(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 section to study, evaluate, test, demonstrate, or apply technologies and practices to improve environmental performance.

(6) EMPLOYMENT OF CLEAN ENERGY ON 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 Administration.

(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 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.

(f) 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.

(g) 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 technology research and development that are specific to the United States maritime industry, and seek to fill those gaps;

(D) conduct research, development, testing, and demonstration of emerging 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 educational information 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-COMBATANT 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 on Transportation and Infrastructure of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives, including detailing any findings from the study; and

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

SEC. 5001. TABLE OF CONTENTS.

Title VI—HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS MATTERS

Subtitle B—DHS Trade and Economic Security Council

Subtitle C—Transnational Criminal Investigative Units

(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 technical feasibility and economic achievability of each measure; and

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

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

GOVERNMENTAL AFFAIRS MATTERS

Mr. PETERS (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. INHOFE (for himself and Mr. INhofE) 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.

TTITLE 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.

Subtitle B—DHS Trade and Economic Security Council


Subtitle C—Transnational Criminal Investigative Units

Sec. 5121. Short title.
Subtitle A—Global Catastrophic Risk Management Act of 2022

SEC. 501. SHORT TITLE.
This subtitle may be cited as the “Global Catastrophic Risk Management Act of 2022”.

SEC. 502. DEFINITIONS.
In this subtitle:
(1) BASIC NEED.—The term “basic need” means any good, service, or activity necessary to protect the health, safety, and general welfare of the civilian population of the United States and includes—
(B) water;
(C) shelter;
(D) basic communication services;
(E) basic sanitation and health services; and
(F) public safety.

(2) CATASTROPHIC INCIDENT.—The term “catastrophic incident” means any natural or man-made disaster that results in extraordinary levels of casualties or damage, mass evacuations, or disruption severe enough to affect population, infrastructure, environment, economy, national morale, or government functions in an area; and
(C) may include an incident—
(i) with a sustained national impact over a prolonged period of time;
(ii) 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. 5830(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.

(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 64(b) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 746(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 1984 (25 U.S.C. 5131).

TITLIE LI—HOMELAND SECURITY

Subtitle A—Global Catastrophic Risk Management Act of 2022

SEC. 501. SHORT TITLE.
This subtitle may be cited as the “Global Catastrophic Risk Management Act of 2022”.

SEC. 502. DEFINITIONS.
In this subtitle:
(1) BASIC NEED.—The term “basic need” means any good, service, or activity necessary to protect the health, safety, and general welfare of the civilian population of the United States and includes—
(B) food;
(C) water;
(D) shelter;
(E) basic communication services;
(F) basic sanitation and health services; and
(G) public safety.

(2) CATASTROPHIC INCIDENT.—The term “catastrophic incident” means any natural or man-made disaster that results in extraordinary levels of casualties or damage, mass evacuations, or disruption severe enough to affect population, infrastructure, environment, economy, national morale, or government functions in an area; and
(C) may include an incident—
(i) with a sustained national impact over a prolonged period of time;
(ii) 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. 5830(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.
(10) the Secretary of the Interior and the Director of the United States Geological Survey;
(11) the Administrator of the Environment 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 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. 5105. REPORT REQUIRED.
(a) In General.—Not later than 1 year after the date of enactment of this Act, and every 5 years thereafter, the President, with the support of the National Security Council, shall submit to Congress a report containing a comprehensive list of potential 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; and
(2) a plan for increased senior leader involvement in continuity of operations and continuity of government exercises; and

SEC. 5106. ENHANCED CATASTROPHIC INCIDENT ANNEX.
(a) IN GENERAL.—The President, with support from the committee, shall supplement each Federal Interagency Operational Plan for an annex to an Executive order that ensures 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 nonprofit relief during periods of heightened tension or other catastrophic incidents; and

SEC. 5107. ELEMENTS OF THE STRATEGY.
(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 13662 (85 Fed. Reg. 79379; relating to governance and integration of Federal mission resilience), Presidential Policy Directive–9 (90 Fed. Reg. 62270; relating to national continuity policy), or successor policies, to account for catastrophic and existential risk cumulatively or for particular threats;
(2) an assessment of the need to revise Executive Order 13662 (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 the authority of the President to take offline or destroy critical infrastructure; and
(3) a comprehensive list of potential catastrophic and existential risk.
(c) Consultation Requirement.—In preparing the report required under subsection (a) the President shall consult with—
(1) the Chairman of the Joint Chiefs of Staff;
(2) the Secretary of State;
(3) the Secretary of Defense;
(4) the Administrator of the Federal Emergency Management Agency; and
(5) other stakeholders.

