Guard, when establishing the Center.

''(4) FUNCTIONS.—The Center shall—

''(A) support eligible entities regarding the development and use of clean energy and necessary infrastructure to support the deployment of clean energy on vessels of the United States;

''(B) monitor and assess, on an ongoing basis, the current state of knowledge regarding emerging marine technologies in the United States;

''(C) identify any significant gaps in emerging marine technologies research specific to the United States maritime industry, and seek to fill those gaps;

''(D) conduct research, development, testing, and evaluation for equipment, technologies, and techniques to address the components under subsection (a)(2);

''(E) provide—

''(i) guidance on best available technologies;

''(ii) technical analysis;

''(iii) assistance with understanding complex regulatory requirements; and

''(iv) documentation of best practices in the maritime industry, including training and informational webinars on solutions for the maritime industry; and

''(F) work with academic and private sector response training centers and Domestic Maritime Workforce Training and Education Centers of Excellence to develop maritime strategies applicable to various segments of the United States maritime industry, including the inland, deep water, and coastal fleets.''.

SEC. 3542. QUIETING FEDERAL NON-COMBATIVE VESSELS.

(a) IN GENERAL.—The Secretary of Defense, in consultation with the Administrator of the National Oceanic and Atmospheric Administration, the Administrator of the Maritime Administration, and the Secretary of the department in which the Coast Guard is operating, shall, not later than 18 months after the date of enactment of this section, submit a report to the committees identified under subsection (b) and publish an unclassified report—

(1) identifying existing, at the time of submission, non-classified naval technologies that reduce underwater noise; and

(2) evaluating the effectiveness and feasibility of incorporating such technologies in the design, procurement, and construction of non-combatant vessels of the United States.

(b) COMMITTEES.—The report under subsection (a) shall be submitted the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives.

SEC. 3543. STUDY ON STORMWATER IMPACTS ON SALMON.

(a) IN GENERAL.—Not later than 90 days after the date of enactment of this section, the Administrator of the National Oceanic and Atmospheric Administration, in concert with the Secretary of Transportation and the Administrator of the Environmental Protection Agency, shall commence a study that—

(1) examines the existing science on tire-related chemicals in stormwater runoff at ports and associated transportation infrastructure and the impacts of such chemicals on Pacific salmon and steelhead;

(2) examines the challenges of studying tire-related chemicals in stormwater runoff at ports and associated transportation infrastructure and the impacts of such chemicals on Pacific salmon and steelhead;

(3) provides recommendations for improving monitoring of stormwater and research related to run-off for tire-related chemicals and the impacts of such chemicals on Pacific salmon and steelhead at ports and associated transportation infrastructure near ports; and

(4) provides recommendations based on the best available science on relevant management approaches at ports and associated transportation infrastructure under their respective jurisdictions.

(b) SUBMISSION OF STUDY.—Not later than 18 months after commencing the study under subsection (a), the Administrator of the National Oceanic and Atmospheric Administration, in concert with the Secretary of Transportation and the Administrator of the Environmental Protection Agency, shall—

(1) submit the study to the Committee on and Environment and Public Works Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives, including detailing any findings from the study; and

(2) make such study publicly available.

SEC. 3544. STUDY TO EVALUATE EFFECTIVE VESSEL QUIETING MEASURES.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this title, the Administrator of the Maritime Administration, in consultation with the Under Secretary of Commerce for Oceans and Atmosphere and the Secretary of the Department in which the Coast Guard is operating, shall submit to the committees identified under subsection (b), and make publicly available on the website of the Department of Transportation, a report that includes, at a minimum—

(1) a review of technology-based controls and best management practices for reducing vessel-generated underwater noise; and

(2) for each technology-based control and best management practice identified, an evaluation of—

(A) the applicability of each measure to various vessel types;

(B) the technical feasibility and economic achievability of each measure; and

(C) the co-benefits and trade-offs of each measure.

(b) COMMITTEES.—The report under subsection (a) shall be submitted to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives.

SA 6438. Mr. PETERS (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS MATTERS

SEC. 5001. TABLE OF CONTENTS.

The table of contents for this division is as follows:

DIVISION E—HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS MATTERS

Sec. 5001. Table of contents.

TITLE LI—HOMELAND SECURITY

Subtitle A—Global Catastrophic Risk Management Act of 2022

Sec. 5101. Short title.
Sec. 5102. Definitions.
Sec. 5103. Interagency committee on global catastrophic risk.
Sec. 5104. Report required.
Sec. 5105. Report on continuity of operations and continuity of government planning.
Sec. 5106. Enhanced catastrophic incident annex.
Sec. 5107. Validation of the strategy through an exercise.
Sec. 5108. Recommendations.
Sec. 5109. Reporting requirements.
Sec. 5110. Rule of construction.

Subtitle B—DHS Trade and Economic Security Council

Sec. 5111. DHS Trade and Economic Security Council.

Subtitle C—Transnational Criminal Investigative Units

Sec. 5121. Short title.

Sec. 5122. Stipends for Transnational Criminal Investigative Units.
Subtitle D—Technological Hazards Preparedness and Training
Sec. 5131. Short title.
Sec. 5132. Definitions.
Sec. 5133. Assistance and Training for Communities with Technological Hazards and Related Emerging Threats.
Sec. 5134. Authorization of Appropriations.
Sec. 5135. Savings provision.
Subtitle E—Offices of Countering Weapons of Mass Destruction and Health Security
Sec. 5141. Short title.
CHAPTER 1—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE
Sec. 5142. Countering Weapons of Mass Destruction Office.
Sec. 5143. Rule of construction.
CHAPTER 2—OFFICE OF HEALTH SECURITY
Sec. 5144. Office of Health Security.
Sec. 5145. Medical countermeasures program.
Sec. 5146. Confidentiality of medical quality assurance records.
Sec. 5147. Portability of licensure.
Sec. 5148. Technical and conforming amendments.
Subtitle F—Satellite Cybersecurity Act
Sec. 5151. Short title.
Sec. 5152. Definitions.
Sec. 5153. Report on commercial satellite cybersecurity.
Sec. 5154. Responsibilities of the cybersecurity and infrastructure security agency.
Sec. 5155. Strategy.
Sec. 5156. Rules of construction.
Subtitle G—Pray Safe Act
Sec. 5161. Short title.
Sec. 5162. Definitions.
Sec. 5163. Federal Clearinghouse on Safety and Security Best Practices for Faith-Based Organizations and Houses of Worship.
Sec. 5164. Notification of Clearinghouse.
Sec. 5165. Grant program overview.
Sec. 5166. Other resources.
Sec. 5167. Rule of construction.
Sec. 5168. Exemption.
Subtitle H—Invent Here, Make Here for Homeland Security Act
Sec. 5171. Short title.
Sec. 5172. Preference for United States industry.
Subtitle I—DHS Joint Task Forces Reauthorization
Sec. 5181. Short title.
Sec. 5182. Sense of the Senate.
Sec. 5183. Amending section 708 of the Homeland Security Act of 2002.
Subtitle J—Other Provisions
CHAPTER 1—DEEPFAKE TASK FORCE
Sec. 5191 Short title.
Sec. 5192. National deepfake and digital provenance task force.
CHAPTER 2—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS
Sec. 5194. CISA Technical Corrections and Improvements.
CHAPTER 3—POST-DISASTER MENTAL HEALTH RESPONSE ACT
Sec. 5198. Post-Disaster Mental Health Response.
TITLE LII—GOVERNMENTAL AFFAIRS
Subtitle A—Safeguarding American Innovation
Sec. 5201. Short title.
Sec. 5202. Federal Research Security Council.
Sec. 5203. Federal grant application fraud.
Sec. 5204. Restricting the acquisition of emerging technologies by certain aliens.
Subtitle B—Intragovernmental Cybersecurity Information Sharing Act
Sec. 5211. Requirement for information sharing agreements.
Subtitle C—Improving Government for America's Taxpayers
Sec. 5221. Government Accountability Office unimplemented priority recommendations.
Subtitle D—Advancing American AI Act
Sec. 5231. Short title.
Sec. 5232. Purposes.
Sec. 5233. Definitions.
Sec. 5234. Principles and policies for use of artificial intelligence in Government.
Sec. 5235. Agency inventories and artificial intelligence use cases.
Sec. 5236. Rapid pilot, deployment and scale of applied artificial intelligence capabilities to demonstrate modernization activities related to use cases.
Sec. 5237. Enabling entrepreneurs and agency missions.
Subtitle E—Strategic EV Management
Sec. 5241. Short Title.
Sec. 5242. Definitions.
Sec. 5243. Strategic guidance.
Sec. 5244. Study of Federal fleet vehicles.
Subtitle F—Congressionally Mandated Reports
Sec. 5251. Short title.
Sec. 5252. Definitions.
Sec. 5253. Establishment of online portal for congressionally mandated reports.
Sec. 5254. Federal agency responsibilities.
Sec. 5255. Changing or removing reports.
Sec. 5256. Withholding of information.
Sec. 5257. Implementation.
Sec. 5258. Determination of budgetary effects.

TITLE LI—HOMELAND SECURITY

Subtitle A—Global Catastrophic Risk Management Act of 2022

SEC. 5101. SHORT TITLE.

This subtitle may be cited as the ''Global Catastrophic Risk Management Act of 2022''.

SEC. 5102. DEFINITIONS.

In this subtitle:

(1) BASIC NEED.—The term ''basic need''—

(A) means any good, service, or activity necessary to protect the health, safety, and general welfare of the civilian population of the United States; and

(B) includes—

(i) food;

(ii) water;

(iii) shelter;

(iv) basic communication services;

(v) basic sanitation and health services; and

(vi) public safety.

(2) CATASTROPHIC INCIDENT.—The term ''catastrophic incident''—

(A) means any natural or man-made disaster that results in extraordinary levels of casualties or damage, mass evacuations, or disruption severely affecting the population, infrastructure, environment, economy, national morale, or government functions in an area; and

(B) may include an incident—

(i) with a sustained national impact over a prolonged period of time;

(ii) that may rapidly exceed resources available to State and local government and private sector authorities in the impacted area; or

(iii) that may significantly interrupt governmental operations and emergency services to such an extent that national security could be threatened.

(3) COMMITTEE.—The term ''committee'' means the interagency committee on global catastrophic risk established under section 5103.

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

(5) EXISTENTIAL RISK.—The term ''existential risk'' means the potential for an outcome that would result in human extinction.

(6) GLOBAL CATASTROPHIC RISK.—The term ''global catastrophic risk'' means the risk of events or incidents consequential enough to significantly harm, set back, or destroy human civilization at the global scale.

(7) GLOBAL CATASTROPHIC AND EXISTENTIAL THREATS.—The term ''global catastrophic and existential threats'' means those threats that with varying likelihood can produce consequences severe enough to result in significant harm or destruction of human civilization at the global scale, or lead to human extinction. Examples of global catastrophic and existential threats include severe global pandemics, nuclear war, asteroid and comet impacts, supervolcanoes, sudden and severe changes to the climate, and intentional or accidental threats arising from the use and development of emerging technologies.

(8) NATIONAL EXERCISE PROGRAM.—The term ''national exercise program'' means activities carried out to test and evaluate the national preparedness goal and related plans and strategies as described in section 648(b) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 748(b)).

(9) TRIBAL GOVERNMENT.—The term ''Tribal government'' means the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent list published pursuant to section 104 of the Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 5131).

SEC. 5103. INTERAGENCY COMMITTEE ON GLOBAL CATASTROPHIC RISK.

(a) ESTABLISHMENT.—Not later than 90 days after the date of enactment of this Act, the President shall establish an interagency committee on global catastrophic risk.

(b) MEMBERSHIP.—The committee shall include senior representatives of—

(1) the Assistant to the President for National Security Affairs;

(2) the Director of the Office of Science and Technology Policy;

(3) the Director of National Intelligence and the Director of the National Intelligence Council;

(4) the Secretary of Homeland Security and the Administrator of the Federal Emergency Management Agency;

(5) the Secretary of State and the Under Secretary of State for Arms Control and International Security;

(6) the Attorney General and the Director of the Federal Bureau of Investigation;

(7) the Secretary of Energy, the Under Secretary of Energy for Nuclear Security, and the Director of Science;

(8) the Secretary of Health and Human Services, the Assistant Secretary for Preparedness and Response, and the Assistant Secretary of Global Affairs;

(9) the Secretary of Commerce, the Under Secretary of Commerce for Oceans and Atmosphere, and the Under Secretary of Commerce for Standards and Technology;

(10) the Secretary of the Interior and the Director of the United States Geological Survey;
(11) the Administrator of the Environmental Protection Agency and the Assistant Administrator for Water;
(12) the Administrator of the National Aeronautics and Space Administration;
(13) the Director of the National Science Foundation;
(14) the Secretary of the Treasury;
(15) the Chair of the Board of Governors of the Federal Reserve System;
(16) the Secretary of Defense, the Assistant Secretary of the Army for Civil Works, and the Chief of Engineers and Commanding General of the Army Corps of Engineers;
(17) the Chairman of the Joint Chiefs of Staff;
(18) the Administrator of the United States Agency for International Development; and
(19) other stakeholders the President determines appropriate.

(c) CHAIRMANSHIP.—The committee shall be co-chaired by a senior representative of the President and the Deputy Administrator of the Federal Emergency Management Agency for Resilience.

SEC. 5104. REPORT REQUIRED.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and every 10 years thereafter, the President, with support from the committee, shall conduct and submit to Congress a report containing a detailed assessment of global catastrophic and existential risk.

(b) MATTERS COVERED.—Each report required under subsection (a) shall include —

(1) expert estimates of cumulative global catastrophic and existential risk in the next 30 years, including separate estimates for the likelihood of occurrence and potential consequences;
(2) expert-informed analyses of the risk of the most concerning specific global catastrophic and existential threats, including separate estimates, where reasonably feasible and credible, of each threat for its likelihood of occurrence and its potential consequences, as well as associated uncertainties;
(3) a comprehensive list of potential catastrophic or existential threats, including even those that may have very low likelihood;
(4) technical assessments and lay explanations of the analyzed global catastrophic and existential risks, including their qualitative character and key factors affecting their likelihood of occurrence and potential consequences;
(5) an explanation of any factors that limit the ability of the President to assess the risk both cumulatively and for particular threats, and how those limitations may be overcome through future research or with additional resources, programs, or authorities;
(6) a review of the effectiveness of intelligence collection, early warning and detection systems, or other functions and programs necessary to evaluate the risk of particular global catastrophic and existential threats, if any exist and as applicable for particular threats;
(7) a forecast of if and why global catastrophic and existential risk is likely to increase or decrease significantly in the next 30 years, both qualitatively and quantitatively, as well as a description of associated uncertainties;
(8) proposals for how the Federal Government may more adequately assess global catastrophic and existential risk on an ongoing basis in future years;
(9) recommendations for legislative actions, as appropriate, to support the evaluation and assessment of global catastrophic and existential risk; and
(10) other matters deemed appropriate by the President.

(c) CONSULTATION REQUIREMENT.—In producing the report required under subsection (a), the President, with support from the committee, shall regularly consult with experts on global catastrophic and existential risks, including from non-governmental, academic, and private sector institutions.

(d) FORM.—The report required under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 5105. REPORT ON CONTINUITY OF OPERATIONS AND CONTINUITY OF GOVERNMENT PLANNING.

(a) IN GENERAL.—Not later than 180 days after the submission of the report required under section 5104, the President, with support from the committee, shall produce a report on the adequacy of continuity of operations and continuity of government plans based on the assessed global catastrophic and existential risk.

(b) MATTERS COVERED.—The report required under subsection (a) shall include—

(1) a detailed assessment of the ability of continuity of government and continuity of operations plans and programs, as defined by Executive Order 13961 (85 Fed. Reg. 79379; relating to governance and integration of Federal mission resilience), Presidential Policy Directive–40 (July 15, 2016; relating to national continuity policy), or successor policies, to maintain national essential functions following global catastrophes, both cumulatively and for particular threats;
(2) an assessment of the need to revise Executive Order 13961 (85 Fed. Reg. 79379; relating to governance and integration of Federal mission resilience), Presidential Policy Directive–40 (July 15, 2016; relating to national continuity policy), or successor policies to account for global catastrophic and existential risk cumulatively or for particular threats;
(3) an assessment of any technology gaps limiting mitigation of global catastrophic and existential risks for continuity of operations and continuity of government plans;
(4) a budget proposal for continuity of government and continuity of operations programs necessary to adequately maintain national essential functions during global catastrophes;
(5) recommendations for legislative actions and technology development and implementation actions necessary to improve continuity of government and continuity of operations plans and programs;
(6) a plan for increased senior leader involvement in continuity of operations and continuity of government exercises; and
(7) other matters deemed appropriate by the co-chairs of the committee.

(c) FORM.—The report required under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 5106. ENHANCED CATASTROPHIC INCIDENT ANNEX.

(a) IN GENERAL.—The President, with support from the committee, shall supplement each Federal Interagency Operational Plan to include an annex containing a strategy to ensure the health, safety, and general welfare of the civilian population affected by catastrophic incidents by—

(1) providing for the basic needs of the civilian population of the United States that is impacted by catastrophic incidents in the United States;
(2) coordinating response efforts with State and local governments, the private sector, and nonprofit relief organizations;
(3) promoting personal and local readiness and non-reliance on government relief during periods of heightened tension or after catastrophic incidents; and
(4) developing international partnerships with allied nations for the provision of relief services and goods.

(b) ELEMENTS OF THE STRATEGY.—The strategy required under subsection (a) shall include a description of—

(1) actions the President will take to ensure the basic needs of the civilian population of the United States in a catastrophic incident are met;
(2) how the President will coordinate with non-Federal entities to multiply resources and enhance relief capabilities, including—
(A) State and local governments;
(B) Tribal governments;
(C) State disaster relief agencies;
(D) State and local disaster relief managers;
(E) State National Guards;
(F) law enforcement and first response entities; and
(G) nonprofit relief services;
(3) actions the President will take to enhance individual resiliency to the effects of a catastrophic incident, which actions shall include—
(A) readiness alerts to the public during periods of elevated threat;
(B) efforts to enhance domestic supply and availability of critical goods and basic necessities; and
(C) information campaigns to ensure the public is aware of response plans and services that will be activated when necessary;
(4) efforts the President will undertake and agreements the President will seek with international allies to enhance the readiness of the United States to provide for the general welfare;
(5) how the strategy will be implemented should multiple levels of critical infrastructure be destroyed or taken offline entirely for an extended period of time; and
(6) the authorities the President would implicate in responding to a catastrophic incident.

(c) ASSUMPTIONS.—In designing the strategy under subsection (a), the President shall account for certain factors to make the strategy operationally viable, including the assumption that—

(1) multiple levels of critical infrastructure have been taken offline or destroyed by catastrophic incidents or the effects of catastrophic incidents;
(2) impacted sectors may include—
(A) the transportation sector;
(B) the communication sector;
(C) the energy sector;
(D) the healthcare and public health sector;
(E) the water and wastewater sector; and
(F) the financial sector;
(3) State, local, Tribal, and territorial governments have been equally affected or made largely inoperable by catastrophic incidents or the effects of catastrophic incidents;
(4) the emergency has exceeded the response capabilities of State and local governments under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) and other relevant disaster response laws; and
(5) the United States military is sufficiently engaged in armed or cyber conflict with State or non-State adversaries, or is otherwise unable to augment domestic response capabilities in a significant manner due to a catastrophic incident.

(d) EXISTING PLANS.—The President may incorporate existing contingency plans in the strategy developed under subsection (a) so long as those contingency plans are amended to be operational in accordance with the requirements under this section.

(e) AVAILABILITY.—The strategy developed under subsection (a) shall be available to the public but may include a classified, or other

restricted, annex to be made available to the appropriate committees of Congress and appropriate government entities.

SEC. 5107. VALIDATION OF THE STRATEGY THROUGH AN EXERCISE.

Not later than 1 year after the addition of the annex required under section 5106, the Department of Homeland Security shall lead an exercise as part of the national exercise program, in coordination with the committee, to test and enhance the operationalization of the strategy required under section 5106.

SEC. 5108. RECOMMENDATIONS.

(a) IN GENERAL.—The President shall provide recommendations to Congress for—

(1) actions that should be taken to prepare the United States to implement the strategy required under section 5106, increase readiness, and address preparedness gaps for responding to the impacts of catastrophic incidents on citizens of the United States; and

(2) additional authorities that should be considered for Federal agencies and the President to more effectively implement the strategy required under section 5106.

(b) INCLUSION IN REPORTS.—The President may include the recommendations required under subsection (a) in a report submitted under section 5109.

SEC. 5109. REPORTING REQUIREMENTS.

Not later than 1 year after the date on which Department of Homeland Security leads the exercise under section 5107, the President shall submit to Congress a report that includes—

(1) a description of the efforts of the President to develop and update the strategy required under section 5106; and

(2) an after-action report following the conduct of the exercise described in section 5107.

SEC. 5110. RULE OF CONSTRUCTION.

Nothing in this subtitle shall be construed to supersede the civilian emergency management authority of the Administrator of the Federal Emergency Management Agency under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) or the Post Katrina Emergency Management Reform Act (6 U.S.C. 701 et seq.).

Subtitle B—DHS Trade and Economic Security Council

SEC. 5111. DHS TRADE AND ECONOMIC SECURITY COUNCIL.

(a) ESTABLISHMENT OF THE DHS TRADE AND ECONOMIC SECURITY COUNCIL.—

(1) DEFINITIONS.—In this subsection:

(A) COUNCIL.—The term ''Council'' means the DHS Trade and Economic Security Council established under paragraph (2).

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

(C) ECONOMIC SECURITY.—The term ''economic security'' has the meaning given that term in section 890B(c)(2) of the Homeland Security Act of 2002 (6 U.S.C. 474(c)(2)).

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

(2) DHS TRADE AND ECONOMIC SECURITY COUNCIL.—In accordance with the mission of the Department under section 101(b) of the Homeland Security Act of 2002 (6 U.S.C. 111(b)), and in particular paragraph (1)(F) of that section, the Secretary shall establish a standing council of component heads or their designees within the Department, which shall be known as the ''DHS Trade and Economic Security Council''.

(3) DUTIES OF THE COUNCIL.—Pursuant to the scope of the mission of the Department as described in paragraph (2), the Council shall provide to the Secretary advice and recommendations on matters of trade and economic security, including—

(A) identifying concentrated risks for trade and economic security;

(B) setting priorities for securing the trade and economic security of the United States;

(C) coordinating Department-wide activity on trade and economic security matters;

(D) with respect to the development of the continuity of the economy plan of the President under section 9603 of the William M. (Mac) Thornberry National Defense Authorization Act of Fiscal Year 2021 (6 U.S.C. 322);

(E) proposing statutory and regulatory changes impacting trade and economic security; and

(F) any other matters the Secretary considers appropriate.

(4) CHAIR AND VICE CHAIR.—The Under Secretary for Strategy, Policy, and Plans of the Department—

(A) shall serve as Chair of the Council; and

(B) may designate a Council member as a Vice Chair.

(5) MEETINGS.—The Council shall meet not less frequently than quarterly, as well as—

(A) at the call of the Chair; or

(B) at the direction of the Secretary.

(6) BRIEFINGS.—Not later than 180 days after the date of enactment of this Act and every 180 days thereafter for 4 years, the Council shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the actions and activities of the Council.

(b) ASSISTANT SECRETARY FOR TRADE AND ECONOMIC SECURITY.—Section 709 of the Homeland Security Act of 2002 (6 U.S.C. 349) is amended—

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

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

''(g) ASSISTANT SECRETARY FOR TRADE AND ECONOMIC SECURITY.—

''(1) IN GENERAL.—There is established within the Office of Strategy, Policy, and Plans an Assistant Secretary for Trade and Economic Security.

''(2) DUTIES.—At the direction of the Under Secretary for Strategy, Policy, and Plans, the Assistant Secretary for Trade and Economic Security shall be responsible for policy formulation regarding matters relating to economic security and trade, as such matters relate to the mission and the operations of the Department.

''(3) ADDITIONAL RESPONSIBILITIES.—In addition to the duties specified in paragraph (2), the Assistant Secretary for Trade and Economic Security, at the direction of the Under Secretary for Strategy, Policy, and Plans, may—

''(A) oversee—

''(i) coordination of supply chain policy; and

''(ii) assessments and reports to Congress related to critical economic security domains;

''(B) serve as the representative of the Under Secretary for Strategy, Policy, and Plans for the purposes of representing the Department on—

''(i) the Committee on Foreign Investment in the United States; and

''(ii) the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector;

''(C) coordinate with stakeholders in other Federal departments and agencies and nongovernmental entities with trade and economic security interests, authorities, and responsibilities; and

''(D) perform such additional duties as the Secretary or the Under Secretary of Strategy, Policy, and Plans may prescribe.

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

''(A) CRITICAL ECONOMIC SECURITY DOMAIN.—The term 'critical economic security domain' means any infrastructure, industry, technology, or intellectual property (or combination thereof) that is essential for the economic security of the United States.

''(B) ECONOMIC SECURITY.—The term 'economic security' has the meaning given that term in section 890B(c)(2).''.

(c) RULE OF CONSTRUCTION.—Nothing in this section or the amendments made by this section shall be construed to affect or diminish the authority otherwise granted to any other officer of the Department of Homeland Security.

Subtitle C—Transnational Criminal Investigative Units

SEC. 5121. SHORT TITLE.

This subtitle may be cited as the ''Transnational Criminal Investigative Unit Stipend Act''.

SEC. 5122. STIPENDS FOR TRANSNATIONAL CRIMINAL INVESTIGATIVE UNITS.

(a) IN GENERAL.—Subtitle H of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 451 et seq.) is amended by adding at the end the following:

''SEC. 890C. TRANSNATIONAL CRIMINAL INVESTIGATIVE UNITS.

''(a) IN GENERAL.—The Secretary shall operate Transnational Criminal Investigative Units within United States Immigration and Customs Enforcement, Homeland Security Investigations.

''(b) COMPOSITION.—Each Transnational Criminal Investigative Unit shall be composed of trained foreign law enforcement officials who shall collaborate with Homeland Security Investigations to investigate and prosecute individuals involved in transnational criminal activity.

''(c) VETTING REQUIREMENT.—

''(1) IN GENERAL.—Upon entry into a Transnational Criminal Investigative Unit, and at periodic intervals while serving in such a unit, foreign law enforcement officials shall be required to pass certain security evaluations, which may include a background check, a polygraph examination, a urinalysis test, or other measures that the Director of U.S. Immigration and Customs Enforcement determines to be appropriate.

''(2) REPORT.—The Director of U.S. Immigration and Customs Enforcement shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives that describes—

''(A) the procedures used for vetting Transnational Criminal Investigative Unit members; and

''(B) any additional measures that should be implemented to prevent personnel in vetted units from being compromised by criminal organizations.

''(d) MONETARY STIPEND.—The Director of U.S. Immigration and Customs Enforcement is authorized to pay vetted members of a Transnational Criminal Investigative Unit a monetary stipend in an amount associated with their duties dedicated to unit activities.

''(e) ANNUAL BRIEFING.—The Director of U.S. Immigration and Customs Enforcement, during the 5-year period beginning on the date of the enactment of this Act, shall provide an annual unclassified briefing to the congressional committees referred to in subsection (c)(2), which may include a classified session, if necessary, that identifies—

''(1) the number of vetted members of Transnational Criminal Investigative Unit in each country;

''(2) the amount paid in stipends to such members, disaggregated by country; and

''(3) relevant enforcement statistics, such as arrests and progress made on joint investigations, in each such country.''.

(b) CLERICAL AMENDMENT.—The table of contents for the Homeland Security Act of

2002 (Public Law 107–296) is amended by inserting after the item relating to section 890B the following:

''Sec. 890C. Transnational Criminal Investigative Units.''.

Subtitle D—Technological Hazards Preparedness and Training

SEC. 5131. SHORT TITLE.

This subtitle may be cited as the ''Technological Hazards Preparedness and Training Act of 2022''.

SEC. 5132. DEFINITIONS.

In this subtitle:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Federal Emergency Management Agency.

(2) INDIAN TRIBAL GOVERNMENT.—The term ''Indian Tribal government'' has the meaning given the term ''Indian tribal government'' in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(3) LOCAL GOVERNMENT; STATE.—The terms ''local government'' and ''State'' have the meanings given those terms in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).

(4) TECHNOLOGICAL HAZARD AND RELATED EMERGING THREAT.—The term ''technological hazard and related emerging threat''—

(A) means a hazard that involves materials created by humans that pose a unique hazard to the general public and environment and which may result from—

(i) an accident;

(ii) an emergency caused by another hazard; or

(iii) intentional use of the hazardous materials; and

(B) includes a chemical, radiological, biological, and nuclear hazard.

SEC. 5133. ASSISTANCE AND TRAINING FOR COMMUNITIES WITH TECHNOLOGICAL HAZARDS AND RELATED EMERGING THREATS.

(a) IN GENERAL.—The Administrator shall maintain the capacity to provide States and local governments with technological hazards and related emerging threats technical assistance, training, and other preparedness programming to build community resilience to technological hazards and related emerging threats.

(b) AUTHORITIES.—The Administrator shall carry out subsection (a) in accordance with—

(1) the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.);

(2) section 1236 of the Disaster Recovery Reform Act of 2018 (42 U.S.C. 5196g); and

(3) the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109–295; 120 Stat. 1394).

(c) ASSESSMENT AND NOTIFICATION.—In carrying out subsection (a), the Administrator shall—

(1) use any available and appropriate multi-hazard risk assessment and mapping tools and capabilities to identify the communities that have the highest risk of and vulnerability to a technological hazard in each State; and

(2) ensure each State and Indian Tribal government is aware of—

(A) the communities identified under paragraph (1); and

(B) the availability of programming under this section for—

(i) technological hazards and related emerging threats preparedness; and

(ii) building community capability.

(d) REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Administrator shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Appropriations of the Senate, the Committee on Homeland Security of the House of Representatives, the Committee on Appropriations of the House of Representatives, and the Committee on Transportation and Infrastructure of the House of Representatives a report relating to—

(1) actions taken to implement this section; and

(2) technological hazards and related emerging threats preparedness programming provided under this section during the 1-year period preceding the date of submission of the report.

(e) CONSULTATION.—The Secretary of Homeland Security may seek continuing input relating to technological hazards and related emerging threats preparedness needs by consulting State, Tribal, territorial, and local emergency services organizations and private sector stakeholders.

SEC. 5134. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to carry out this subtitle $20,000,000 for each of fiscal years 2023 through 2024.

SEC. 5135. SAVINGS PROVISION.

Nothing in this subtitle shall diminish or divert resources from—

(1) the full completion of federally-led chemical surety material storage missions or chemical demilitarization missions that are underway as of the date of enactment of this Act; or

(2) any transitional activities or other community assistance incidental to the completion of the missions described in paragraph (1).

Subtitle E—Offices of Countering Weapons of Mass Destruction and Health Security

SEC. 5141. SHORT TITLE.

This subtitle may be cited as the ''Offices of Countering Weapons of Mass Destruction and Health Security Act of 2022''.

CHAPTER 1—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

SEC. 5142. COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE.

(a) HOMELAND SECURITY ACT OF 2002.—Title XIX of the Homeland Security Act of 2002 (6 U.S.C. 590 et seq.) is amended—

(1) in section 1901 (6 U.S.C. 591)—

(A) in subsection (c), by amending paragraphs (1) and (2) to read as follows:

''(1) matters and strategies pertaining to—

''(A) weapons of mass destruction; and

''(B) chemical, biological, radiological, nuclear, and other related emerging threats; and

''(2) coordinating the efforts of the Department to counter—

''(A) weapons of mass destruction; and

''(B) chemical, biological, radiological, nuclear, and other related emerging threats.''; and

(B) by striking subsection (e);

(2) by amending section 1921 (6 U.S.C. 591g) to read as follows:

''SEC. 1921. MISSION OF THE OFFICE.

''The Office shall be responsible for—

''(1) coordinating the efforts of the Department to counter—

''(A) weapons of mass destruction; and

''(B) chemical, biological, radiological, nuclear, and other related emerging threats; and

''(2) enhancing the ability of Federal, State, local, Tribal, and territorial partners to prevent, detect, protect against, and mitigate the impacts of attacks using—

''(A) weapons of mass destruction against the United States; and

''(B) chemical, biological, radiological, nuclear, and other related emerging threats against the United States.'';

(3) in section 1922 (6 U.S.C. 591h)—

(A) by striking subsection (b); and

(B) by redesignating subsection (c) as subsection (b);

(4) in section 1923 (6 U.S.C. 592)—

(A) by redesignating subsections (a) and (b) as subsections (b) and (d), respectively;

(B) by inserting before subsection (b), as so redesignated, the following:

''(a) OFFICE RESPONSIBILITIES.—

''(1) IN GENERAL.—For the purposes of coordinating the efforts of the Department to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, the Office shall—

''(A) provide expertise and guidance to Department leadership and components on chemical, biological, radiological, nuclear, and other related emerging threats, subject to the research, development, testing, and evaluation coordination requirement described in subparagraph (G);

''(B) in coordination with the Office for Strategy, Policy, and Plans, lead development of policies and strategies to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats on behalf of the Department;

''(C) identify, assess, and prioritize capability gaps relating to the strategic and mission objectives of the Department for weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats;

''(D) in coordination with the Office of Intelligence and Analysis, support components of the Department, and Federal, State, local, Tribal, and territorial partners, provide intelligence and information analysis and reports on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats;

''(E) in consultation with the Science and Technology Directorate, assess risk to the United States from weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats;

''(F) lead development and prioritization of Department requirements to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, subject to the research, development, testing, and evaluation coordination requirement described in subparagraph (G), which requirements shall be—

''(i) developed in coordination with end users; and

''(ii) reviewed by the Joint Requirements Council, as directed by the Secretary;

''(G) in coordination with the Science and Technology Directorate, direct, fund, and coordinate capability development activities to counter weapons of mass destruction and all chemical, biological, radiological, nuclear, and other related emerging threats research, development, test, and evaluation matters, including research, development, testing, and evaluation expertise, threat characterization, technology maturation, prototyping, and technology transition;

''(H) acquire, procure, and deploy counter weapons of mass destruction capabilities, and serve as the lead advisor of the Department on component acquisition, procurement, and deployment of counter-weapons of mass destruction capabilities;

''(I) in coordination with the Office of Health Security, support components of the Department, and Federal, State, local, Tribal, and territorial partners on chemical, biological, radiological, nuclear, and other related emerging threats health matters;

''(J) provide expertise on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats to Department and Federal partners to support engagements and efforts with international partners subject to the research, development, testing, and evaluation

coordination requirement under subparagraph (G); and

''(K) carry out any other duties assigned to the Office by the Secretary.

''(2) DETECTION AND REPORTING.—For purposes of the detection and reporting responsibilities of the Office for weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, the Office shall—

''(A) in coordination with end users, including State, local, Tribal, and territorial partners, as appropriate—

''(i) carry out a program to test and evaluate technology, in consultation with the Science and Technology Directorate, to detect and report on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats weapons or unauthorized material, in coordination with other Federal agencies, as appropriate, and establish performance metrics to evaluate the effectiveness of individual detectors and detection systems in detecting those weapons or material—

''(I) under realistic operational and environmental conditions; and

''(II) against realistic adversary tactics and countermeasures;

''(B) in coordination with end users, conduct, support, coordinate, and encourage a transformational program of research and development to generate and improve technologies to detect, protect against, and report on the illicit entry, transport, assembly, or potential use within the United States of weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats weapons or unauthorized material, and coordinate with the Under Secretary for Science and Technology on research and development efforts relevant to the mission of the Office and the Under Secretary for Science and Technology;

''(C) before carrying out operational testing under subparagraph (A), develop a testing and evaluation plan that articulates the requirements for the user and describes how these capability needs will be tested in developmental test and evaluation and operational test and evaluation;

''(D) as appropriate, develop, acquire, and deploy equipment to detect and report on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats weapons or unauthorized material in support of Federal, State, local, Tribal, and territorial governments;

''(E) support and enhance the effective sharing and use of appropriate information on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats and related emerging issues generated by elements of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), law enforcement agencies, other Federal agencies, State, local, Tribal, and territorial governments, and foreign governments, as well as provide appropriate information to those entities;

''(F) consult, as appropriate, with the Federal Emergency Management Agency and other departmental components, on weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats and efforts to mitigate, prepare, and respond to all threats in support of the State, local, and Tribal communities; and

''(G) perform other duties as assigned by the Secretary.'';

(C) in subsection (b), as so redesignated—

(i) in the subsection heading, by striking ''MISSION'' and inserting ''RADIOLOGICAL AND NUCLEAR RESPONSIBILITIES'';

(ii) in paragraph (1)—

(I) by inserting ''deploy,'' after ''acquire,''; and

(II) by striking ''deployment'' and inserting ''operations'';

(iii) by striking paragraphs (6) through (10);

(iv) redesignating paragraphs (11) and (12) as paragraphs (6) and (7), respectively;

(v) in paragraph (6)(B), as so redesignated, by striking ''national strategic five-year plan referred to in paragraph (10)'' and inserting ''United States national technical nuclear forensics strategic planning'';

(vi) in paragraph (7)(C)(v), as so redesignated—

(I) in the matter preceding subclause (I), by inserting ''except as otherwise provided,'' before ''require''; and

(II) in subclause (II)—

(aa) in the matter preceding item (aa), by striking ''death or disability'' and inserting ''death, disability, or a finding of good cause as determined by the Assistant Secretary (including extreme hardship, extreme need, or the needs of the Office) and for which the Assistant Secretary may grant a waiver of the repayment obligation''; and

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

(vii) by striking paragraph (13); and

(viii) by redesignating paragraph (14) as paragraph (8); and

(D) by inserting after subsection (b), as so redesignated, the following:

''(c) CHEMICAL AND BIOLOGICAL RESPONSIBILITIES.—The Office—

''(1) shall be responsible for coordinating with other Federal efforts to enhance the ability of Federal, State, local, and Tribal governments to prevent, detect, protect against, and mitigate the impacts of chemical and biological threats against the United States; and

''(2) shall—

''(A) serve as a primary entity of the Federal Government to further develop, acquire, deploy, and support the operations of a national biosurveillance system in support of Federal, State, local, Tribal, and territorial governments, and improve that system over time;

''(B) enhance the chemical and biological detection efforts of Federal, State, local, Tribal, and territorial governments and provide guidance, tools, and training to help ensure a managed, coordinated response; and

''(C) collaborate with the Biomedical Advanced Research and Development Authority, the Office of Health Security, the Defense Advanced Research Projects Agency, and the National Aeronautics and Space Administration, and other relevant Federal stakeholders, and receive input from industry, academia, and the national laboratories on chemical and biological surveillance efforts.'';

(5) in section 1924 (6 U.S.C. 593), by striking ''section 11011 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note).'' and inserting ''section 4092 of title 10, United States Code, except that the authority shall be limited to facilitate the recruitment of experts in the chemical, biological, radiological, or nuclear specialties.'';

(6) in section 1927(a)(1)(C) (6 U.S.C. 596a(a)(1)(C))—

(A) in clause (i), by striking ''required under section 1036 of the National Defense Authorization Act for Fiscal Year 2010'';

(B) in clause (ii), by striking ''and'' at the end;

(C) in clause (iii), by striking the period at the end and inserting ''; and''; and

(D) by adding at the end the following:

''(iv) includes any other information regarding national technical nuclear forensics activities carried out under section 1923.'';

(7) in section 1928 (6 U.S.C. 596b)—

(A) in subsection (c)(1), by striking ''from among high-risk urban areas under section 2003'' and inserting ''based on the capability and capacity of the jurisdiction, as well as the relative threat, vulnerability, and consequences from terrorist attacks and other high-consequence events utilizing nuclear or other radiological materials''; and

(B) by striking subsection (d) and inserting the following:

''(d) REPORT.—Not later than 2 years after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2022, the Secretary shall submit to the appropriate congressional committees an update on the STC program.''; and

(8) by adding at the end the following:

''SEC. 1929. ACCOUNTABILITY.

''(a) DEPARTMENTWIDE STRATEGY.—

''(1) IN GENERAL.—Not later than 180 days after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2022, and every 4 years thereafter, the Secretary shall create a Departmentwide strategy and implementation plan to counter weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats, which should—

''(A) have clearly identified authorities, specified roles, objectives, benchmarks, accountability, and timelines;

''(B) incorporate the perspectives of non-Federal and private sector partners; and

''(C) articulate how the Department will contribute to relevant national-level strategies and work with other Federal agencies.

''(2) CONSIDERATION.—The Secretary shall appropriately consider weapons of mass destruction and chemical, biological, radiological, nuclear, and other related emerging threats when creating the strategy and implementation plan required under paragraph (1).

''(3) REPORT.—The Office shall submit to the appropriate congressional committees a report on the updated Departmentwide strategy and implementation plan required under paragraph (1).

''(b) DEPARTMENTWIDE BIODEFENSE REVIEW AND STRATEGY.—

''(1) IN GENERAL.—Not later than 180 days after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2022, the Secretary, in consultation with appropriate stakeholders representing Federal, State, Tribal, territorial, academic, private sector, and nongovernmental entities, shall conduct a Departmentwide review of biodefense activities and strategies.