(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 survival of the civilian population of the United States in a catastrophic incident are met;
(2) how the President will coordinate with national entities to mobilize 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) how 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) 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
(5) the steps the President will take to ensure that international allies enhance the readiness of the United States to provide for the general welfare.

(b) Elements of the Strategy.—The strategy required under subsection (a) shall include—
(1) a forecast of if and why global catastrophic and existential risk.
(b) Elements of the Strategy.—The strategy required under subsection (a) shall include—
(1) a forecast of if and why global catastrophic and existential risk.
(b) Elements of the Strategy.—The strategy required under subsection (a) shall include—
(1) a forecast of if and why global catastrophic and existential risk.
(b) Elements of the Strategy.—The strategy required under subsection (a) shall include—
(1) a forecast of if and why global catastrophic and existential risk.
restricted, annex to be made available to the appropriate committees of Congress and appropriate government entities.

SEC. 5107. VALIDATION OF THE STRATEGY FOR THE UNITED STATES 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 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) and 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 180 days after the date on which Department of Homeland Security leads the exercise under section 5107, the President shall submit to Congress a report that—

(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—

(a) supplant the existing 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 8900(c)(2) of title 6 (relating to the Economic Security Act).

(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 council 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 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 9903 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 322); and

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

(F) any other matters the Secretary considers appropriate.

(4) CHAIR AND VICE CHAIR.—(A) The Under Secretary for Strategy, Policy, and Plans of the Department 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 the 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 Representatives on the actions and activities of the Council.

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

‘‘(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 described 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 non-governmental 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.

(3) DUTY TO IMPLEMENT.—(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 8900(c)(2).

(C) RULE OF CONSTRUCTION.—Nothing in 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.—(1) The Secretary shall operate Transnational Criminal Investigative Units within United States Immigration and Customs Enforcement, Homeland Security Investigations, and相应的 Title.

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

(c) VETOING REQUIREMENT.—

(1) IN GENERAL.—Upon entry into a Transnational Criminal Investigative Unit, and at periodic intervals while serving in such 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) REVOCATION.—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 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. This subtitle may be cited as the ‘‘Transnational Criminal Investigative Unit Stipend Act’’. This subtitle may be cited as the ‘‘Transnational Criminal Investigative Unit Stipend Act’’.

Subtitle D—Other Matters

SEC. 5123. OTHER MATTERS.

Not later than 1 year after 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 section, as necessary, that identifies—

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

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

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

(b) CLEMENT AMENDMENT.—The table of contents for the Homeland Security Act of...
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 such term in ‘‘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).

SEC. 5133. ASSISTANCE AND TRAINING FOR COMMUNITIES WITH TECHNOLOGICAL HAZARDS AND RELATED EMERGING THREATS.
(a) IN GENERAL.—The Administrator shall maintain the capability 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) AUTHORIZATIONS.—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) subsection 1236 of the Disaster Recovery Reform Act of 2018 (42 U.S.C. 5191c); and

(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 information 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 to—
(i) technological hazards and related emerging threats preparedness; and
(ii) coordinate 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 Representatives, the Committee on Appropriations of the House of Representatives, and the Committee on Transportation and Infrastructure in 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.

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 2027.