''(2) REVIEW.—The review required under paragraph (1) shall—

''(A) identify with specificity the biodefense lines of effort of the Department, including relating to biodefense roles, responsibilities, and capabilities of components and offices of the Department;

''(B) assess how such components and offices coordinate internally and with public and private partners in the biodefense enterprise;

''(C) identify any policy, resource, capability, or other gaps in the Department's ability to assess, prevent, protect against, and respond to biological threats; and

''(D) identify any organizational changes or reforms necessary for the Department to effectively execute its biodefense mission and role, including with respect to public and private partners in the biodefense enterprise.

''(3) STRATEGY.—Not later than 1 year after completion of the review required under paragraph (1), the Secretary shall issue a biodefense strategy for the Department that—

''(A) is informed by such review and is aligned with section 1086 of the National Defense Authorization Act for Fiscal Year 2017 (6 U.S.C. 104; relating to the development of a national biodefense strategy and associated implementation plan, including a review and assessment of biodefense policies, practices, programs, and initiatives) or any successor strategy; and

''(B) shall—

''(i) describe the biodefense mission and role of the Department, as well as how such mission and role relates to the biodefense lines of effort of the Department;

''(ii) clarify, as necessary, biodefense roles, responsibilities, and capabilities of the components and offices of the Department involved in the biodefense lines of effort of the Department;

''(iii) establish how biodefense lines of effort of the Department are to be coordinated within the Department;

''(iv) establish how the Department engages with public and private partners in the biodefense enterprise, including other Federal agencies, national laboratories and sites, and State, local, Tribal, and territorial entities, with specificity regarding the frequency and nature of such engagement by Department components and offices with State, local, Tribal and territorial entities; and

''(v) include information relating to—

''(I) milestones and performance metrics that are specific to the biodefense mission and role of the Department described in clause (i); and

''(II) implementation of any operational changes necessary to carry out clauses (iii) and (iv).

''(4) PERIODIC UPDATE.—Beginning not later than 5 years after the issuance of the biodefense strategy and implementation plans required under paragraph (3), and not less often than once every 5 years thereafter, the Secretary shall review and update, as necessary, such strategy and plans.

''(5) CONGRESSIONAL OVERSIGHT.—Not later than 30 days after the issuance of the biodefense strategy and implementation plans required under paragraph (3), the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding such strategy and plans.

''(c) EMPLOYEE MORALE.—Not later than 180 days after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2022, the Office shall submit to and brief the appropriate congressional committees on a strategy and plan to continuously improve morale within the Office.

''(d) COMPTROLLER GENERAL.—Not later than 1 year after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2022, the Comptroller General of the United States shall conduct a review of and brief the appropriate congressional committees on—

''(1) the efforts of the Office to prioritize the programs and activities that carry out the mission of the Office, including research and development;

''(2) the consistency and effectiveness of stakeholder coordination across the mission of the Department, including operational and support components of the Department and State and local entities; and

''(3) the efforts of the Office to manage and coordinate the lifecycle of research and development within the Office and with other components of the Department, including the Science and Technology Directorate.

''(e) NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE.—

''(1) STUDY.—The Secretary shall enter into an agreement with the National Academies of Sciences, Engineering, and Medicine to conduct a consensus study and report to the Secretary and the appropriate congressional committees on—

''(A) the role of the Department in preparing, detecting, and responding to biological and health security threats to the homeland;

''(B) recommendations to improve departmental biosurveillance efforts against biological threats, including any relevant biological detection methods and technologies; and

''(C) the feasibility of different technological advances for biodetection compared to the cost, risk reduction, and timeliness of those advances.

''(2) BRIEFING.—Not later than 1 year after the date on which the Secretary receives the report required under paragraph (1), the Secretary shall brief the appropriate congressional committees on—

''(A) the implementation of the recommendations included in the report; and

''(B) the status of biological detection at the Department, and, if applicable, timelines for the transition from Biowatch to updated technology.

''(f) ADVISORY COUNCIL.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of the Offices of Countering Weapons of Mass Destruction and Health Security Act of 2022, the Secretary shall establish an advisory body to advise on the ongoing coordination of the efforts of the Department to counter weapons of mass destruction, to be known as the Advisory Council for Countering Weapons of Mass Destruction (in this subsection referred to as the 'Advisory Council').

''(2) MEMBERSHIP.—The members of the Advisory Council shall—

''(A) be appointed by the Assistant Secretary; and

''(B) to the extent practicable, represent a geographic (including urban and rural) and substantive cross section of officials, from State, local, and Tribal governments, academia, the private sector, national laboratories, and nongovernmental organizations, including, as appropriate—

''(i) members selected from the emergency management field and emergency response providers;

''(ii) State, local, and Tribal government officials;

''(iii) experts in the public and private sectors with expertise in chemical, biological, radiological, and nuclear agents and weapons;

''(iv) representatives from the national laboratories; and

''(v) such other individuals as the Assistant Secretary determines to be appropriate.

''(3) RESPONSIBILITIES.— The Advisory Council shall—

''(A) advise the Assistant Secretary on all aspects of countering weapons of mass destruction;

''(B) incorporate State, local, and Tribal government, national laboratories, and private sector input in the development of the strategy and implementation plan of the Department for countering weapons of mass destruction; and

''(C) establish performance criteria for a national biological detection system and review the testing protocol for biological detection prototypes.

''(4) CONSULTATION.—To ensure input from and coordination with State, local, and Tribal governments, the Assistant Secretary shall regularly consult and work with the Advisory Council on the administration of Federal assistance provided by the Department, including with respect to the development of requirements for countering weapons of mass destruction programs, as appropriate.

''(5) VOLUNTARY SERVICE.—The members of the Advisory Council shall serve on the Advisory Council on a voluntary basis.

''(6) FACA.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Advisory Council.''.

(b) COUNTERING WEAPONS OF MASS DESTRUCTION ACT OF 2018.—Section 2 of the Countering Weapons of Mass Destruction Act of 2018 (Public Law 115–387; 132 Stat. 5162) is amended—

(1) in subsection (b)(2) (6 U.S.C. 591 note), by striking ''1927'' and inserting ''1926''; and

(2) in subsection (g) (6 U.S.C. 591 note)—

(A) in the matter preceding paragraph (1), by striking ''one year after the date of the enactment of this Act, and annually thereafter,'' and inserting ''June 30 of each year,''; and

(B) in paragraph (2), by striking ''Security, including research and development activities'' and inserting ''Security''.

(c) SECURITY AND ACCOUNTABILITY FOR EVERY PORT ACT OF 2006.—The Security and Accountability for Every Port Act of 2006 (6 U.S.C. 901 et seq.) is amended—

(1) in section 1(b) (Public Law 109–347; 120 Stat 1884), by striking the item relating to section 502; and

(2) by striking section 502 (6 U.S.C. 592a).

SEC. 5143. RULE OF CONSTRUCTION.

Nothing in this chapter or the amendments made by this chapter shall be construed to affect or diminish the authorities or responsibilities of the Under Secretary for Science and Technology.

CHAPTER 2—OFFICE OF HEALTH SECURITY

SEC. 5144. OFFICE OF HEALTH SECURITY.

(a) ESTABLISHMENT.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) in section 103 (6 U.S.C. 113)—

(A) in subsection (a)(2)—

(i) by striking ''the Assistant Secretary for Health Affairs,''; and

(ii) by striking ''Affairs, or'' and inserting ''Affairs or''; and

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

''(6) A Chief Medical Officer.'';

(2) by adding at the end the following:

''TITLE XXIII—OFFICE OF HEALTH SECURITY'';

(3) by redesignating section 1931 (6 U.S.C. 597) as section 2301 and transferring such section to appear after the heading for title XXIII, as added by paragraph (2); and

(4) in section 2301, as so redesignated—

(A) in the section heading, by striking ''**CHIEF MEDICAL OFFICER**'' and inserting ''**OFFICE OF HEALTH SECURITY**'';

(B) by striking subsections (a) and (b) and inserting the following:

''(a) IN GENERAL.—There is established in the Department an Office of Health Security.

''(b) HEAD OF OFFICE OF HEALTH SECURITY.—The Office of Health Security shall be headed by a chief medical officer, who shall—

''(1) be the Assistant Secretary for Health Security and the Chief Medical Officer of the Department;

''(2) be a licensed physician possessing a demonstrated ability in and knowledge of medicine and public health;

''(3) be appointed by the President; and

''(4) report directly to the Secretary.'';

(C) in subsection (c)—

(i) in the matter preceding paragraph (1), by striking ''medical issues related to natural disasters, acts of terrorism, and other man-made disasters'' and inserting ''oversight of all medical, public health, and workforce health and safety matters of the Department'';

(ii) in paragraph (1), by striking '', the Administrator of the Federal Emergency Management Agency, the Assistant Secretary, and other Department officials'' and inserting ''and all other Department officials'';

(iii) in paragraph (4), by striking ''and'' at the end;

(iv) by redesignating paragraph (5) as paragraph (13); and

(v) by inserting after paragraph (4) the following:

''(5) overseeing all medical and public health activities of the Department, including the delivery, advisement, and oversight of direct patient care and the organization, management, and staffing of component operations that deliver direct patient care;

''(6) advising the head of each component of the Department that delivers direct patient care regarding the recruitment and appointment of a component chief medical officer and deputy chief medical officer or the employee who functions in the capacity of chief medical officer and deputy chief medical officer;

''(7) advising the Secretary and the head of each component of the Department that delivers direct patient care regarding knowledge and skill standards for medical personnel and the assessment of that knowledge and skill;

''(8) advising the Secretary and the head of each component of the Department that delivers patient care regarding the collection, storage, and oversight of medical records;

''(9) with respect to any psychological health counseling or assistance program of the Department, including such a program of a law enforcement, operational, or support component of the Department, advising the head of each such component with such a program regarding—

''(A) ensuring such program includes safeguards against adverse action, including automatic referrals for a fitness for duty examination, by such component with respect to any employee solely because such employee self-identifies a need for psychological health counseling or assistance or receives such counseling or assistance;

''(B) increasing the availability and number of local psychological health professionals with experience providing psychological support services to personnel;

''(C) establishing a behavioral health curriculum for employees at the beginning of their careers to provide resources early regarding the importance of psychological health;

''(D) establishing periodic management training on crisis intervention and such component's psychological health counseling or assistance program;

''(E) improving any associated existing employee peer support programs, including by making additional training and resources available for peer support personnel in the workplace across such component;

''(F) developing and implementing a voluntary alcohol treatment program that includes a safe harbor for employees who seek treatment;

''(G) including, when appropriate, collaborating and partnering with key employee stakeholders and, for those components with employees with an exclusive representative, the exclusive representative with respect to such a program;

''(10) in consultation with the Chief Information Officer of the Department—

''(A) identifying methods and technologies for managing, updating, and overseeing patient records; and

''(B) setting standards for technology used by the components of the Department regarding the collection, storage, and oversight of medical records;

''(11) advising the Secretary and the head of each component of the Department that delivers direct patient care regarding contracts for the delivery of direct patient care, other medical services, and medical supplies;

''(12) coordinating with the Countering Weapons of Mass Destruction Office and other components of the Department as directed by the Secretary to enhance the ability of Federal, State, local, Tribal, and territorial governments to prevent, detect, protect against, and mitigate the health effects of chemical, biological, radiological, and nuclear issues; and''; and

(D) by adding at the end the following:

''(d) ASSISTANCE AND AGREEMENTS.—The Secretary, acting through the Chief Medical Officer, in support of the medical and public health activities of the Department, may—

''(1) provide technical assistance, training, and information and distribute funds through grants and cooperative agreements to State, local, Tribal, and territorial governments and nongovernmental organizations;

''(2) enter into other transactions;

''(3) enter into agreements with other Federal agencies; and

''(4) accept services from personnel of components of the Department and other Federal agencies on a reimbursable or nonreimbursable basis.

''(e) OFFICE OF HEALTH SECURITY PRIVACY OFFICER.—There shall be a Privacy Officer in the Office of Health Security with primary responsibility for privacy policy and compliance within the Office, who shall—

''(1) report directly to the Chief Medical Officer; and

''(2) ensure privacy protections are integrated into all Office of Health Security activities, subject to the review and approval of the Privacy Officer of the Department to the extent consistent with the authority of the Privacy Officer of the Department under section 222.

''(f) ACCOUNTABILITY.—

''(1) STRATEGY AND IMPLEMENTATION PLAN.—Not later than 180 days after the date of enactment of this section, and every 4 years thereafter, the Secretary shall create a Departmentwide strategy and implementation plan to address health threats.

''(2) BRIEFING.—Not later than 90 days after the date of enactment of this section, the Secretary shall brief the appropriate congressional committees on the organizational transformations of the Office of Health Security, including how best practices were used in the creation of the Office of Health Security.'';

(5) by redesignating section 710 (6 U.S.C. 350) as section 2302 and transferring such section to appear after section 2301, as so redesignated;

(6) in section 2302, as so redesignated—

(A) in the section heading, by striking ''**MEDICAL SUPPORT**'' and inserting ''**SAFETY**'';

(B) in subsection (a), by striking ''Under Secretary for Management'' each place that term appears and inserting ''Chief Medical Officer''; and

(C) in subsection (b)—

(i) in the matter preceding paragraph (1), by striking ''Under Secretary for Management, in coordination with the Chief Medical Officer,'' and inserting ''Chief Medical Officer''; and

(ii) in paragraph (3), by striking ''as deemed appropriate by the Under Secretary,'';

(7) by redesignating section 528 (6 U.S.C. 321q) as section 2303 and transferring such section to appear after section 2302, as so redesignated; and

(8) in section 2303(a), as so redesignated, by striking ''Assistant Secretary for the Countering Weapons of Mass Destruction Office'' and inserting ''Chief Medical Officer''.

(b) TRANSITION AND TRANSFERS.—

(1) TRANSITION.—The individual appointed pursuant to section 1931 of the Homeland Security Act of 2002 (6 U.S.C. 597) of the Department of Homeland Security, as in effect on the day before the date of enactment of this Act, and serving as the Chief Medical Officer of the Department of Homeland Security on the day before the date of enactment of this Act, shall continue to serve as the Chief Medical Officer of the Department on and after the date of enactment of this Act without the need for reappointment.

(2) RULE OF CONSTRUCTION.—The rule of construction described in section 2(hh) of the Presidential Appointment Efficiency and Streamlining Act of 2011 (5 U.S.C. 3132 note) shall not apply to the Chief Medical Officer of the Department of Homeland Security, including the incumbent who holds the position on the day before the date of enactment of this Act, and such officer shall be paid pursuant to section 3132(a)(2) or 5315 of title 5, United States Code.

(3) TRANSFER.—The Secretary of Homeland Security shall transfer to the Chief Medical Officer of the Department of Homeland Security—

(A) all functions, personnel, budget authority, and assets of the Under Secretary for Management relating to workforce health and safety, as in existence on the day before the date of enactment of this Act;

(B) all functions, personnel, budget authority, and assets of the Assistant Secretary for the Countering Weapons of Mass Destruction Office relating to the Chief Medical Officer, including the Medical Operations Directorate of the Countering Weapons of Mass Destruction Office, as in existence on the day before the date of enactment of this Act; and

(C) all functions, personnel, budget authority, and assets of the Assistant Secretary for the Countering Weapons of Mass Destruction Office associated with the efforts pertaining to the program coordination activities relating to defending the food, agriculture, and veterinary defenses of the Office, as in existence on the day before the date of enactment of this Act.

SEC. 5145. MEDICAL COUNTERMEASURES PROGRAM.

The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by redesignating section 1932 (6 U.S.C. 597a) as section 2304 and transferring such section to appear after section 2303, as so redesignated by section 5144 of this subtitle.

SEC. 5146. CONFIDENTIALITY OF MEDICAL QUALITY ASSURANCE RECORDS.

Title XXIII of the Homeland Security Act of 2002, as added by this chapter, is amended by adding at the end the following:

''SEC. 2305. CONFIDENTIALITY OF MEDICAL QUALITY ASSURANCE RECORDS.

''(a) DEFINITIONS.—In this section:

''(1) HEALTH CARE PROVIDER.—The term 'health care provider' means an individual who—

''(A) is—

''(i) an employee of the Department;

''(ii) a detailee to the Department from another Federal agency;

''(iii) a personal services contractor of the Department; or

''(iv) hired under a contract for services;

''(B) performs health care services as part of duties of the individual in that capacity; and

''(C) has a current, valid, and unrestricted license or certification—

''(i) that is issued by a State, the District of Columbia, or a commonwealth, territory, or possession of the United States; and

''(ii) that is for the practice of medicine, osteopathic medicine, dentistry, nursing, emergency medical services, or another health profession.

''(2) MEDICAL QUALITY ASSURANCE PROGRAM.—The term 'medical quality assurance program' means any activity carried out by the Department to assess the quality of medical care, including activities conducted by individuals, committees, or other review bodies responsible for quality assurance, credentials, infection control, incident reporting, the delivery, advisement, and oversight of direct patient care and assessment (including treatment procedures, blood, drugs, and therapeutics), medical records, health resources management review, and identification and prevention of medical, mental health, or dental incidents and risks.

''(3) MEDICAL QUALITY ASSURANCE RECORD OF THE DEPARTMENT.—The term 'medical quality assurance record of the Department' means all information, including the proceedings, records (including patient records that the Department creates and maintains as part of a system of records), minutes, and reports that—

''(A) emanate from quality assurance program activities described in paragraph (2); and

''(B) are produced or compiled by the Department as part of a medical quality assurance program.

''(b) CONFIDENTIALITY OF RECORDS.—A medical quality assurance record of the Department that is created as part of a medical quality assurance program—

''(1) is confidential and privileged; and

''(2) except as provided in subsection (d), may not be disclosed to any person or entity.

''(c) PROHIBITION ON DISCLOSURE AND TESTIMONY.—Except as otherwise provided in this section—

''(1) no part of any medical quality assurance record of the Department may be subject to discovery or admitted into evidence in any judicial or administrative proceeding; and

''(2) an individual who reviews or creates a medical quality assurance record of the Department or who participates in any proceeding that reviews or creates a medical quality assurance record of the Department may not be permitted or required to testify in any judicial or administrative proceeding with respect to the record or with respect to any finding, recommendation, evaluation, opinion, or action taken by that individual in connection with the record.

''(d) AUTHORIZED DISCLOSURE AND TESTIMONY.—

''(1) IN GENERAL.—Subject to paragraph (2), a medical quality assurance record of the Department may be disclosed, and a person described in subsection (c)(2) may give testimony in connection with the record, only as follows:

''(A) To a Federal agency or private organization, if the medical quality assurance record of the Department or testimony is needed by the Federal agency or private organization to—

''(i) perform licensing or accreditation functions related to Department health care facilities, a facility affiliated with the Department, or any other location authorized by the Secretary for the performance of health care services; or

''(ii) perform monitoring, required by law, of Department health care facilities, a facility affiliated with the Department, or any other location authorized by the Secretary for the performance of health care services.

''(B) To an administrative or judicial proceeding concerning an adverse action related to the credentialing of or health care provided by a present or former health care provider by the Department.

''(C) To a governmental board or agency or to a professional health care society or organization, if the medical quality assurance record of the Department or testimony is needed by the board, agency, society, or organization to perform licensing, credentialing, or the monitoring of professional standards with respect to any health care provider who is or was a health care provider for the Department.

''(D) To a hospital, medical center, or other institution that provides health care services, if the medical quality assurance record of the Department or testimony is needed by the institution to assess the professional qualifications of any health care provider who is or was a health care provider for the Department and who has applied for or been granted authority or employment to provide health care services in or on behalf of the institution.

''(E) To an employee, a detailee, or a contractor of the Department who has a need for the medical quality assurance record of the Department or testimony to perform official duties or duties within the scope of their contract.

''(F) To a criminal or civil law enforcement agency or instrumentality charged under applicable law with the protection of the public health or safety, if a qualified representative of the agency or instrumentality makes a written request that the medical quality assurance record of the Department or testimony be provided for a purpose authorized by law.

''(G) In an administrative or judicial proceeding commenced by a criminal or civil law enforcement agency or instrumentality described in subparagraph (F), but only with respect to the subject of the proceeding.

''(2) PERSONALLY IDENTIFIABLE INFORMATION.—

''(A) IN GENERAL.—With the exception of the subject of a quality assurance action, personally identifiable information of any person receiving health care services from the Department or of any other person associated with the Department for purposes of a medical quality assurance program that is disclosed in a medical quality assurance record of the Department shall be deleted from that record before any disclosure of the record is made outside the Department.

''(B) APPLICATION.—The requirement under subparagraph (A) shall not apply to the release of information that is permissible under section 552a of title 5, United States Code (commonly known as the 'Privacy Act of 1974').

''(e) DISCLOSURE FOR CERTAIN PURPOSES.—Nothing in this section shall be construed—

''(1) to authorize or require the withholding from any person or entity aggregate statistical information regarding the results of medical quality assurance programs; or

''(2) to authorize the withholding of any medical quality assurance record of the Department from a committee of either House of Congress, any joint committee of Congress, or the Comptroller General of the United States if the record pertains to any matter within their respective jurisdictions.

''(f) PROHIBITION ON DISCLOSURE OF INFORMATION, RECORD, OR TESTIMONY.—A person or entity having possession of or access to a medical quality assurance record of the Department or testimony described in this section may not disclose the contents of the record or testimony in any manner or for any purpose except as provided in this section.

''(g) EXEMPTION FROM FREEDOM OF INFORMATION ACT.—A medical quality assurance record of the Department shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the 'Freedom of Information Act').

''(h) LIMITATION ON CIVIL LIABILITY.—A person who participates in the review or creation of, or provides information to a person or body that reviews or creates, a medical quality assurance record of the Department shall not be civilly liable for that participation or for providing that information if the participation or provision of information was provided in good faith based on prevailing professional standards at the time the medical quality assurance program activity took place.

''(i) APPLICATION TO INFORMATION IN CERTAIN OTHER RECORDS.—Nothing in this section shall be construed as limiting access to the information in a record created and maintained outside a medical quality assurance program, including the medical record of a patient, on the grounds that the information was presented during meetings of a review body that are part of a medical quality assurance program.

''(j) PENALTY.—Any person who willfully discloses a medical quality assurance record of the Department other than as provided in this section, knowing that the record is a medical quality assurance record of the Department shall be fined not more than $3,000 in the case of a first offense and not more than $20,000 in the case of a subsequent offense.

''(k) RELATIONSHIP TO COAST GUARD.—The requirements of this section shall not apply to any medical quality assurance record of the Department that is created by or for the Coast Guard as part of a medical quality assurance program.''.

SEC. 5147. PORTABILITY OF LICENSURE.

(a) TRANSFER.—Section 16005 of the CARES Act (6 U.S.C. 320 note) is redesignated as section 2306 of the Homeland Security Act of 2002 and transferred so as to appear after section 2305, as added by section 5146 of this subtitle.

(b) REPEAL.—Section 2306 of the Homeland Security Act of 2002, as so redesignated by subsection (a), is amended by striking subsection (c).

SEC. 5148. TECHNICAL AND CONFORMING AMENDMENTS.

The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) in the table of contents in section 1(b) (Public Law 107–296; 116 Stat. 2135)—

(A) by striking the items relating to sections 528 and 529 and inserting the following:

''Sec. 528. Transfer of equipment during a public health emergency.'';

(B) by striking the items relating to sections 710, 711, 712, and 713 and inserting the following:

''Sec. 710. Employee engagement.
''Sec. 711. Annual employee award program.
''Sec. 712. Acquisition professional career program.'';

(C) by inserting after the item relating to section 1928 the following:

''Sec. 1929. Accountability.'';

(D) by striking the items relating to subtitle C of title XIX and sections 1931 and 1932; and

(E) by adding at the end the following:

''TITLE XXIII—OFFICE OF HEALTH SECURITY

''Sec. 2301. Office of Health Security.
''Sec. 2302. Workforce health and safety.
''Sec. 2303. Coordination of Department of Homeland Security efforts related to food, agriculture, and veterinary defense against terrorism.

''Sec. 2304. Medical countermeasures.
''Sec. 2305. Confidentiality of medical quality assurance records.
''Sec. 2306. Portability of licensure.'';

(2) by redesignating section 529 (6 U.S.C. 321r) as section 528;

(3) in section 704(e)(4) (6 U.S.C. 344(e)(4)), by striking ''section 711(a)'' and inserting ''section 710(a))'';

(4) by redesignating sections 711, 712, and 713 as sections 710, 711, and 712, respectively;

(5) in subsection (d)(3) of section 1923 (6 U.S.C. 592), as so redesignated by section 5142 of this Act—

(A) in the paragraph heading, by striking ''HAWAIIAN NATIVE-SERVING'' and inserting ''NATIVE HAWAIIAN-SERVING''; and

(B) by striking ''Hawaiian native-serving'' and inserting '' 'Native Hawaiian-serving'';

(6) by striking the subtitle heading for subtitle C of title XIX; and

(7) in section 2306, as so redesignated by section 5147 of this chapter—

(A) by inserting ''**PORTABILITY OF LICENSURE.**'' after ''2306.''; and

(B) in subsection (a), by striking ''(a) Notwithstanding'' and inserting the following:

''(a) IN GENERAL.—Notwithstanding''.

Subtitle F—Satellite Cybersecurity Act

SEC. 5151. SHORT TITLE.

This subtitle may be cited as the ''Satellite Cybersecurity Act''.

SEC. 5152. DEFINITIONS.

In this subtitle:

(1) CLEARINGHOUSE.—The term ''clearinghouse'' means the commercial satellite system cybersecurity clearinghouse required to be developed and maintained under section 5154(b)(1).

(2) COMMERCIAL SATELLITE SYSTEM.—The term ''commercial satellite system''—

(A) means a system that—

(i) is owned or operated by a non-Federal entity based in the United States; and

(ii) is composed of not less than 1 earth satellite; and

(B) includes—

(i) any ground support infrastructure for each satellite in the system; and

(ii) any transmission link among and between any satellite in the system and any ground support infrastructure in the system.

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

(4) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given the term in section 2200 of the Homeland Security Act of 2002, as added by section 5194 of this Act.

(5) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given the term in section 2200 of the Homeland Security Act of 2002, as added by section 5194 of this Act.

SEC. 5153. REPORT ON COMMERCIAL SATELLITE CYBERSECURITY.

(a) STUDY.—The Comptroller General of the United States shall conduct a study on the actions the Federal Government has taken to support the cybersecurity of commercial satellite systems, including as part of any action to address the cybersecurity of critical infrastructure sectors.

(b) REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall report 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 Space, Science, and Technology of the House of Representatives on the study conducted under subsection (a), which shall include information on—

(1) efforts of the Federal Government to—

(A) address or improve the cybersecurity of commercial satellite systems; and

(B) support related efforts with international entities or the private sector;

(2) the resources made available to the public by Federal agencies to address cybersecurity risks and threats to commercial satellite systems, including resources made available through the clearinghouse;

(3) the extent to which commercial satellite systems and the cybersecurity threats to such systems are addressed in Federal and non-Federal critical infrastructure risk analyses and protection plans;

(4) the extent to which Federal agencies are reliant on satellite systems owned wholly or in part or controlled by foreign entities, and how Federal agencies mitigate associated cybersecurity risks;

(5) the extent to which Federal agencies coordinate or duplicate authorities and take other actions focused on the cybersecurity of commercial satellite systems; and

(6) as determined appropriate by the Comptroller General of the United States, recommendations for further Federal action to support the cybersecurity of commercial satellite systems, including recommendations on information that should be shared through the clearinghouse.

(c) CONSULTATION.—In carrying out subsections (a) and (b), the Comptroller General of the United States shall coordinate with appropriate Federal agencies and organizations, including—

(1) the Department of Homeland Security;

(2) the Department of Commerce;

(3) the Department of Defense;

(4) the Department of Transportation;

(5) the Federal Communications Commission;

(6) the National Aeronautics and Space Administration;

(7) the National Executive Committee for Space-Based Positioning, Navigation, and Timing; and

(8) the National Space Council.

(d) BRIEFING.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall provide a briefing to the appropriate congressional committees on the study conducted under subsection (a).

(e) CLASSIFICATION.—The report made under subsection (b) shall be unclassified but may include a classified annex.

SEC. 5154. RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) DEFINITIONS.—In this section:

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

(2) SMALL BUSINESS CONCERN.—The term ''small business concern'' has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).

(b) ESTABLISHMENT OF COMMERCIAL SATELLITE SYSTEM CYBERSECURITY CLEARINGHOUSE.—

(1) IN GENERAL.—Subject to the availability of appropriations, not later than 180 days after the date of enactment of this Act, the Director shall develop and maintain a commercial satellite system cybersecurity clearinghouse.

(2) REQUIREMENTS.—The clearinghouse—

(A) shall be publicly available online;

(B) shall contain publicly available commercial satellite system cybersecurity resources, including the voluntary recommendations consolidated under subsection (c)(1);

(C) shall contain appropriate materials for reference by entities that develop, operate, or maintain commercial satellite systems;

(D) shall contain materials specifically aimed at assisting small business concerns with the secure development, operation, and maintenance of commercial satellite systems; and

(E) may contain controlled unclassified information distributed to commercial entities through a process determined appropriate by the Director.

(3) CONTENT MAINTENANCE.—The Director shall maintain current and relevant cybersecurity information on the clearinghouse.

(4) EXISTING PLATFORM OR WEBSITE.—To the extent practicable, the Director shall establish and maintain the clearinghouse using an online platform, a website, or a capability in existence as of the date of enactment of this Act.

(c) CONSOLIDATION OF COMMERCIAL SATELLITE SYSTEM CYBERSECURITY RECOMMENDATIONS.—

(1) IN GENERAL.—The Director shall consolidate voluntary cybersecurity recommendations designed to assist in the development, maintenance, and operation of commercial satellite systems.

(2) REQUIREMENTS.—The recommendations consolidated under paragraph (1) shall include materials appropriate for a public resource addressing the following:

(A) Risk-based, cybersecurity-informed engineering, including continuous monitoring and resiliency.

(B) Planning for retention or recovery of positive control of commercial satellite systems in the event of a cybersecurity incident.

(C) Protection against unauthorized access to vital commercial satellite system functions.

(D) Physical protection measures designed to reduce the vulnerabilities of a commercial satellite system's command, control, and telemetry receiver systems.

(E) Protection against jamming, eavesdropping, hijacking, computer network exploitation, spoofing, threats to optical satellite communications, and electromagnetic pulse.

(F) Security against threats throughout a commercial satellite system's mission lifetime.

(G) Management of supply chain risks that affect the cybersecurity of commercial satellite systems.

(H) Protection against vulnerabilities posed by ownership of commercial satellite systems or commercial satellite system companies by foreign entities.

(I) Protection against vulnerabilities posed by locating physical infrastructure, such as satellite ground control systems, in foreign countries.

(J) As appropriate, and as applicable pursuant to the maintenance requirement under subsection (b)(3), relevant findings and recommendations from the study conducted by the Comptroller General of the United States under section 5153(a).

(K) Any other recommendations to ensure the confidentiality, availability, and integrity of data residing on or in transit through commercial satellite systems.

(d) IMPLEMENTATION.—In implementing this section, the Director shall—

(1) to the extent practicable, carry out the implementation in partnership with the private sector;

(2) coordinate with—

(A) the National Space Council and the head of any other agency determined appropriate by the National Space Council; and

(B) the heads of appropriate Federal agencies with expertise and experience in satellite operations, including the entities described in section 5153(c) to enable the alignment of Federal efforts on commercial satellite system cybersecurity and, to the extent practicable, consistency in Federal recommendations relating to commercial satellite system cybersecurity; and

(3) consult with non-Federal entities developing commercial satellite systems or otherwise supporting the cybersecurity of commercial satellite systems, including private, consensus organizations that develop relevant standards.

(e) SUNSET AND REPORT.—

(1) IN GENERAL.—This section shall cease to have force or effect on the date that is 7 years after the date of the enactment of this Act.

(2) REPORT.—Not later than 6 years after the date of enactment of this Act, the Director 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 Space, Science, and Technology of the House of Representatives a report summarizing—

(A) any partnership with the private sector described in subsection (d)(1);

(B) any consultation with a non-Federal entity described in subsection (d)(3);

(C) the coordination carried out pursuant to subsection (d)(2);

(D) the establishment and maintenance of the clearinghouse pursuant to subsection (b);

(E) the recommendations consolidated pursuant to subsection (c)(1); and

(F) any feedback received by the Director on the clearinghouse from non-Federal entities.

SEC. 5155. STRATEGY.

Not later than 120 days after the date of the enactment of this Act, the National Space Council, in coordination with the Director of the Office of Space Commerce and the heads of other relevant agencies, shall submit to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Space, Science, and Technology and the Committee on Homeland Security of the House of Representatives a strategy for the activities of Federal agencies to address and improve the cybersecurity of commercial satellite systems, which shall include an identification of—

(1) proposed roles and responsibilities for relevant agencies; and

(2) as applicable, the extent to which cybersecurity threats to such systems are addressed in Federal and non-Federal critical infrastructure risk analyses and protection plans.

SEC. 5156. RULES OF CONSTRUCTION.

Nothing in this subtitle shall be construed to—

(1) designate commercial satellite systems or other space assets as a critical infrastructure sector; or

(2) infringe upon or alter the authorities of the agencies described in section 5153(c).

Subtitle G—Pray Safe Act

SEC. 5161. SHORT TITLE.

This subtitle may be cited as the ''Pray Safe Act''.

SEC. 5162. DEFINITIONS.

In this subtitle—

(1) the term ''Clearinghouse'' means the Federal Clearinghouse on Safety Best Practices for Faith-Based Organizations and Houses of Worship established under section 2220E of the Homeland Security Act of 2002, as added by section 5163 of this subtitle;

(2) the term ''Department'' means the Department of Homeland Security;

(3) the terms ''faith-based organization'' and ''house of worship'' have the meanings given such terms under section 2220E of the Homeland Security Act of 2002, as added by section 5163 of this subtitle; and

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

SEC. 5163. FEDERAL CLEARINGHOUSE ON SAFETY AND SECURITY BEST PRACTICES FOR FAITH-BASED ORGANIZATIONS AND HOUSES OF WORSHIP.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following:

''SEC. 2220E. FEDERAL CLEARINGHOUSE ON SAFETY AND SECURITY BEST PRACTICES FOR FAITH-BASED ORGANIZATIONS AND HOUSES OF WORSHIP.

''(a) DEFINITIONS.—In this section—

''(1) the term 'Clearinghouse' means the Clearinghouse on Safety and Security Best Practices for Faith-Based Organizations and Houses of Worship established under subsection (b)(1);

''(2) the term 'faith-based organization' means a group, center, or nongovernmental organization with a religious, ideological, or spiritual motivation, character, affiliation, or purpose;

''(3) the term 'house of worship' means a place or building, including synagogues, mosques, temples, and churches, in which congregants practice their religious or spiritual beliefs; and

''(4) the term 'safety and security', for the purpose of the Clearinghouse, means prevention of, protection against, or recovery from threats, including manmade disasters, natural disasters, or violent attacks.

''(b) ESTABLISHMENT.—

''(1) IN GENERAL.—Not later than 270 days after the date of enactment of the Pray Safe Act, the Secretary, in consultation with the Attorney General, the Executive Director of the White House Office of Faith-Based and Neighborhood Partnerships, and the head of any other agency that the Secretary determines appropriate, shall establish a Federal Clearinghouse on Safety and Security Best Practices for Faith-Based Organizations and Houses of Worship within the Department.

''(2) PURPOSE.—The Clearinghouse shall be the primary resource of the Federal Government—

''(A) to educate and publish online best practices and recommendations for safety and security for faith-based organizations and houses of worship; and

''(B) to provide information relating to Federal grant programs available to faith-based organizations and houses of worship.

''(3) PERSONNEL.—

''(A) ASSIGNMENTS.—The Clearinghouse shall be assigned such personnel and resources as the Secretary considers appropriate to carry out this section.

''(B) DETAILEES.—The Secretary may coordinate detailees as required for the Clearinghouse.

''(C) DESIGNATED POINT OF CONTACT.—There shall be not less than 1 employee assigned or detailed to the Clearinghouse who shall be the designated point of contact to provide information and assistance to faith-based organizations and houses of worship, including assistance relating to the grant program established under section 5165 of the Pray Safe Act. The contact information of the designated point of contact shall be made available on the website of the Clearinghouse.

''(D) QUALIFICATION.—To the maximum extent possible, any personnel assigned or detailed to the Clearinghouse under this paragraph should be familiar with faith-based organizations and houses of worship and with physical and online security measures to identify and prevent safety and security risks.

''(c) CLEARINGHOUSE CONTENTS.—

''(1) EVIDENCE-BASED TIERS.—

''(A) IN GENERAL.—The Secretary, in consultation with the Attorney General, the Executive Director of the White House Office of Faith-Based and Neighborhood Partnerships, and the head of any other agency that the Secretary determines appropriate, shall develop tiers for determining evidence-based practices that demonstrate a significant effect on improving safety or security, or both, for faith-based organizations and houses of worship.

''(B) REQUIREMENTS.—The tiers required to be developed under subparagraph (A) shall—

''(i) prioritize—

''(I) strong evidence from not less than 1 well-designed and well-implemented experimental study; and

''(II) moderate evidence from not less than 1 well-designed and well-implemented quasi-experimental study; and

''(ii) consider promising evidence that demonstrates a rationale based on high-quality research findings or positive evaluations that such activity, strategy, or intervention is likely to improve security and promote safety for faith-based organizations and houses of worship.

''(2) CRITERIA FOR BEST PRACTICES AND RECOMMENDATIONS.—The best practices and recommendations of the Clearinghouse shall, at a minimum—

''(A) identify areas of concern for faith-based organizations and houses of worship, including event planning recommendations, checklists, facility hardening, tabletop exercise resources, and other resilience measures;

''(B) involve comprehensive safety measures, including threat prevention, preparedness, protection, mitigation, incident response, and recovery to improve the safety posture of faith-based organizations and houses of worship upon implementation;

''(C) involve comprehensive safety measures, including preparedness, protection, mitigation, incident response, and recovery to improve the resiliency of faith-based organizations and houses of worship from manmade and natural disasters;

''(D) include any evidence or research rationale supporting the determination of the Clearinghouse that the best practices or recommendations under subparagraph (B) have been shown to have a significant effect on improving the safety and security of individuals in faith-based organizations and houses of worship, including—

''(i) findings and data from previous Federal, State, local, Tribal, territorial, private sector, and nongovernmental organization research centers relating to safety, security, and targeted violence at faith-based organizations and houses of worship; and

''(ii) other supportive evidence or findings relied upon by the Clearinghouse in determining best practices and recommendations to improve the safety and security posture of a faith-based organization or house of worship upon implementation; and

''(E) include an overview of the available resources the Clearinghouse can provide for faith-based organizations and houses of worship.

''(3) ADDITIONAL INFORMATION.—The Clearinghouse shall maintain and make available a comprehensive index of all Federal grant programs for which faith-based organizations and houses of worship are eligible, which shall include the performance metrics for each grant management that the recipient will be required to provide.

''(4) PAST RECOMMENDATIONS.—To the greatest extent practicable, the Clearinghouse shall identify and present, as appropriate, best practices and recommendations issued by Federal, State, local, Tribal, territorial, private sector, and nongovernmental organizations relevant to the safety and security of faith-based organizations and houses of worship.

''(d) ASSISTANCE AND TRAINING.—The Secretary may produce and publish materials on the Clearinghouse to assist and train faith-based organizations, houses of worship, and law enforcement agencies on the implementation of the best practices and recommendations.

''(e) CONTINUOUS IMPROVEMENT.—

''(1) IN GENERAL.—The Secretary shall—

''(A) collect for the purpose of continuous improvement of the Clearinghouse—

''(i) Clearinghouse data analytics;

''(ii) user feedback on the implementation of resources, best practices, and recommendations identified by the Clearinghouse; and

''(iii) any evaluations conducted on implementation of the best practices and recommendations of the Clearinghouse; and

''(B) in coordination with the Faith-Based Security Advisory Council of the Department, the Department of Justice, the Executive Director of the White House Office of Faith-Based and Neighborhood Partnerships, and any other agency that the Secretary determines appropriate—

''(i) assess and identify Clearinghouse best practices and recommendations for which there are no resources available through Federal Government programs for implementation;

''(ii) provide feedback on the implementation of best practices and recommendations of the Clearinghouse; and

''(iii) propose additional recommendations for best practices for inclusion in the Clearinghouse; and

''(C) not less frequently than annually, examine and update the Clearinghouse in accordance with—

''(i) the information collected under subparagraph (A); and

''(ii) the recommendations proposed under subparagraph (B)(iii).

''(2) ANNUAL REPORT TO CONGRESS.—The Secretary shall submit to Congress, on an annual basis, a report on the updates made to the Clearinghouse during the preceding 1-year period under paragraph (1)(C), which shall include a description of any changes made to the Clearinghouse.''.

(b) TECHNICAL 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—

(1) by moving the item relating to section 2220D to appear after the item relating to section 2220C; and

(2) by inserting after the item relating to section 2220D the following:

''Sec. 2220E. Federal Clearinghouse on Safety Best Practices for Faith-Based Organizations and Houses of Worship.''.

SEC. 5164. NOTIFICATION OF CLEARINGHOUSE.

The Secretary shall provide written notification of the establishment of the Clearinghouse, with an overview of the resources required as described in section 2220E of the Homeland Security Act of 2002, as added by section 5163 of this subtitle, and section 5165 of this subtitle, to—

(1) every State homeland security advisor;

(2) every State department of homeland security;

(3) other Federal agencies with grant programs or initiatives that aid in the safety and security of faith-based organizations and houses of worship, as determined appropriate by the Secretary;

(4) every Federal Bureau of Investigation Joint Terrorism Task Force;

(5) every Homeland Security Fusion Center;

(6) every State or territorial Governor or other chief executive;

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

(8) the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives.