SEC. 5135. SAVINGS PROVISION.
Nothing in this subtitle shall diminish or divert resources from—
(1) the full implementation 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 I—COUNTERING WEAPONS OF MASS DESTRUCTION OFFICE

SEC. 5142. DEFINITIONS 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) by redesignating subsections (a) and (b) as subsections (b) and (d), respectively;
(B) by inserting before subsection (b), as so redesignated, the following:

‘‘(A) in general.—For the purposes of coordinating the efforts of the Department to counter weapons of mass destruction and chemical, biological, and related emerging threats, the Office shall—

(1) provide expertise and guidance to Federal, State, local, Tribal, and territorial partners to prevent weapons of mass destruction and chemical, biological, and related emerging threats; and
(2) coordinate capability development activities to counter weapons of mass destruction and chemical, biological, and related emerging threats, including international partnerships subject to the requisition of the Secretary of Homeland Security;’’;

(2) in section 1921 (6 U.S.C. 591g)—
(A) by striking subsection (b) and redesignating subsection (c) as subsection (b); and
(B) by redesigning subsections (a) and (b) as subsections (b) and (d), respectively;

(3) in section 1922 (6 U.S.C. 591h)—
(A) by striking subsection (b) and redesignating subsection (c) as subsection (b); and
(B) by redesigning subsections (a) and (b) as subsections (b) and (d), respectively;

(4) in section 1923 (6 U.S.C. 592)—
(A) by redesigning 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, and related emerging threats, the Office shall—

(1) 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);

(G) 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;

(2) coordinate the efforts of the Department to counter weapons of mass destruction and chemical, biological, and related emerging threats;’’.

(5) in section 1924 (6 U.S.C. 592a)—
(A) by redesigning 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, and related emerging threats, the Office shall—

(1) 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);

(G) 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;

(2) coordinate the efforts of the Department to counter weapons of mass destruction and chemical, biological, and related emerging threats;’’.

(6) in section 1925 (6 U.S.C. 592b)—
(A) by redesigning 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, and related emerging threats, the Office shall—

(1) 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);

(G) 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, and related emerging threats on behalf of the Department;’’.

(b) TECHNOLOGICAL HAZARD AND RELATED EMERGING THREAT.—The term ‘‘technological hazard and related emerging threat’’ means any threat that involves materials created by humans that pose a unique hazard to the general public and environment and which may result from—
(1) an accident;
(2) an emergency caused by another hazard; or
(3) intentional use of the hazardous materials;

and

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

(c) ASSESSMENT AND NOTIFICATION.—In carrying out subsection (a), the Administrator shall—
(1) maintain a broad and comprehensive technology characterization, technology maturation, and technology testing capability to counter weapons of mass destruction and chemical, biological, and related emerging threats; and
(2) coordinate the efforts of the Department to counter—
(A) weapons of mass destruction; and
(B) chemical, biological, radiological, nuclear, and other related emerging threats; and

(d) REPORT.—Not later than 1 year after the date of enactment of this Act, 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 Representatives, the Committee on Appropriations of the House of Representatives, and the Committee on Transportation and Infrastructure in the House of Representatives a report relating to—
(1) the full implementation 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).

(4) in section 1926 (6 U.S.C. 592c)—
(A) by redesigning 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, and related emerging threats, the Office shall—

(1) 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);

(G) 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, and related emerging threats on behalf of the Department;’’.

(5) in section 1927 (6 U.S.C. 592d)—
(A) by redesigning 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, and related emerging threats, the Office shall—

(1) 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);

(G) 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, and related emerging threats on behalf of the Department;’’.
coordination requirement under subpara-
graph (G); and

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

(2) OFFICE.—For pur-
poses of the detection and reporting responsi-
bilities of the Office for weapons of mass
destruction and chemical, biological, radi-
ological, nuclear, and other related emerging
threats, the Office shall—

(A) in coordination with end users, in-
cluding State, local, Tribal, and territorial
governments, as appropriate—

(i) carry out a program to test and evalu-
ate technology, in consultation with the
Science and Technology Directorate, to de-
tect and report on weapons of mass destruc-
tion and chemical, biological, radiological,
nuclear, and other related emerging threats
weapons or unauthorized material, in coordi-
nation with other Federal agencies, as appro-
priate, and establish performance metrics to
evaluate the effectiveness of individual de-
tectors and detection systems in detecting
those weapons or material—

(II) in paragraph (1)—

(1) in paragraph (1)—

(I) by inserting “deploy,” after “acquire,”;

and

(II) by striking “deployment” and insert-
ing “technology”;