SEC. 5165. GRANT PROGRAM OVERVIEW.

(a) DHS GRANTS AND RESOURCES.—The Secretary shall include a grants program overview on the website of the Clearinghouse that shall—

(1) be the primary location for all information regarding Department grant programs that are open to faith-based organizations and houses of worship;

(2) directly link to each grant application and any applicable user guides;

(3) identify all safety and security homeland security assistance programs managed by the Department that may be used to implement best practices and recommendation of the Clearinghouse;

(4) annually, and concurrent with the application period for any grant identified under paragraph (1), provide information related to the required elements of grant applications to aid smaller faith based organizations and houses of worship in earning access to Federal grants; and

(5) provide frequently asked questions and answers for the implementation of best practices and recommendations of the Clearinghouse and best practices for applying for a grant identified under paragraph (1).

(b) OTHER FEDERAL GRANTS AND RESOURCES.—Each Federal agency notified under section 5164(3) shall provide necessary information on any Federal grant programs or resources of the Federal agency that are available for faith-based organizations and houses of worship to the Secretary or the appropriate point of contact for the Clearinghouse.

(c) STATE GRANTS AND RESOURCES.—

(1) IN GENERAL.—Any State notified under paragraph (1), (2), or (6) of section 5164 may provide necessary information on any grant programs or resources of the State available for faith-based organizations and houses of worship to the Secretary or the appropriate point of contact for the Clearinghouse.

(2) IDENTIFICATION OF RESOURCES.—The Clearinghouse shall, to the extent practicable, identify, for each State—

(A) each agency responsible for safety for faith-based organizations and houses of worship in the State, or any State that does not have such an agency designated;

(B) any grant program that may be used for the purposes of implementing best practices and recommendations of the Clearinghouse; and

(C) any resources or programs, including community prevention or intervention efforts, that may be used to assist in targeted violence and terrorism prevention.

SEC. 5166. OTHER RESOURCES.

The Secretary shall, on the website of the Clearinghouse, include a separate section for other resources that shall provide a centralized list of all available points of contact to seek assistance in grant applications and in carrying out the best practices and recommendations of the Clearinghouse, including—

(1) a list of contact information to reach Department personnel to assist with grant-related questions;

(2) the applicable Cybersecurity and Infrastructure Security Agency contact information to connect houses of worship with Protective Security Advisors;

(3) contact information for all Department Fusion Centers, listed by State;

(4) information on the If you See Something Say Something Campaign of the Department; and

(5) any other appropriate contacts.

SEC. 5167. RULE OF CONSTRUCTION.

Nothing in this subtitle or the amendments made by this subtitle shall be construed to create, satisfy, or waive any requirement under Federal civil rights laws, including—

(1) title II of the Americans With Disabilities Act of 1990 (42 U.S.C. 12131 et seq.); or

(2) title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.).

SEC. 5168. EXEMPTION.

Chapter 35 of title 44, United States Code (commonly known as the ''Paperwork Reduction Act'') shall not apply to any rulemaking or information collection required under this subtitle or under section 2220E of the Homeland Security Act of 2002, as added by section 5163 of this subtitle.

Subtitle H—Invent Here, Make Here for Homeland Security Act

SEC. 5171. SHORT TITLE.

This subtitle may be cited as the ''Invent Here, Make Here for Homeland Security Act''.

SEC. 5172. PREFERENCE FOR UNITED STATES INDUSTRY.

Section 308 of the Homeland Security Act of 2002 (6 U.S.C. 188) is amended by adding at the end the following:

''(d) PREFERENCE FOR UNITED STATES INDUSTRY.—

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

''(A) COUNTRY OF CONCERN.—The term 'country of concern' means a country that—

''(i) is a covered nation, as that term is defined in section 4872(d) of title 10, United States Code; or

''(ii) the Secretary determines is engaged in conduct that is detrimental to the national security of the United States.

''(B) FUNDING AGREEMENT; NONPROFIT ORGANIZATION; SUBJECT INVENTION.—The terms 'funding agreement', 'nonprofit organization', and 'subject invention' have the meanings given those terms in section 201 of title 35, United States Code.

''(C) MANUFACTURED SUBSTANTIALLY IN THE UNITED STATES.—The term 'manufactured substantially in the United States' means manufactured substantially from all articles, materials, or supplies mined, produced, or manufactured in the United States.

''(D) RELEVANT CONGRESSIONAL COMMITTEES.—The term 'relevant congressional committees' means—

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

''(ii) the Committee on Homeland Security of the House of Representatives.

''(2) PREFERENCE.—Subject to the other provisions of this subsection, no firm or nonprofit organization which receives title to any subject invention developed under a funding agreement entered into with the Department and no assignee of any such firm or nonprofit organization shall grant the exclusive right to use or sell any subject invention unless the products embodying the subject invention or produced through the use of the subject invention will be manufactured substantially in the United States.

''(3) WAIVERS.—

''(A) IN GENERAL.—Subject to subparagraph (B), in individual cases, the requirement for an agreement described in paragraph (2) may be waived by the Secretary upon a showing by the firm, nonprofit organization, or assignee that reasonable but unsuccessful efforts have been made to grant licenses on

similar terms to potential licensees that would be likely to manufacture substantially in the United States or that under the circumstances domestic manufacture is not commercially feasible.

''(B) CONDITIONS ON WAIVERS GRANTED BY DEPARTMENT.—

''(i) BEFORE GRANT OF WAIVER.—Before granting a waiver under subparagraph (A), the Secretary shall—

''(I) consult with the relevant congressional committees regarding the decision of the Secretary to grant the waiver; and

''(II) comply with the procedures developed and implemented pursuant to section 70923(b)(2) of the Build America, Buy America Act (subtitle A of title IX of division G of Public Law 117–58).

''(ii) PROHIBITION ON GRANTING CERTAIN WAIVERS.—The Secretary may not grant a waiver under subparagraph (A) if, as a result of the waiver, products embodying the applicable subject invention, or produced through the use of the applicable subject invention, will be manufactured substantially in a country of concern.''.

Subtitle I—DHS Joint Task Forces Reauthorization

SEC. 5181. SHORT TITLE.

This subtitle may be cited as the ''DHS Joint Task Forces Reauthorization Act of 2022''.

SEC. 5182. SENSE OF THE SENATE.

It is the sense of the Senate that the Department of Homeland Security should consider using the authority under subsection (b) of section 708 of the Homeland Security Act of 2002 (6 U.S.C. 348(b)) to create a Joint Task Force described in such subsection to improve coordination and response to the number of encounters and amount of seizures of illicit narcotics along the southwest border.

SEC. 5183. AMENDING SECTION 708 OF THE HOMELAND SECURITY ACT OF 2002.

Section 708(b) of the Homeland Security Act of 2002 (6 U.S.C. 348(b)) is amended—

(1) by striking paragraph (8) and inserting the following:

''(8) JOINT TASK FORCE STAFF.—

''(A) IN GENERAL.—Each Joint Task Force shall have a staff, composed of officials from relevant components and offices of the Department, to assist the Director of that Joint Task Force in carrying out the mission and responsibilities of that Joint Task Force.

''(B) REPORT.—The Secretary shall include in the report submitted under paragraph (6)(F)—

''(i) the number of personnel permanently assigned to each Joint Task Force by each component and office; and

''(ii) the number of personnel assigned on a temporary basis to each Joint Task Force by each component and office.'';

(2) in paragraph (9)—

(A) in the heading, by inserting ''STRATEGY AND OF'' after ''ESTABLISHMENT OF'';

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

''(A) using leading practices in performance management and lessons learned by other law enforcement task forces and joint operations, establish a strategy for each Joint Task Force that contains—

''(i) the mission of each Joint Task Force and strategic goals and objectives to assist the Joint Task Force in accomplishing that mission; and

''(ii) outcome-based and other appropriate performance metrics to evaluate the effectiveness of each Joint Task Force and measure progress towards the goals and objectives described in clause (i), which include—

''(I) targets for current and future fiscal years; and

''(II) a description of the methodology used to establish those metrics and any limitations with respect to data or information used to assess performance;'';

(C) in subparagraph (B)—

(i) by striking ''enactment of this section'' and insert ''enactment of the DHS Joint Task Forces Reauthorization Act of 2022'';

(ii) by inserting ''strategy and'' after ''Senate the''; and

(iii) by striking the period at the end and inserting ''; and''; and

(D) by striking subparagraph (C) and inserting the following:

''(C) beginning not later than 1 year after the date of enactment of the DHS Joint Task Forces Reauthorization Act of 2022, submit annually to each committee specified in subparagraph (B) a report that—

''(i) contains the evaluation described in subparagraphs (A) and (B); and

''(ii) outlines the progress in implementing outcome-based and other performance metrics referred to in subparagraph (A)(ii).'';

(3) in paragraph (11)(A), by striking the period at the end and inserting the following: '', which shall include—

''(i) the justification, focus, and mission of the Joint Task Force; and

''(ii) a strategy for the conduct of the Joint Task Force, including goals and performance metrics for the Joint Task Force.'';

(4) in paragraph (12)—

(A) in subparagraph (A), by striking ''January 31, 2018, and January 31, 2021, the Inspector General of the Department'' and inserting ''1 year after the date of enactment of the DHS Joint Task Forces Reauthorization Act of 2022, the Comptroller General of the United States''; and

(B) in subparagraph (B), by striking clauses (i) and (ii) and inserting the following:

''(i) an assessment of the structure of each Joint Task Force;

''(ii) an assessment of the effectiveness of oversight over each Joint Task Force;

''(iii) an assessment of the strategy of each Joint Task Force; and

''(iv) an assessment of staffing levels and resources of each Joint Task Force.''; and

(5) in paragraph (13), by striking ''2022'' and inserting ''2024''.

Subtitle J—Other Provisions

CHAPTER 1—DEEPFAKE TASK FORCE

SEC. 5191 SHORT TITLE.

This chapter may be cited as the ''Deepfake Task Force Act''.

SEC. 5192. NATIONAL DEEPFAKE AND DIGITAL PROVENANCE TASK FORCE.

(a) DEFINITIONS.—In this section:

(1) DIGITAL CONTENT FORGERY.—The term ''digital content forgery'' means audio, visual, or text content fabricated or manipulated with the intent to mislead and be indistinguishable from reality, created through the use of technologies, including those that apply artificial intelligence techniques such as generative adversarial networks.

(2) DIGITAL CONTENT PROVENANCE.—The term ''digital content provenance'' means the verifiable chronology of the origin and history of a piece of digital content, such as an image, video, audio recording, or electronic document.

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

(A) a private sector or nonprofit organization; or

(B) an institution of higher education.

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

(5) RELEVANT CONGRESSIONAL COMMITTEES.—The term ''relevant congressional committees'' means—

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

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

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

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

(E) the Committee on the Judiciary of the Senate; and

(F) the Committee on the Judiciary of the House of Representatives.

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

(7) TASK FORCE.—The term ''Task Force'' means the National Deepfake and Provenance Task Force established under subsection (b)(1).

(b) ESTABLISHMENT OF TASK FORCE.—

(1) ESTABLISHMENT.—The Secretary, in coordination with the Administrator of the National Telecommunications and Information Administration, shall establish a task force, to be known as ''the National Deepfake Provenance Task Force'', to—

(A) investigate the feasibility of, and obstacles to, developing and deploying standards and technologies for determining digital content provenance;

(B) propose policy changes to reduce the proliferation and impact of digital content forgeries, such as the adoption of digital content provenance and technology standards;

(C) serve as a formal mechanism for interagency coordination and information sharing to facilitate the creation and implementation of a national strategy to address the growing threats posed by digital content forgeries; and

(D) investigate existing digital content forgery generation technologies, potential detection methods, and disinformation mitigation solutions.

(2) MEMBERSHIP.—

(A) CHAIRPERSON.—The Secretary, or a designee of the Secretary, shall serve as chairperson of the Task Force.

(B) COMPOSITION.—The Task Force shall be composed of not fewer than 13 members, of whom—

(i) not fewer than 5 shall be representatives from the Federal Government, including the chairperson of the Task Force, the Director of the National Institute of Standards and Technology, and the Administrator of the National Telecommunications and Information Administration;

(ii) not fewer than 4 shall be representatives from institutions of higher education; and

(iii) not fewer than 4 shall be representatives from private or nonprofit organizations.

(C) APPOINTMENT.—Not later than 120 days after the date of enactment of this Act, the chairperson of the Task Force shall appoint members to the Task Force in accordance with subparagraph (B) from among technical experts in—

(i) artificial intelligence;

(ii) media manipulation;

(iii) digital forensics;

(iv) secure digital content and delivery;

(v) cryptography;

(vi) privacy;

(vii) civil rights; or

(viii) related subjects.

(D) TERM OF APPOINTMENT.—The term of a member of the Task Force shall end on the date described in subsection (g)(1).

(E) VACANCY.—Any vacancy occurring in the membership of the Task Force shall be filled in the same manner in which the original appointment was made.

(F) EXPENSES FOR NON-FEDERAL MEMBERS.—Members of the Task Force described in clauses (ii) and (iii) of subparagraph (B) shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for employees under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Task Force.

(c) COORDINATED PLAN.—

(1) IN GENERAL.—The Task Force shall develop a coordinated plan to—

(A) reduce the proliferation and impact of digital content forgeries, including by exploring how the adoption of a digital content provenance standard could assist with reducing the proliferation of digital content forgeries;

(B) develop mechanisms for content creators to—

(i) cryptographically certify the authenticity of original media and non-deceptive manipulations; and

(ii) enable the public to validate the authenticity of original media and non-deceptive manipulations to establish digital content provenance; and

(C) increase the ability of internet companies, journalists, watchdog organizations, other relevant entities, and members of the public to meaningfully scrutinize and identify potential digital content forgeries.

(2) CONTENTS.—The plan required under paragraph (1) shall include the following:

(A) A Government-wide research and development agenda to—

(i) improve technologies and systems to detect digital content forgeries; and

(ii) relay information about digital content provenance to content consumers.

(B) An assessment of the feasibility of, and obstacles to, the deployment of technologies and systems to capture, preserve, and display digital content provenance.

(C) A framework for conceptually distinguishing between digital content with benign or helpful alternations and digital content forgeries.

(D) An assessment of the technical feasibility of, and challenges in, distinguishing between—

(i) benign or helpful alterations to digital content; and

(ii) intentionally deceptive or obfuscating alterations to digital content.

(E) A discussion of best practices, including any necessary standards, for the adoption and effective use of technologies and systems to determine digital content provenance and detect digital content forgeries while protecting fair use.

(F) Conceptual proposals for necessary research projects and experiments to further develop successful technology to ascertain digital content provenance.

(G) Proposed policy changes, including changes in law, to—

(i) incentivize the adoption of technologies, systems, open standards, or other means to detect digital content forgeries and determine digital content provenance; and

(ii) reduce the incidence, proliferation, and impact of digital content forgeries.

(H) Recommendations for models for public-private partnerships to fight disinformation and reduce digital content forgeries, including partnerships that support and collaborate on—

(i) industry practices and standards for determining digital content provenance;

(ii) digital literacy education campaigns and user-friendly detection tools for the public to reduce the proliferation and impact of disinformation and digital content forgeries;

(iii) industry practices and standards for documenting relevant research and progress in machine learning; and

(iv) the means and methods for identifying and addressing the technical and financial infrastructure that supports the proliferation of digital content forgeries, such as inauthentic social media accounts and bank accounts.

(I) An assessment of privacy and civil liberties requirements associated with efforts to deploy technologies and systems to determine digital content provenance or reduce the proliferation of digital content forgeries, including statutory or other proposed policy changes.

(J) A determination of metrics to define the success of—

(i) technologies or systems to detect digital content forgeries;

(ii) technologies or systems to determine digital content provenance; and

(iii) other efforts to reduce the incidence, proliferation, and impact of digital content forgeries.

(d) CONSULTATIONS.—In carrying out subsection (c), the Task Force shall consult with the following:

(1) The Director of the National Science Foundation.

(2) The National Academies of Sciences, Engineering, and Medicine.

(3) The Director of the National Institute of Standards and Technology.

(4) The Director of the Defense Advanced Research Projects Agency.

(5) The Director of the Intelligence Advanced Research Projects Activity of the Office of the Director of National Intelligence.

(6) The Secretary of Energy.

(7) The Secretary of Defense.

(8) The Attorney General.

(9) The Secretary of State.

(10) The Federal Trade Commission.

(11) The United States Trade Representative.

(12) Representatives from private industry and nonprofit organizations.

(13) Representatives from institutions of higher education.

(14) Such other individuals as the Task Force considers appropriate.

(e) STAFF.—

(1) IN GENERAL.—Staff of the Task Force shall be comprised of detailees with expertise in artificial intelligence or related fields from—

(A) the Department of Homeland Security;

(B) the National Telecommunications and Information Administration;

(C) the National Institute of Standards and Technology; or

(D) any other Federal agency the chairperson of the Task Force consider appropriate with the consent of the head of the Federal agency.

(2) OTHER ASSISTANCE.—

(A) IN GENERAL.—The chairperson of the Task Force may enter into an agreement with an eligible entity for the temporary assignment of employees of the eligible entity to the Task Force in accordance with this paragraph.

(B) APPLICATION OF ETHICS RULES.—An employee of an eligible entity assigned to the Task Force under subparagraph (A)—

(i) shall be considered a special Government employee for the purpose of Federal law, including—

(I) chapter 11 of title 18, United States Code; and

(II) the Ethics in Government Act of 1978 (5 U.S.C. App.); and

(ii) notwithstanding section 202(a) of title 18, United States Code, may be assigned to the Task Force for a period of not more than 2 years.

(C) FINANCIAL LIABILITY.—An agreement entered into with an eligible entity under subparagraph (A) shall require the eligible entity to be responsible for any costs associated with the assignment of an employee to the Task Force.

(D) TERMINATION.—The chairperson of the Task Force may terminate the assignment of an employee to the Task Force under subparagraph (A) at any time and for any reason.

(f) TASK FORCE REPORTS.—

(1) INTERIM REPORT.—

(A) IN GENERAL.—Not later than 1 year after the date on which all of the appointments have been made under subsection (b)(2)(C), the Task Force shall submit to the President and the relevant congressional committees an interim report containing the findings, conclusions, and recommendations of the Task Force.

(B) CONTENTS.—The report required under subparagraph (A) shall include specific recommendations for ways to reduce the proliferation and impact of digital content forgeries, including the deployment of technologies and systems to determine digital content provenance.

(2) FINAL REPORT.—Not later than 180 days after the date of the submission of the interim report under paragraph (1)(A), the Task Force shall submit to the President and the relevant congressional committees a final report containing the findings, conclusions, and recommendations of the Task Force, including the plan developed under subsection (c).

(3) REQUIREMENTS.—With respect to each report submitted under this subsection—

(A) the Task Force shall make the report publicly available; and

(B) the report—

(i) shall be produced in an unclassified form; and

(ii) may include a classified annex.

(g) TERMINATION.—

(1) IN GENERAL.—The Task Force shall terminate on the date that is 90 days after the date on which the Task Force submits the final report under subsection (f)(2).

(2) RECORDS.—Upon the termination of the Task Force under paragraph (1), each record of the Task Force shall become a record of the National Archives and Records Administration.

CHAPTER 2—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS

SEC. 5194. CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS.

(a) TECHNICAL AMENDMENT RELATING TO DOTGOV ACT OF 2020.—

(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).

(b) CONSOLIDATION OF DEFINITIONS.—

(1) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) 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) 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—

''(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.

''(6) 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.

''(7) 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.

''(8) 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.

''(9) 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.

''(10) 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.

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

''(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 an interference, a compromise, or an 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) 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.

''(18) 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.

''(19) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

''(20) 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.

''(21) 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.

''(22) 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.

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

(2) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(A) by amending section 2201 (6 U.S.C. 651) to read as follows:

''SEC. 2201. DEFINITION.

''In this subtitle, the term 'Cybersecurity Advisory Committee' means the advisory committee established under section 2219(a).'';

(B) in section 2202 (6 U.S.C. 652)—

(i) in subsection (a)(1), by striking ''(in this subtitle referred to as the Agency)'';

(ii) in subsection (b)(1), by striking ''in this subtitle referred to as the 'Director')''; and

(iii) in subsection (f)—

(I) in paragraph (1), by inserting ''Executive'' before ''Assistant Director''; and

(II) in paragraph (2), by inserting ''Executive'' before ''Assistant Director'';

(C) in section 2209 (6 U.S.C. 659)—

(i) by striking subsection (a);

(ii) by redesignating subsections (b) through subsection (o) as subsections (a) through (n), respectively;

(iii) in subsection (c)(1), as so redesignated—

(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'';

(iv) 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'';

(v) in subsection (j), as so redesignated, by striking ''subsection (c)(8)'' and inserting ''subsection (b)(8)'';

(vi) by redesignating the first subsections (p) and (q) and second subsections (p) and (q) as subsections (o) and (p) and subsections (q) and (r), respectively; and

(vii) in subsection (o), 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)'';

(D) in section 2210 (6 U.S.C. 660)—

(i) by striking subsection (a);

(ii) by redesignating subsections (b) through (e) as subsections (a) through (d), respectively;

(iii) 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

(iv) in subsection (c), as so redesignated, by striking ''subsection (c)'' and inserting ''subsection (b)'';

(E) in section 2211 (6 U.S.C. 661), by striking subsection (h);

(F) in section 2212 (6 U.S.C. 662), by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations'';

(G) in section 2213 (6 U.S.C. 663)—

(i) by striking subsection (a);

(ii) by redesignating subsections (b) through (f) as subsections (a) through (e), respectively;

(iii) in subsection (b), as so redesignated, by striking ''subsection (b)'' each place it appears and inserting ''subsection (a)'';

(iv) in subsection (c), as so redesignated, in the matter preceding paragraph (1), by striking ''subsection (b)'' and inserting ''subsection (a)''; and

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

(I) in paragraph (1)—

(aa) in the matter preceding subparagraph (A), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(bb) in subparagraph (A), by striking ''subsection (c)(1)'' and inserting ''subsection (b)(1)''; and

(cc) 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)'';

(H) in section 2216 (6 U.S.C. 665b)—

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

(ii) 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.'';

(I) in section 2218(c)(4)(A) (6 U.S.C. 665d(4)(A)), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(J) in section 2220A (6 U.S.C. 665g)—

(i) in subsection (a)—

(I) by striking paragraphs (1), (2), (5), and (6); and

(II) by redesignating paragraphs (3), (4), (7), (8), (9), (10), (11), and (12) as paragraphs (1) through (8), respectively;

(ii) in subsection (e)(2)(B)(xiv)(II)(aa), by striking ''information sharing and analysis organization'' and inserting ''Information Sharing and Analysis Organization'';

(iii) in subsection (p), by striking ''appropriate committees of Congress'' and inserting ''appropriate congressional committees''; and

(iv) in subsection (q)(4), in the matter preceding clause (i), by striking ''appropriate committees of Congress'' and inserting ''appropriate congressional committees''

(K) in section 2220C(f) (6 U.S.C. 665i(f))—

(i) by striking paragraph (1);

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

(iii) in paragraph (2), as so redesignated, by striking ''(enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501(9))'' and inserting ''(6 U.S.C. 1501)''; and

(L) in section 2222 (6 U.S.C. 671)—

(i) by striking paragraphs (3), (5), and (8);

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

(iii) by redesignating paragraphs (6) and (7) as paragraphs (4) and (5), respectively.

(3) 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—

(A) by inserting before the item relating to subtitle A of title XXII the following:

''Sec. 2200. Definitions.''; and

(B) by striking the item relating to section 2201 and insert the following:

''Sec. 2201. Definition.''.

(4) CYBERSECURITY ACT OF 2015 DEFINITIONS.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(A) 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.'';

(B) 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

(C) 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.''.

(c) ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.—

(1) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

(A) in section 222 (6 U.S.C. 1521)—

(i) in paragraph (2), by striking ''section 2210'' and inserting ''section 2200''; and

(ii) in paragraph (4), by striking ''section 2209'' and inserting ''section 2200'';

(B) 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)'';

(C) in section 226 (6 U.S.C. 1524)—

(i) 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

(ii) in subsection (c)(1)(A)(vi), by striking ''section 2213(c)(5)'' and inserting ''section 2213(b)(5)''; and

(D) in section 227(b) (6 U.S.C. 1525(b)), by striking ''section 2213(d)(2)'' and inserting ''section 2213(c)(2)''.

(2) 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))''.

(3) 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—

(A) in subsection (a)—

(i) by striking paragraph (5);

(ii) by redesignating paragraphs (6) and (7) as paragraphs (5) and (6), respectively;

(iii) 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.'';

(B) in subsection (c)(3)(B), by striking ''section 2201(5)'' and inserting ''section 2200''; and

(C) in subsection (d), by striking ''section 2215 of the Homeland Security Act of 2002, as added by this section'' and inserting ''section 2218 of the Homeland Security Act of 2002 (6 U.S.C. 665d)''.

(4) NATIONAL SECURITY ACT OF 1947.—Section 113B(b)(4) 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)''.

(5) IoT CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c(b)(3)) 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

(6) 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''.

(7) 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''.

CHAPTER 3—POST-DISASTER MENTAL HEALTH RESPONSE ACT

SEC. 5198. POST-DISASTER MENTAL HEALTH RESPONSE.

(a) SHORT TITLE.—This section may be cited as the ''Post-Disaster Mental Health Response Act''.

(b) CRISIS COUNSELING ASSISTANCE AND TRAINING.—Section 502(a)(6) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5192(a)(6)) is amended by inserting ''and section 416'' after ''section 408''.

TITLE LII—GOVERNMENTAL AFFAIRS

Subtitle A—Safeguarding American Innovation

SEC. 5201. SHORT TITLE.

This title may be cited as the ''Safeguarding American Innovation Act''.

SEC. 5202. FEDERAL RESEARCH SECURITY COUNCIL.

(a) IN GENERAL.—Subtitle V of title 31, United States Code, is amended by adding at the end the following:

''CHAPTER 79—FEDERAL RESEARCH SECURITY COUNCIL

''Sec.
''7901. Definitions.
''7902. Federal Research Security Council establishment and membership.
''7903. Functions and authorities.
''7904. Annual report.
''7905. Requirements for Executive agencies.

''§ 7901. Definitions

''In this chapter:

''(1) 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 Commerce, Science, and Transportation of the Senate;

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

''(D) the Committee on Foreign Relations of the Senate;

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

''(F) the Committee on Health, Education, Labor, and Pensions of the Senate;

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

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

''(I) the Committee on Energy and Commerce of the House of Representatives;

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

''(K) the Committee on Foreign Affairs of the House of Representatives;

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

''(M) the Committee on Science, Space, and Technology of the House of Representatives; and

''(N) the Committee on Education and Labor of the House of Representatives.

''(2) COUNCIL.—The term 'Council' means the Federal Research Security Council established under section 7902(a).

''(3) EXECUTIVE AGENCY.—The term 'Executive agency' has the meaning given that term in section 105 of title 5.

''(4) FEDERAL RESEARCH SECURITY RISK.—The term 'Federal research security risk' means the risk posed by malign state actors and other persons to the security and integrity of research and development conducted using research and development funds awarded by Executive agencies.

''(5) INSIDER.—The term 'insider' means any person with authorized access to any United States Government resource, including personnel, facilities, information, research, equipment, networks, or systems.

''(6) INSIDER THREAT.—The term 'insider threat' means the threat that an insider will use his or her authorized access (wittingly or unwittingly) to harm the national and economic security of the United States or negatively affect the integrity of a Federal agency's normal processes, including damaging the United States through espionage, sabotage, terrorism, unauthorized disclosure of national security information or nonpublic information, a destructive act (which may include physical harm to another in the workplace), or through the loss or degradation of departmental resources, capabilities, and functions.

''(7) RESEARCH AND DEVELOPMENT.—

''(A) IN GENERAL.—The term 'research and development' means all research activities, both basic and applied, and all development activities.

''(B) DEVELOPMENT.—The term 'development' means experimental development.

''(C) EXPERIMENTAL DEVELOPMENT.—The term 'experimental development' means creative and systematic work, drawing upon knowledge gained from research and practical experience, which—

''(i) is directed toward the production of new products or processes or improving existing products or processes; and

''(ii) like research, will result in gaining additional knowledge.

''(D) RESEARCH.—The term 'research'—

''(i) means a systematic study directed toward fuller scientific knowledge or understanding of the subject studied; and

''(ii) includes activities involving the training of individuals in research techniques if such activities—

''(I) utilize the same facilities as other research and development activities; and

''(II) are not included in the instruction function.

''(8) UNITED STATES RESEARCH COMMUNITY.—The term 'United States research community' means—

''(A) research and development centers of Executive agencies;

''(B) private research and development centers in the United States, including for profit and nonprofit research institutes;

''(C) research and development centers at institutions of higher education (as defined in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)));

''(D) research and development centers of States, United States territories, Indian tribes, and municipalities;

''(E) government-owned, contractor-operated United States Government research and development centers; and

''(F) any person conducting federally funded research or receiving Federal research grant funding.

''§ 7902. Federal Research Security Council establishment and membership

''(a) ESTABLISHMENT.—There is established, in the Office of Management and Budget, a Federal Research Security Council, which shall develop federally funded research and development grant making policy and management guidance to protect the national and economic security interests of the United States.

''(b) MEMBERSHIP.—

''(1) IN GENERAL.—The following agencies shall be represented on the Council:

''(A) The Office of Management and Budget.

''(B) The Office of Science and Technology Policy.

''(C) The Department of Defense.

''(D) The Department of Homeland Security.

''(E) The Office of the Director of National Intelligence.

''(F) The Department of Justice.

''(G) The Department of Energy.

''(H) The Department of Commerce.

''(I) The Department of Health and Human Services.

''(J) The Department of State.

''(K) The Department of Transportation.

''(L) The National Aeronautics and Space Administration.

''(M) The National Science Foundation.

''(N) The Department of Education.

''(O) The Small Business Administration.

''(P) The Council of Inspectors General on Integrity and Efficiency.

''(Q) Other Executive agencies, as determined by the Chairperson of the Council.

''(2) LEAD REPRESENTATIVES.—

''(A) DESIGNATION.—Not later than 45 days after the date of the enactment of the Safeguarding American Innovation Act, the head of each agency represented on the Council shall designate a representative of that agency as the lead representative of the agency on the Council.

''(B) FUNCTIONS.—The lead representative of an agency designated under subparagraph (A) shall ensure that appropriate personnel, including leadership and subject matter experts of the agency, are aware of the business of the Council.

''(c) CHAIRPERSON.—

''(1) DESIGNATION.—Not later than 45 days after the date of the enactment of the Safeguarding American Innovation Act, the Director of the Office of Management and Budget shall designate a senior level official from the Office of Management and Budget to serve as the Chairperson of the Council.

''(2) FUNCTIONS.—The Chairperson shall perform functions that include—

''(A) subject to subsection (d), developing a schedule for meetings of the Council;

''(B) designating Executive agencies to be represented on the Council under subsection (b)(1)(Q);

''(C) in consultation with the lead representative of each agency represented on the Council, developing a charter for the Council; and

''(D) not later than 7 days after completion of the charter, submitting the charter to the appropriate congressional committees.

''(3) LEAD SCIENCE ADVISOR.—The Director of the Office of Science and Technology Policy shall designate a senior level official to be the lead science advisor to the Council for purposes of this chapter.

''(4) LEAD SECURITY ADVISOR.—The Director of the National Counterintelligence and Security Center shall designate a senior level official from the National Counterintelligence and Security Center to be the lead security advisor to the Council for purposes of this chapter.

''(d) MEETINGS.—The Council shall meet not later than 60 days after the date of the enactment of the Safeguarding American Innovation Act and not less frequently than quarterly thereafter.

''§ 7903. Functions and authorities

''(a) DEFINITIONS.—In this section:

''(1) IMPLEMENTING.—The term 'implementing' means working with the relevant Federal agencies, through existing processes and procedures, to enable those agencies to put in place and enforce the measures described in this section.

''(2) UNIFORM APPLICATION PROCESS.—The term 'uniform application process' means a process employed by Federal science agencies to maximize the collection of information regarding applicants and applications, as determined by the Council.

''(b) IN GENERAL.—The Chairperson of the Council shall consider the missions and responsibilities of Council members in determining the lead agencies for Council functions. The Council shall perform the following functions:

''(1) Developing and implementing, across all Executive agencies that award research and development grants, awards, and contracts, a uniform application process for grants in accordance with subsection (c).

''(2) Developing and implementing policies and providing guidance to prevent malign foreign interference from unduly influencing the peer review process for federally funded research and development.

''(3) Identifying or developing criteria for sharing among Executive agencies and with law enforcement and other agencies, as appropriate, information regarding individuals who violate disclosure policies and other policies related to research security.

''(4) Identifying an appropriate Executive agency—

''(A) to accept and protect information submitted by Executive agencies and non-Federal entities based on the process established pursuant to paragraph (1); and

''(B) to facilitate the sharing of information received under subparagraph (A) to support, consistent with Federal law—

''(i) the oversight of federally funded research and development;

''(ii) criminal and civil investigations of misappropriated Federal funds, resources, and information; and

''(iii) counterintelligence investigations.

''(5) Identifying, as appropriate, Executive agencies to provide—

''(A) shared services, such as support for conducting Federal research security risk assessments, activities to mitigate such risks, and oversight and investigations with respect to grants awarded by Executive agencies; and

''(B) common contract solutions to support the verification of the identities of persons participating in federally funded research and development.

''(6) Identifying and issuing guidance, in accordance with subsection (e) and in coordination with the National Insider Threat Task Force established by Executive Order 13587 (50 U.S.C. 3161 note) for expanding the scope of Executive agency insider threat programs, including the safeguarding of research and development from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels and the distinct needs, missions, and systems of each such agency.

''(7) Identifying and issuing guidance for developing compliance and oversight programs for Executive agencies to ensure that research and development grant recipients accurately report conflicts of interest and conflicts of commitment in accordance with subsection (c)(1). Such programs shall include an assessment of—

''(A) a grantee's support from foreign sources and affiliations, appointments, or participation in talent programs with foreign funding institutions or laboratories; and

''(B) the impact of such support and affiliations, appointments, or participation in talent programs on United States national security and economic interests.

''(8) Providing guidance to Executive agencies regarding appropriate application of consequences for violations of disclosure requirements.

''(9) Developing and implementing a cross-agency policy and providing guidance related to the use of digital persistent identifiers for individual researchers supported by, or working on, any Federal research grant with the goal to enhance transparency and security, while reducing administrative burden for researchers and research institutions.

''(10) Engaging with the United States research community in conjunction with the National Science and Technology Council and the National Academies Science, Technology and Security Roundtable created under section 1746 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 42 U.S.C. 6601 note) in performing the functions described in paragraphs (1), (2), and (3) and with respect to issues relating to Federal research security risks.

''(11) Carrying out such other functions, consistent with Federal law, that are necessary to reduce Federal research security risks.

''(c) REQUIREMENTS FOR UNIFORM GRANT APPLICATION PROCESS.—In developing the uniform application process for Federal research and development grants required under subsection (b)(1), the Council shall—

''(1) ensure that the process—

''(A) requires principal investigators, co-principal investigators, and key personnel associated with the proposed Federal research or development grant project—

''(i) to disclose biographical information, all affiliations, including any foreign military, foreign government-related organizations, and foreign-funded institutions, and all current and pending support, including from foreign institutions, foreign governments, or foreign laboratories, and all support received from foreign sources; and

''(ii) to certify the accuracy of the required disclosures under penalty of perjury; and

''(B) uses a machine-readable application form to assist in identifying fraud and ensuring the eligibility of applicants;

''(2) design the process—

''(A) to reduce the administrative burden on persons applying for Federal research and development funding; and

''(B) to promote information sharing across the United States research community, while safeguarding sensitive information; and

''(3) complete the process not later than 1 year after the date of the enactment of the Safeguarding American Innovation Act.

''(d) REQUIREMENTS FOR INFORMATION SHARING CRITERIA.—In identifying or developing criteria and procedures for sharing information with respect to Federal research security risks under subsection (b)(3), the Council shall ensure that such criteria address, at a minimum—

''(1) the information to be shared;

''(2) the circumstances under which sharing is mandated or voluntary;

''(3) the circumstances under which it is appropriate for an Executive agency to rely on information made available through such sharing in exercising the responsibilities and authorities of the agency under applicable laws relating to the award of grants;

''(4) the procedures for protecting intellectual capital that may be present in such information; and

''(5) appropriate privacy protections for persons involved in Federal research and development.

''(e) REQUIREMENTS FOR INSIDER THREAT PROGRAM GUIDANCE.—In identifying or developing guidance with respect to insider threat programs under subsection (b)(6), the Council shall ensure that such guidance provides for, at a minimum—

''(1) such programs—

''(A) to deter, detect, and mitigate insider threats; and

''(B) to leverage counterintelligence, security, information assurance, and other relevant functions and resources to identify and counter insider threats; and

''(2) the development of an integrated capability to monitor and audit information for the detection and mitigation of insider threats, including through—

''(A) monitoring user activity on computer networks controlled by Executive agencies;

''(B) providing employees of Executive agencies with awareness training with respect to insider threats and the responsibilities of employees to report such threats;

''(C) gathering information for a centralized analysis, reporting, and response capability; and

''(D) information sharing to aid in tracking the risk individuals may pose while moving across programs and affiliations;

''(3) the development and implementation of policies and procedures under which the insider threat program of an Executive agency accesses, shares, and integrates information and data derived from offices within the agency and shares insider threat information with the executive agency research sponsors;

''(4) the designation of senior officials with authority to provide management, accountability, and oversight of the insider threat program of an Executive agency and to make resource recommendations to the appropriate officials; and

''(5) such additional guidance as is necessary to reflect the distinct needs, missions, and systems of each Executive agency.

''(f) ISSUANCE OF WARNINGS RELATING TO RISKS AND VULNERABILITIES IN INTERNATIONAL SCIENTIFIC COOPERATION.—

''(1) IN GENERAL.—The Council, in conjunction with the lead security advisor designated under section 7902(c)(4), shall establish a process for informing members of the United States research community and the public, through the issuance of warnings described in paragraph (2), of potential risks and vulnerabilities in international scientific cooperation that may undermine the integrity and security of the United States research community or place at risk any federally funded research and development.

''(2) CONTENT.—A warning described in this paragraph shall include, to the extent the Council considers appropriate, a description of—

''(A) activities by the national government, local governments, research institutions, or universities of a foreign country—

''(i) to exploit, interfere, or undermine research and development by the United States research community; or

''(ii) to misappropriate scientific knowledge resulting from federally funded research and development;

''(B) efforts by strategic competitors to exploit the research enterprise of a foreign country that may place at risk—

''(i) the science and technology of that foreign country; or

''(ii) federally funded research and development; and

''(C) practices within the research enterprise of a foreign country that do not adhere to the United States scientific values of openness, transparency, reciprocity, integrity, and merit-based competition.

''(g) EXCLUSION ORDERS.—To reduce Federal research security risk, the Interagency Suspension and Debarment Committee shall provide quarterly reports to the Director of the Office of Management and Budget and the Director of the Office of Science and Technology Policy that detail—

''(1) the number of ongoing investigations by Council Members related to Federal research security that may result, or have resulted, in agency pre-notice letters, suspensions, proposed debarments, and debarments;

''(2) Federal agencies' performance and compliance with interagency suspensions and debarments;

''(3) efforts by the Interagency Suspension and Debarment Committee to mitigate Federal research security risk;

''(4) proposals for developing a unified Federal policy on suspensions and debarments; and

''(5) other current suspension and debarment related issues.

''(h) SAVINGS PROVISION.—Nothing in this section may be construed—

''(1) to alter or diminish the authority of any Federal agency; or

''(2) to alter any procedural requirements or remedies that were in place before the date of the enactment of the Safeguarding American Innovation Act.

''§ 7904. Annual report

''Not later than November 15 of each year, the Chairperson of the Council shall submit a report to the appropriate congressional committees that describes the activities of the Council during the preceding fiscal year.

''§ 7905. Requirements for Executive agencies

''(a) IN GENERAL.—The head of each Executive agency on the Council shall be responsible for—

''(1) assessing Federal research security risks posed by persons participating in federally funded research and development;

''(2) avoiding or mitigating such risks, as appropriate and consistent with the standards, guidelines, requirements, and practices identified by the Council under section 7903(b);

''(3) prioritizing Federal research security risk assessments conducted under paragraph (1) based on the applicability and relevance of the research and development to the national security and economic competitiveness of the United States;

''(4) ensuring that initiatives impacting Federally funded research grant making policy and management to protect the national and economic security interests of the United States are integrated with the activities of the Council; and

''(5) ensuring that the initiatives of the Council comply with title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.).

''(b) INCLUSIONS.—The responsibility of the head of an Executive agency for assessing Federal research security risk described in subsection (a) includes—

''(1) developing an overall Federal research security risk management strategy and implementation plan and policies and processes to guide and govern Federal research security risk management activities by the Executive agency;

''(2) integrating Federal research security risk management practices throughout the lifecycle of the grant programs of the Executive agency;

''(3) sharing relevant information with other Executive agencies, as determined appropriate by the Council in a manner consistent with section 7903; and

''(4) reporting on the effectiveness of the Federal research security risk management strategy of the Executive agency consistent with guidance issued by the Office of Management and Budget and the Council.''.

(b) CLERICAL AMENDMENT.—The table of chapters at the beginning of title 31, United States Code, is amended by inserting after the item relating to chapter 77 the following:

''79. Federal Research Security Council ..... 7901.''.

SEC. 5203. FEDERAL GRANT APPLICATION FRAUD.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''§ 1041. Federal grant application fraud

''(a) DEFINITIONS.—In this section:

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

''(2) FEDERAL GRANT.—The term 'Federal grant'—

''(A) means a grant awarded by a Federal agency;

''(B) includes a subgrant awarded by a non-Federal entity to carry out a Federal grant program; and

''(C) does not include—

''(i) direct United States Government cash assistance to an individual;

''(ii) a subsidy;

''(iii) a loan;

''(iv) a loan guarantee; or

''(v) insurance.

''(3) FEDERAL GRANT APPLICATION.—The term 'Federal grant application' means an application for a Federal grant.

''(4) FOREIGN COMPENSATION.—The term 'foreign compensation' means a title, monetary compensation, access to a laboratory or other resource, or other benefit received from—

''(A) a foreign government;

''(B) a foreign government institution; or

''(C) a foreign public enterprise.

''(5) FOREIGN GOVERNMENT.—The term 'foreign government' includes a person acting or purporting to act on behalf of—

''(A) a faction, party, department, agency, bureau, subnational administrative entity, or military of a foreign country; or

''(B) a foreign government or a person purporting to act as a foreign government, regardless of whether the United States recognizes the government.

''(6) FOREIGN GOVERNMENT INSTITUTION.—The term 'foreign government institution' means a foreign entity owned by, subject to the control of, or subject to regulation by a foreign government.

''(7) FOREIGN PUBLIC ENTERPRISE.—The term 'foreign public enterprise' means an enterprise over which a foreign government directly or indirectly exercises a dominant influence.

''(8) LAW ENFORCEMENT AGENCY.—The term 'law enforcement agency'—

''(A) means a Federal, State, local, or Tribal law enforcement agency; and

''(B) includes—

''(i) the Office of Inspector General of an establishment (as defined in section 12 of the Inspector General Act of 1978 (5 U.S.C. App.)) or a designated Federal entity (as defined in section 8G(a) of the Inspector General Act of 1978 (5 U.S.C. App.)); and

''(ii) the Office of Inspector General, or similar office, of a State or unit of local government.

''(9) OUTSIDE COMPENSATION.—The term 'outside compensation' means any compensation, resource, or support (regardless of monetary value) made available to the applicant in support of, or related to, any research endeavor, including a title, research grant, cooperative agreement, contract, institutional award, access to a laboratory, or other resource, including materials, travel compensation, or work incentives.

''(b) PROHIBITION.—It shall be unlawful for any individual to knowingly—

''(1) prepare or submit a Federal grant application that fails to disclose the receipt of any outside compensation, including foreign compensation, by the individual, the value of which is not less than $1,000;

''(2) forge, counterfeit, or otherwise falsify a document for the purpose of obtaining a Federal grant; or

''(3) prepare, submit, or assist in the preparation or submission of a Federal grant application or document in connection with a Federal grant application that—

''(A) contains a material false statement;

''(B) contains a material misrepresentation; or

''(C) fails to disclose a material fact.

''(c) EXCEPTION.—Subsection (b) does not apply to an activity—

''(1) carried out in connection with a lawfully authorized investigative, protective, or intelligence activity of—

''(A) a law enforcement agency; or

''(B) a Federal intelligence agency; or

''(2) authorized under chapter 224.

''(d) PENALTY.—Any individual who violates subsection (b)—

''(1) shall be fined in accordance with this title, imprisoned for not more than 5 years, or both, in accordance with the level of severity of that individual's violation of subsection (b); and

''(2) shall be prohibited from receiving a Federal grant during the 5-year period beginning on the date on which a sentence is imposed on the individual under paragraph (1).''.

(b) CLERICAL AMENDMENT.—The analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Federal grant application fraud.''.

SEC. 5204. RESTRICTING THE ACQUISITION OF EMERGING TECHNOLOGIES BY CERTAIN ALIENS.

(a) IN GENERAL.—The Secretary of State may impose the sanctions described in subsection (c) if the Secretary determines an alien is seeking to enter the United States to knowingly acquire sensitive or emerging technologies to undermine national security interests of the United States by benefitting an adversarial foreign government's security or strategic capabilities.

(b) RELEVANT FACTORS.—To determine whether to impose sanctions under subsection (a), the Secretary of State shall—

(1) take account of information and analyses relevant to implementing subsection (a) from the Office of the Director of National Intelligence, the Department of Health and Human Services, the Department of Defense, the Department of Homeland Security, the Department of Energy, the Department of Commerce, and other appropriate Federal agencies;

(2) take account of the continual expert assessments of evolving sensitive or emerging technologies that foreign adversaries are targeting;

(3) take account of relevant information concerning the foreign person's employment or collaboration, to the extent known, with—

(A) foreign military and security related organizations that are adversarial to the United States;

(B) foreign institutions involved in the theft of United States research;

(C) entities involved in export control violations or the theft of intellectual property;

(D) a government that seeks to undermine the integrity and security of the United States research community; or

(E) other associations or collaborations that pose a national security threat based on intelligence assessments; and

(4) weigh the proportionality of risks and the factors listed in paragraphs (1) through (3).

(c) SANCTIONS DESCRIBED.—The sanctions described in this subsection are the following:

(1) INELIGIBILITY FOR VISAS AND ADMISSION TO THE UNITED STATES.—An alien described in subsection (a) may be—

(A) inadmissible to the United States;

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

(C) 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.).

(2) CURRENT VISAS REVOKED.—

(A) IN GENERAL.—An alien described in subsection (a) is subject to revocation of any visa or other entry documentation regardless of when the visa or other entry documentation is or was issued.

(B) IMMEDIATE EFFECT.—A revocation under clause (A) shall take effect immediately, and automatically cancel any other valid visa or entry documentation that is in the alien's possession, in accordance with section 221(i) of the Immigration and Nationality Act.

(3) EXCEPTION TO COMPLY WITH INTERNATIONAL OBLIGATIONS.—The sanctions described in this subsection shall not apply with respect to an alien if admitting or paroling the alien into the United States is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations.

(d) REPORTING REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, and semi-annually thereafter until the sunset date set forth in subsection (f), the Secretary of State, in coordination with the Director of National Intelligence, the Director of the Office of Science and Technology Policy, the Secretary of Homeland Security, the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the heads of other appropriate Federal agencies, shall submit a report to the Committee on the Judiciary of the Senate, the Committee on Foreign Relations of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Oversight and Reform of the House of Representatives that identifies—

(1) any criteria, if relevant used to describe the alien in subsection (a);

(2) the number of individuals determined to be subject to sanctions under subsection (a), including the nationality of each such individual and the reasons for each sanctions determination; and

(3) the number of days from the date of the consular interview until a final decision is issued for each application for a visa considered under this section, listed by applicants' country of citizenship and relevant consulate.

(e) CLASSIFICATION OF REPORT.—Each report required under subsection (d) shall be submitted, to the extent practicable, in an unclassified form, but may be accompanied by a classified annex.

(f) SUNSET.—This section shall cease to be effective on the date that is 2 years after the date of the enactment of this Act.

Subtitle B—Intragovernmental Cybersecurity Information Sharing Act

SEC. 5211. REQUIREMENT FOR INFORMATION SHARING AGREEMENTS.

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

(b) APPROPRIATE OFFICIALS DEFINED.—In this section, the term ''appropriate officials'' means—

(1) the Majority Leader, Minority Leader, and the Secretary of the Senate with respect to an agreement with the Sergeant at Arms and Doorkeeper of the Senate; and

(2) the Speaker, the Minority Leader, and the Sergeant at Arms of the House of Representatives with respect to an agreement with the Chief Administrative Officer of the House of Representatives.

(c) REQUIREMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the President, the Sergeant at Arms and Doorkeeper of the Senate, and the Chief Administrative Officer of the House of Representatives, in consultation with appropriate officials, shall enter into 1 or more cybersecurity information sharing agreements to enhance collaboration between the executive branch and Congress on implementing cybersecurity measures to improve the protection of legislative branch information technology.

(2) DELEGATION.—If the President delegates the duties under paragraph (1), the designee of the President shall coordinate with appropriate Executive agencies (as defined in section 105 of title 5, United States Code, including the Executive Office of the President) and appropriate officers in the executive branch in entering any agreement described in paragraph (1).

(d) ELEMENTS.—The parties to a cybersecurity information sharing agreement under subsection (c) shall jointly develop such elements of the agreement as the parties find appropriate, which may include—

(1) direct and timely sharing of technical indicators and contextual information on cyber threats and vulnerabilities, and the means for such sharing;

(2) direct and timely sharing of classified and unclassified reports on cyber threats and activities consistent with the protection of sources and methods;

(3) seating of cybersecurity personnel of the Office of the Sergeant at Arms and Doorkeeper of the Senate or the Office of the Chief Administrative Officer of the House of Representatives at cybersecurity operations centers; and

(4) any other elements the parties find appropriate.

(e) BRIEFING TO CONGRESS.—Not later than 210 days after the date of enactment of this Act, and periodically thereafter, the President shall brief the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate, the Committee on Homeland Security and the Committee on House Administration of the House of Representatives, and appropriate officials on the status of the implementation of the agreements required under subsection (c).

Subtitle C—Improving Government for America's Taxpayers

SEC. 5221. GOVERNMENT ACCOUNTABILITY OFFICE UNIMPLEMENTED PRIORITY RECOMMENDATIONS.

The Comptroller General of the United States shall, as part of the Comptroller General's annual reporting to committees of Congress—

(1) consolidate Matters for Congressional Consideration from the Government Accountability Office in one report organized by policy topic that includes the amount of time such Matters have been unimplemented and submit such report to congressional leadership and the oversight committees of each House;

(2) with respect to the annual letters sent by the Comptroller General to individual agency heads and relevant congressional committees on the status of unimplemented priority recommendations, identify any additional congressional oversight actions that can help agencies implement such priority recommendations and address any underlying issues relating to such implementation;

(3) make publicly available the information described in paragraphs (1) and (2); and

(4) publish any known costs of unimplemented priority recommendations, if applicable.

Subtitle D—Advancing American AI Act

SEC. 5231. SHORT TITLE.

This subtitle may be cited as the ''Advancing American AI Act''.

SEC. 5232. PURPOSES.

The purposes of this subtitle are to—

(1) encourage agency artificial intelligence-related programs and initiatives that enhance the competitiveness of the United States and foster an approach to artificial intelligence that builds on the strengths of the United States in innovation and entrepreneurialism;

(2) enhance the ability of the Federal Government to translate research advances into artificial intelligence applications to modernize systems and assist agency leaders in fulfilling their missions;

(3) promote adoption of modernized business practices and advanced technologies across the Federal Government that align with the values of the United States, including the protection of privacy, civil rights, and civil liberties; and

(4) test and harness applied artificial intelligence to enhance mission effectiveness and business practice efficiency.

SEC. 5233. DEFINITIONS.

In this subtitle:

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

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

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

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

(3) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given the term in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note).

(4) ARTIFICIAL INTELLIGENCE SYSTEM.—The term ''artificial intelligence system''—

(A) means any data system, software, application, tool, or utility that operates in whole or in part using dynamic or static machine learning algorithms or other forms of artificial intelligence, whether—

(i) the data system, software, application, tool, or utility is established primarily for the purpose of researching, developing, or implementing artificial intelligence technology; or

(ii) artificial intelligence capability is integrated into another system or agency business process, operational activity, or technology system; and

(B) does not include any common commercial product within which artificial intelligence is embedded, such as a word processor or map navigation system.

(C)

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

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

SEC. 5234. PRINCIPLES AND POLICIES FOR USE OF ARTIFICIAL INTELLIGENCE IN GOVERNMENT.

(a) GUIDANCE.—The Director shall, when developing the guidance required under section 104(a) of the AI in Government Act of 2020 (title I of division U of Public Law 116–260), consider—

(1) the considerations and recommended practices identified by the National Security Commission on Artificial Intelligence in the report entitled ''Key Considerations for the Responsible Development and Fielding of AI'', as updated in April 2021;

(2) the principles articulated in Executive Order 13960 (85 Fed. Reg. 78939; relating to

promoting the use of trustworthy artificial intelligence in Government); and

(3) the input of—

(A) the Privacy and Civil Liberties Oversight Board;

(B) relevant interagency councils, such as the Federal Privacy Council, the Chief Information Officers Council, and the Chief Data Officers Council;

(C) other governmental and nongovernmental privacy, civil rights, and civil liberties experts; and

(D) any other individual or entity the Director determines to be appropriate.

(b) DEPARTMENT POLICIES AND PROCESSES FOR PROCUREMENT AND USE OF ARTIFICIAL INTELLIGENCE-ENABLED SYSTEMS.—Not later than 180 days after the date of enactment of this Act—

(1) the Secretary of Homeland Security, with the participation of the Chief Procurement Officer, the Chief Information Officer, the Chief Privacy Officer, and the Officer for Civil Rights and Civil Liberties of the Department and any other person determined to be relevant by the Secretary of Homeland Security, shall issue policies and procedures for the Department related to—

(A) the acquisition and use of artificial intelligence; and

(B) considerations for the risks and impacts related to artificial intelligence-enabled systems, including associated data of machine learning systems, to ensure that full consideration is given to—

(i) the privacy, civil rights, and civil liberties impacts of artificial intelligence-enabled systems; and

(ii) security against misuse, degradation, or rending inoperable of artificial intelligence-enabled systems; and

(2) the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department shall report to Congress on any additional staffing or funding resources that may be required to carry out the requirements of this subsection.

(c) INSPECTOR GENERAL.—Not later than 180 days after the date of enactment of this Act, the Inspector General of the Department shall identify any training and investments needed to enable employees of the Office of the Inspector General to continually advance their understanding of—

(1) artificial intelligence systems;

(2) best practices for governance, oversight, and audits of the use of artificial intelligence systems; and

(3) how the Office of the Inspector General is using artificial intelligence to enhance audit and investigative capabilities, including actions to—

(A) ensure the integrity of audit and investigative results; and

(B) guard against bias in the selection and conduct of audits and investigations.

(d) ARTIFICIAL INTELLIGENCE HYGIENE AND PROTECTION OF GOVERNMENT INFORMATION, PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES.—

(1) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with a working group consisting of members selected by the Director from appropriate interagency councils, shall develop an initial means by which to—

(A) ensure that contracts for the acquisition of an artificial intelligence system or service—

(i) align with the guidance issued to the head of each agency under section 104(a) of the AI in Government Act of 2020 (title I of division U of Public Law 116–260);

(ii) address protection of privacy, civil rights, and civil liberties;

(iii) address the ownership and security of data and other information created, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a contractor or subcontractor on behalf of the Federal Government; and

(iv) include considerations for securing the training data, algorithms, and other components of any artificial intelligence system against misuse, unauthorized alteration, degradation, or rendering inoperable; and

(B) address any other issue or concern determined to be relevant by the Director to ensure appropriate use and protection of privacy and Government data and other information.

(2) CONSULTATION.—In developing the considerations under paragraph (1)(A)(iv), the Director shall consult with the Secretary of Homeland Security, the Director of the National Institute of Standards and Technology, and the Director of National Intelligence.

(3) REVIEW.—The Director—

(A) should continuously update the means developed under paragraph (1); and

(B) not later than 2 years after the date of enactment of this Act and not less frequently than every 2 years thereafter, shall update the means developed under paragraph (1).

(4) BRIEFING.—The Director shall brief the appropriate congressional committees—

(A) not later than 90 days after the date of enactment of this Act and thereafter on a quarterly basis until the Director first implements the means developed under paragraph (1); and

(B) annually thereafter on the implementation of this subsection.

(5) SUNSET.—This subsection shall cease to be effective on the date that is 5 years after the date of enactment of this Act.

SEC. 5235. AGENCY INVENTORIES AND ARTIFICIAL INTELLIGENCE USE CASES.

(a) INVENTORY.—Not later than 60 days after the date of enactment of this Act, and continuously thereafter for a period of 5 years, the Director, in consultation with the Chief Information Officers Council, the Chief Data Officers Council, and other interagency bodies as determined to be appropriate by the Director, shall require the head of each agency to—

(1) prepare and maintain an inventory of the artificial intelligence use cases of the agency, including current and planned uses;

(2) share agency inventories with other agencies, to the extent practicable and consistent with applicable law and policy, including those concerning protection of privacy and of sensitive law enforcement, national security, and other protected information; and

(3) make agency inventories available to the public, in a manner determined by the Director, and to the extent practicable and in accordance with applicable law and policy, including those concerning the protection of privacy and of sensitive law enforcement, national security, and other protected information.

(b) CENTRAL INVENTORY.—The Director is encouraged to designate a host entity and ensure the creation and maintenance of an online public directory to—

(1) make agency artificial intelligence use case information available to the public and those wishing to do business with the Federal Government; and

(2) identify common use cases across agencies.

(c) SHARING.—The sharing of agency inventories described in subsection (a)(2) may be coordinated through the Chief Information Officers Council, the Chief Data Officers Council, the Chief Financial Officers Council, the Chief Acquisition Officers Council, or other interagency bodies to improve interagency coordination and information sharing for common use cases.

SEC. 5236. RAPID PILOT, DEPLOYMENT AND SCALE OF APPLIED ARTIFICIAL INTELLIGENCE CAPABILITIES TO DEMONSTRATE MODERNIZATION ACTIVITIES RELATED TO USE CASES.

(a) IDENTIFICATION OF USE CASES.—Not later than 270 days after the date of enactment of this Act, the Director, in consultation with the Chief Information Officers Council, the Chief Data Officers Council, and other interagency bodies as determined to be appropriate by the Director, shall identify 4 new use cases for the application of artificial intelligence-enabled systems to support interagency or intra-agency modernization initiatives that require linking multiple siloed internal and external data sources, consistent with applicable laws and policies, including those relating to the protection of privacy and of sensitive law enforcement, national security, and other protected information.

(b) PILOT PROGRAM.—

(1) PURPOSES.—The purposes of the pilot program under this subsection include—

(A) to enable agencies to operate across organizational boundaries, coordinating between existing established programs and silos to improve delivery of the agency mission; and

(B) to demonstrate the circumstances under which artificial intelligence can be used to modernize or assist in modernizing legacy agency systems.

(2) DEPLOYMENT AND PILOT.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the heads of relevant agencies and other officials as the Director determines to be appropriate, shall ensure the initiation of the piloting of the 4 new artificial intelligence use case applications identified under subsection (a), leveraging commercially available technologies and systems to demonstrate scalable artificial intelligence-enabled capabilities to support the use cases identified under subsection (a).

(3) RISK EVALUATION AND MITIGATION PLAN.—In carrying out paragraph (2), the Director shall require the heads of agencies to—

(A) evaluate risks in utilizing artificial intelligence systems; and

(B) develop a risk mitigation plan to address those risks, including consideration of—

(i) the artificial intelligence system not performing as expected;

(ii) the lack of sufficient or quality training data; and

(iii) the vulnerability of a utilized artificial intelligence system to unauthorized manipulation or misuse.

(4) PRIORITIZATION.—In carrying out paragraph (2), the Director shall prioritize modernization projects that—

(A) would benefit from commercially available privacy-preserving techniques, such as use of differential privacy, federated learning, and secure multiparty computing; and

(B) otherwise take into account considerations of civil rights and civil liberties.

(5) USE CASE MODERNIZATION APPLICATION AREAS.—Use case modernization application areas described in paragraph (2) shall include not less than 1 from each of the following categories:

(A) Applied artificial intelligence to drive agency productivity efficiencies in predictive supply chain and logistics, such as—

(i) predictive food demand and optimized supply;

(ii) predictive medical supplies and equipment demand and optimized supply; or

(iii) predictive logistics to accelerate disaster preparedness, response, and recovery.

(B) Applied artificial intelligence to accelerate agency investment return and address mission-oriented challenges, such as—

(i) applied artificial intelligence portfolio management for agencies;

(ii) workforce development and upskilling;

(iii) redundant and laborious analyses;

(iv) determining compliance with Government requirements, such as with grants management; or

(v) outcomes measurement to measure economic and social benefits.

(6) REQUIREMENTS.—Not later than 3 years after the date of enactment of this Act, the Director, in coordination with the heads of relevant agencies and other officials as the Director determines to be appropriate, shall establish an artificial intelligence capability within each of the 4 use case pilots under this subsection that—

(A) solves data access and usability issues with automated technology and eliminates or minimizes the need for manual data cleansing and harmonization efforts;

(B) continuously and automatically ingests data and updates domain models in near real-time to help identify new patterns and predict trends, to the extent possible, to help agency personnel to make better decisions and take faster actions;

(C) organizes data for meaningful data visualization and analysis so the Government has predictive transparency for situational awareness to improve use case outcomes;

(D) is rapidly configurable to support multiple applications and automatically adapts to dynamic conditions and evolving use case requirements, to the extent possible

(E) enables knowledge transfer and collaboration across agencies; and

(F) preserves intellectual property rights to the data and output for benefit of the Federal Government and agencies.

(c) BRIEFING.—Not earlier than 270 days but not later than 1 year after the date of enactment of this Act, and annually thereafter for 4 years, the Director shall brief the appropriate congressional committees on the activities carried out under this section and results of those activities.

(d) SUNSET.—The section shall cease to be effective on the date that is 5 years after the date of enactment of this Act.

SEC. 5237. ENABLING ENTREPRENEURS AND AGENCY MISSIONS.

(a) INNOVATIVE COMMERCIAL ITEMS.—Section 880 of the National Defense Authorization Act for Fiscal Year 2017 (41 U.S.C. 3301 note) is amended—

(1) in subsection (c), by striking ''$10,000,000'' and inserting ''$25,000,000'';

(2) by amending subsection (f) to read as follows:

''(f) DEFINITIONS.—In this section—

''(1) the term 'commercial product'—

''(A) has the meaning given the term 'commercial item' in section 2.101 of the Federal Acquisition Regulation; and

''(B) includes a commercial product or a commercial service, as defined in sections 103 and 103a, respectively, of title 41, United States Code; and

''(2) the term 'innovative' means—

''(A) any new technology, process, or method, including research and development; or

''(B) any new application of an existing technology, process, or method.''; and

(3) in subsection (g), by striking ''2022'' and insert ''2027''.

(b) DHS OTHER TRANSACTION AUTHORITY.—Section 831 of the Homeland Security Act of 2002 (6 U.S.C. 391) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking ''September 30, 2017'' and inserting ''September 30, 2024''; and

(B) by amending paragraph (2) to read as follows:

''(2) PROTOTYPE PROJECTS.—The Secretary—

''(A) may, under the authority of paragraph (1), carry out prototype projects under section 4022 of title 10, United States Code; and

''(B) in applying the authorities of such section 4022, the Secretary shall perform the functions of the Secretary of Defense as prescribed in such section.'';

(2) in subsection (c)(1), by striking ''September 30, 2017'' and inserting ''September 30, 2024''; and

(3) in subsection (d), by striking ''section 845(e)'' and all that follows and inserting ''section 4022(e) of title 10, United States Code.''.

(c) COMMERCIAL OFF THE SHELF SUPPLY CHAIN RISK MANAGEMENT TOOLS.—The General Services Administration is encouraged to pilot commercial off the shelf supply chain risk management tools to improve the ability of the Federal Government to characterize, monitor, predict, and respond to specific supply chain threats and vulnerabilities that could inhibit future Federal acquisition operations.

Subtitle E—Strategic EV Management

SEC. 5241. SHORT TITLE.

This subtitle may be cited as the ''Strategic EV Management Act of 2022''.

SEC. 5242. DEFINITIONS.

In this subtitle:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of General Services.

(2) AGENCY.—The term ''agency'' has the meaning given the term in section 551 of title 5, 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; and

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

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

SEC. 5243. STRATEGIC GUIDANCE.

(a) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Administrator, in consultation with the Director, shall coordinate with the heads of agencies to develop a comprehensive, strategic plan for Federal electric vehicle fleet battery management.

(b) CONTENTS.—The strategic plan required under subsection (a) shall—

(1) maximize both cost and environmental efficiencies; and

(2) incorporate—

(A) guidelines for optimal charging practices that will maximize battery longevity and prevent premature degradation;

(B) guidelines for reusing and recycling the batteries of retired vehicles; and

(C) any other considerations determined appropriate by the Administrator and Director.

(c) MODIFICATION.—The Administrator, in consultation with the Director, may periodically update the strategic plan required under subsection (a) as the Administrator and Director may determine necessary based on new information relating to electric vehicle batteries that becomes available.

(d) CONSULTATION.—In developing the strategic plan required under subsection (a) the Administrator, in consultation with the Director, may consult with appropriate entities, including—

(1) the Secretary of Energy;

(2) the Administrator of the Environmental Protection Agency;

(3) the Chair of the Council on Environmental Quality;

(4) scientists who are studying electric vehicle batteries and reuse and recycling solutions;

(5) laboratories, companies, colleges, universities, or start-ups engaged in battery use, reuse, and recycling research;

(6) industries interested in electric vehicle battery reuse and recycling;

(7) electric vehicle equipment manufacturers and recyclers; and

(8) any other relevant entities, as determined by the Administrator and Director.

(e) REPORT.—

(1) IN GENERAL.—Not later than 3 years after the date of enactment of this Act, the Administrator and the Director shall submit to the appropriate congressional committees a report that describes the strategic plan required under subsection (a).

(2) BRIEFING.—Not later than 4 years after the date of enactment of this Act, the Administrator and the Director shall brief the appropriate congressional committees on the implementation of the strategic plan required under subsection (a) across agencies.

SEC. 5244. STUDY OF FEDERAL FLEET VEHICLES.

Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on how the costs and benefits of operating and maintaining electric vehicles in the Federal fleet compare to the costs and benefits of operating and maintaining internal combustion engine vehicles. The Comptroller General of the United States shall, as part of the Comptroller General's annual reporting to committees of Congress—

(1) consolidate Matters for Congressional Consideration from the Government Accountability Office in one report organized by policy topic that includes the amount of time such Matters have been unimplemented and submit such report to congressional leadership and the oversight committees of each House;

(2) with respect to the annual letters sent by the Comptroller General to individual agency heads and relevant congressional committees on the status of unimplemented priority recommendations, identify any additional congressional oversight actions that can help agencies implement such priority recommendations and address any underlying issues relating to such implementation;

(3) make publicly available the information described in paragraphs (1) and (2); and

(4) publish any known costs of unimplemented priority recommendations, if applicable.

Subtitle F—Congressionally Mandated Reports

SEC. 5251. SHORT TITLE.

This subtitle may be cited as the ''Access to Congressionally Mandated Reports Act''.

SEC. 5252. DEFINITIONS.

In this subtitle:

(1) CONGRESSIONAL LEADERSHIP.—The term ''congressional leadership'' means the Speaker, majority leader, and minority leader of the House of Representatives and the majority leader and minority leader of the Senate.

(2) CONGRESSIONALLY MANDATED REPORT.—

(A) IN GENERAL.—The term ''congressionally mandated report'' means a report of a Federal agency that is required by statute to be submitted to either House of Congress or any committee of Congress or subcommittee thereof.

(B) EXCLUSIONS.—

(i) PATRIOTIC AND NATIONAL ORGANIZATIONS.—The term ''congressionally mandated report'' does not include a report required under part B of subtitle II of title 36, United States Code.

(ii) INSPECTORS GENERAL.—The term ''congressionally mandated report'' does not include a report by an office of an inspector general.

(iii) NATIONAL SECURITY EXCEPTION.—The term ''congressionally mandated report'' does not include a report that is required to be submitted to one or more of the following committees:

(I) The Select Committee on Intelligence, the Committee on Armed Services, the Committee on Appropriations, or the Committee on Foreign Relations of the Senate.

(II) The Permanent Select Committee on Intelligence, the Committee on Armed Services, the Committee on Appropriations, or the Committee on Foreign Affairs of the House of Representatives.

(3) DIRECTOR.—The term ''Director'' means the Director of the Government Publishing Office.

(4) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given the term ''federal agency'' under section 102 of title 40, United States Code, but does not include the Government Accountability Office or an element of the intelligence community.

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

(6) REPORTS ONLINE PORTAL.—The term ''reports online portal'' means the online portal established under section 5253(a).

SEC. 5253. ESTABLISHMENT OF ONLINE PORTAL FOR CONGRESSIONALLY MANDATED REPORTS.

(a) REQUIREMENT TO ESTABLISH ONLINE PORTAL.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall establish and maintain an online portal accessible by the public that allows the public to obtain electronic copies of congressionally mandated reports in one place.

(2) EXISTING FUNCTIONALITY.—To the extent possible, the Director shall meet the requirements under paragraph (1) by using existing online portals and functionality under the authority of the Director in consultation with the Director of National Intelligence.

(3) CONSULTATION.—In carrying out this subtitle, the Director shall consult with congressional leadership, the Clerk of the House of Representatives, the Secretary of the Senate, and the Librarian of Congress regarding the requirements for and maintenance of congressionally mandated reports on the reports online portal.

(b) CONTENT AND FUNCTION.—The Director shall ensure that the reports online portal includes the following:

(1) Subject to subsection (c), with respect to each congressionally mandated report, each of the following:

(A) A citation to the statute requiring the report.

(B) An electronic copy of the report, including any transmittal letter associated with the report, that—

(i) is based on an underlying open data standard that is maintained by a standards organization;

(ii) allows the full text of the report to be searchable; and

(iii) is not encumbered by any restrictions that would impede the reuse or searchability of the report.

(C) The ability to retrieve a report, to the extent practicable, through searches based on each, and any combination, of the following:

(i) The title of the report.

(ii) The reporting Federal agency.

(iii) The date of publication.

(iv) Each congressional committee or subcommittee receiving the report, if applicable.

(v) The statute requiring the report.

(vi) Subject tags.

(vii) A unique alphanumeric identifier for the report that is consistent across report editions.

(viii) The serial number, Superintendent of Documents number, or other identification number for the report, if applicable.

(ix) Key words.

(x) Full text search.

(xi) Any other relevant information specified by the Director.

(D) The date on which the report was required to be submitted, and on which the report was submitted, to the reports online portal.

(E) To the extent practicable, a permanent means of accessing the report electronically.

(2) A means for bulk download of all congressionally mandated reports.

(3) A means for downloading individual reports as the result of a search.

(4) An electronic means for the head of each Federal agency to submit to the reports online portal each congressionally mandated report of the agency, as required by sections 5254 and 5256.

(5) In tabular form, a list of all congressionally mandated reports that can be searched, sorted, and downloaded by—

(A) reports submitted within the required time;

(B) reports submitted after the date on which such reports were required to be submitted; and

(C) to the extent practicable, reports not submitted.

(c) NONCOMPLIANCE BY FEDERAL AGENCIES.—

(1) REPORTS NOT SUBMITTED.—If a Federal agency does not submit a congressionally mandated report to the Director, the Director shall to the extent practicable—

(A) include on the reports online portal—

(i) the information required under clauses (i), (ii), (iv), and (v) of subsection (b)(1)(C); and

(ii) the date on which the report was required to be submitted; and

(B) include the congressionally mandated report on the list described in subsection (b)(5)(C).

(2) REPORTS NOT IN OPEN FORMAT.—If a Federal agency submits a congressionally mandated report that does not meet the criteria described in subsection (b)(1)(B), the Director shall still include the congressionally mandated report on the reports online portal.

(d) DEADLINE.—The Director shall ensure that information required to be published on the reports online portal under this subtitle with respect to a congressionally mandated report or information required under subsection (c) of this section is published—

(1) not later than 30 days after the information is received from the Federal agency involved; or

(2) in the case of information required under subsection (c), not later than 30 days after the deadline under this subtitle for the Federal agency involved to submit information with respect to the congressionally mandated report involved.

(e) EXCEPTION FOR CERTAIN REPORTS.—

(1) EXCEPTION DESCRIBED.—A congressionally mandated report which is required by statute to be submitted to a committee of Congress or a subcommittee thereof, including any transmittal letter associated with the report, shall not be submitted to or published on the reports online portal if the chair of a committee or subcommittee to which the report is submitted notifies the Director in writing that the report is to be withheld from submission and publication under this subtitle.

(2) NOTICE ON PORTAL.—If a report is withheld from submission to or publication on the reports online portal under paragraph (1), the Director shall post on the portal—

(A) a statement that the report is withheld at the request of a committee or subcommittee involved; and

(B) the written notification provided by the chair of the committee or subcommittee specified in paragraph (1).

(f) FREE ACCESS.—The Director may not charge a fee, require registration, or impose any other limitation in exchange for access to the reports online portal.

(g) UPGRADE CAPABILITY.—The reports online portal shall be enhanced and updated as necessary to carry out the purposes of this subtitle.

(h) SUBMISSION TO CONGRESS.—The submission of a congressionally mandated report to the reports online portal pursuant to this subtitle shall not be construed to satisfy any requirement to submit the congressionally mandated report to Congress, or a committee or subcommittee thereof.

SEC. 5254. FEDERAL AGENCY RESPONSIBILITIES.

(a) SUBMISSION OF ELECTRONIC COPIES OF REPORTS.—Not earlier than 30 days or later than 60 days after the date on which a congressionally mandated report is submitted to either House of Congress or to any committee of Congress or subcommittee thereof, the head of the Federal agency submitting the congressionally mandated report shall submit to the Director the information required under subparagraphs (A) through (D) of section 5253(b)(1) with respect to the congressionally mandated report. Notwithstanding section 5256, nothing in this subtitle shall relieve a Federal agency of any other requirement to publish the congressionally mandated report on the online portal of the Federal agency or otherwise submit the congressionally mandated report to Congress or specific committees of Congress, or subcommittees thereof.

(b) GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Director, shall issue guidance to agencies on the implementation of this subtitle.

(c) STRUCTURE OF SUBMITTED REPORT DATA.—The head of each Federal agency shall ensure that each congressionally mandated report submitted to the Director complies with the guidance on the implementation of this subtitle issued by the Director of the Office of Management and Budget under subsection (b).

(d) POINT OF CONTACT.—The head of each Federal agency shall designate a point of contact for congressionally mandated reports.

(e) REQUIREMENT FOR SUBMISSION.—The Director shall not publish any report through the reports online portal that is received from anyone other than the head of the applicable Federal agency, or an officer or employee of the Federal agency specifically designated by the head of the Federal agency.

SEC. 5255. CHANGING OR REMOVING REPORTS.

(a) LIMITATION ON AUTHORITY TO CHANGE OR REMOVE REPORTS.—Except as provided in subsection (b), the head of the Federal agency concerned may change or remove a congressionally mandated report submitted to be published on the reports online portal only if—

(1) the head of the Federal agency consults with each committee of Congress or subcommittee thereof to which the report is required to be submitted (or, in the case of a report which is not required to be submitted to a particular committee of Congress or subcommittee thereof, to each committee

with jurisdiction over the agency, as determined by the head of the agency in consultation with the Speaker of the House of Representatives and the President pro tempore of the Senate) prior to changing or removing the report; and

(2) a joint resolution is enacted to authorize the change in or removal of the report.

(b) EXCEPTIONS.—Notwithstanding subsection (a), the head of the Federal agency concerned—

(1) may make technical changes to a report submitted to or published on the reports online portal;

(2) may remove a report from the reports online portal if the report was submitted to or published on the reports online portal in error; and

(3) may withhold information, records, or reports from publication on the reports online portal in accordance with section 5256.

SEC. 5256. WITHHOLDING OF INFORMATION.

(a) IN GENERAL.—Nothing in this subtitle shall be construed to—

(1) require the disclosure of information, records, or reports that are exempt from public disclosure under section 552 of title 5, United States Code, or that are required to be withheld under section 552a of title 5, United States Code; or

(2) impose any affirmative duty on the Director to review congressionally mandated reports submitted for publication to the reports online portal for the purpose of identifying and redacting such information or records.

(b) WITHHOLDING OF INFORMATION.—

(1) IN GENERAL.—Consistent with subsection (a)(1), the head of a Federal agency may withhold from the Director, and from publication on the reports online portal, any information, records, or reports that are exempt from public disclosure under section 552 of title 5, United States Code, or that are required to be withheld under section 552a of title 5, United States Code.

(2) NATIONAL SECURITY.—Nothing in this subtitle shall be construed to require the publication, on the reports online portal or otherwise, of any report containing information that is classified, or the public release of which could have a harmful effect on national security.

(3) LAW ENFORCEMENT SENSITIVE.—Nothing in this subtitle shall be construed to require the publication on the reports online portal or otherwise of any congressionally mandated report—

(A) containing information that is law enforcement sensitive; or

(B) that describe information security policies, procedures, or activities of the executive branch.

(c) RESPONSIBILITY FOR WITHHOLDING OF INFORMATION.—In publishing congressionally mandated reports to the reports online portal in accordance with this subtitle, the head of each Federal agency shall be responsible for withholding information pursuant to the requirements of this section.

SEC. 5257. IMPLEMENTATION.

(a) REPORTS SUBMITTED TO CONGRESS.—

(1) IN GENERAL.—This subtitle shall apply with respect to any congressionally mandated report which—

(A) is required by statute to be submitted to the House of Representatives, or the Speaker thereof, or the Senate, or the President or President Pro Tempore thereof, at any time on or after the date of the enactment of this Act; or

(B) is included by the Clerk of the House of Representatives or the Secretary of the Senate (as the case may be) on the list of reports received by the House of Representatives or the Senate (as the case may be) at any time on or after the date of the enactment of this Act.

(2) TRANSITION RULE FOR PREVIOUSLY SUBMITTED REPORTS.—To the extent practicable, the Director shall ensure that any congressionally mandated report described in paragraph (1) which was required to be submitted to Congress by a statute enacted before the date of the enactment of this Act is published on the reports online portal under this subtitle.

(b) REPORTS SUBMITTED TO COMMITTEES.—In the case of congressionally mandated reports which are required by statute to be submitted to a committee of Congress or a subcommittee thereof, this subtitle shall apply with respect to—

(1) any such report which is first required to be submitted by a statute which is enacted on or after the date of the enactment of this Act; and

(2) to the maximum extent practical, any congressionally mandated report which was required to be submitted by a statute enacted before the date of enactment of this Act unless—

(A) the chair of the committee, or subcommittee thereof, to which the report was required to be submitted notifies the Director in writing that the report is to be withheld from publication; and

(B) the Director publishes the notification on the reports online portal.

(c) ACCESS FOR CONGRESSIONAL LEADERSHIP.—Notwithstanding any provision of this subtitle or any other provision of law, congressional leadership shall have access to any congressionally mandated report.

SEC. 5258. DETERMINATION OF BUDGETARY EFFECTS.

The budgetary effects of this subtitle, for the purpose of complying with the Statutory Pay-As-You-Go-Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this subtitle, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

SA 6439. Mr. WICKER submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. WAIVER OF NAVIGATION AND VESSEL-INSPECTION LAWS.

Section 501(b) of title 46, United States Code, is amended—

(1) in paragraph (1), by inserting ''in accordance with the requirements of paragraph (3)'' after ''following a determination'';

(2) in paragraph (3)(A), by inserting ''prior to the issuance of a waiver'' before the semicolon at the end; and

(3) by adding at the end the following:

''(5) PROSPECTIVE APPLICATION.—No waiver of the vessel navigation laws may be issued for a vessel if, prior to the waiver request, such vessel was laden with merchandise covered by the requested waiver.''.

SA 6440. Mr. WARNER submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

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

SEC. 575. FOOD INSECURITY AMONG MILITARY FAMILIES: DATA COLLECTION; TRAINING; REPORT.

(a) DATA COLLECTION.—Not later than one year after the date of the enactment of this Act, the Under Secretary of Defense for Personnel and Readiness, acting through the Deputy Assistant Secretary for Military Community and Family Policy, in coordination with the Under Secretary for Food, Nutrition, and Consumer Services of the Department of Agriculture, shall—

(1) develop a survey, in collaboration with the Department of Agriculture, to determine how many members of the Armed Forces serving on active duty, and dependents of such members, are food insecure;

(2) issue the survey to such members and dependents;

(3) collect data from the survey on the use, by such members and dependents, of Federal nutrition assistance programs, including—

(A) the supplemental nutrition assistance program under the Food and Nutrition Act of 2008 (7 U.S.C. 2011 et seq.);

(B) the special supplemental nutrition program for women, infants, and children under section 17 of the Child Nutrition Act of 1966 (42 U.S.C. 1786);

(C) the school lunch program under the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq.); and

(D) the school breakfast program under section 4 of the Child Nutrition Act of 1966 (42 U.S.C. 1773); and

(4) collect data related to the number of such members and dependents who—

(A) are eligible for the basic needs allowance under section 402b of title 37, United States Code; and

(B) receive such basic needs allowance;

(5) develop and carry out a plan to train and designate an individual who will assist members at military installations on how and where to refer such members and their dependents for participation in Federal nutrition assistance programs described in paragraph (3); and

(6) coordinate efforts of the Department of Defense to address food insecurity and nutrition.

(b) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, and annually thereafter, the Under Secretary of Defense for Personnel and Readiness shall submit to the appropriate congressional committees a report including the following:

(A) The number of members of the Armed Forces serving on active duty and their dependents who are food insecure.

(B) The number of such members and their dependents who use the Federal nutrition assistance programs described in subsection (a)(3).

(C) The number of such members and their dependents described in subsection (a)(4).

(D) The status of implementation of the plan under subsection (a)(5).

(2) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this subsection, the term ''appropriate congressional committees'' means—