(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 redesign-
ated, by striking “national strategic five-year
plan referred to in paragraph (10)” and in-
serting “United States national technical
nuclear forensics strategic planning”;

(vi) in paragraph (7)(C)(v), as so redesign-
ated—

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

(II) in subclause (I)—

(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 RESPO-
sibilities.—The Office—

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

(2) shall—

(A) serve as a primary entity of the Fed-
eral Government to further develop, acquire,
deploy, and support the operations of a na-
tional 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 pro-
vide the capability and other gaps in the Department to help en-
sure a managed, coordinated response; and

(C) collaborate with the Biomedical Ad-
vanced Research and Development Author-
ity, the Office of Health Security, the De-
fense Advanced Research Projects Agency,
and the National Aeronautics and Space Ad-
ministration, and other relevant Federal
agencies, to support the development from indus-
try, academia, and the national laboratories
on chemical and biological surveillance ef-
forts;

(2) in section 1924 (6 U.S.C. 593), by striking
“section 1101 of the Strom Thurmond Na-
tional Defense Authorization Act for Fiscal
Year 1999 (6 U.S.C. 3104 note),” and inserting
“section 4002 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.

(3) in section 1227(a)(1)(C) (6 U.S.C.
598a(a)(1)(C) )—

(A) in clause (i), by striking “required
under section 1101 of the National De-
fense Authorization Act for Fiscal
Year 2010”; and

(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 re-
garding 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 inserting “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 con-
sequences 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 congress-
ional committees an update on the STC pro-
gram.”;

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 implementa-
tion plan to counter weapons of mass de-
struction and chemical, biological, radi-
ological, nuclear, and other related emerging
threats, which should—

(A) have clearly identified authorities,
specified roles, objectives, benchmarks, ac-
countability, 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 strate-
ges and work with other Federal agencies.

(2) CONSIDERATION.—The Secretary shall
appropriately consider weapons of mass de-
struction and chemical, biological, radi-
ological, nuclear, and other related emerging
threats when creating the strategy and im-
plementation plan required under paragraph
(1).

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

(4) DEPARTMENTWIDE BIODEFENSE REVIEW
AND STRATEGY.—

(‘‘a) 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,
with appropriate, stakeholders representing Federal, State, Tribal,
territorial, academic, private sector,
and nongovernmental entities, shall conduct a
Departmentwide review of biodefense activi-
ties and strategies.

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

(a) identify with specificity the bio-
defense lines of effort of the Department, in-
cluding relating to biodefense roles, respon-
sibilities, and capabilities of components and
ofices of the Department;

(b) assess how such components and
offices coordinate internally and with public
and private partners in the biodefense enter-
prise;

(c) identify any policy, resource, ca-
pability, 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 responsiblies, including with public
and private partners in the biodefense enter-
prise.
“(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. 384) in relation to the development of a national biodefense strategy and associated implementation plan, including a review and assessment of biodefense policies, practices, and initiatives by 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 the Department engages with public and private partners in the biodefense enterprise, including other Federal agencies, national laboratories and sites, State, local, Tribal, and other Federal 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 (ii) 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), and not less often than once every 5 years thereafter, the Secretary shall—

(A) report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and Governmental Affairs of the House of Representatives regarding such strategy and plans.

(B) establish a panel to advise the Secretary on the effective 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’’).

(6) 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, Tribal, and other Federal, academic, the private sector, national laboratories, and nongovernmental organizations, including, as appropriate—

(i) members designated by 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.

(7) 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.

(8) OFFICE OF HEALTH SECURITY.—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.

(9) VOLUNTARY SERVICE.—The members of the Advisory Council (5 U.S.C. App.) shall not apply to the Advisory Council on a voluntary basis.

(10) COUNTERING WEAPONS OF MASS DESTRUCTION ACT OF 2018.—Section 2 of the Countering Weapons of Mass Destruction Act of 2018 (Public Law 115–237; 122 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’’.


(1) in section 1(b) (Public Law 109–347; 120 Stat. 1841), 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)—

(i) by striking the ‘‘Assistant Secretary for Health Affairs,’’;

(ii) by striking ‘‘Affairs, or’’ and inserting ‘‘Affairs’’; and

(B) in subsection (b), by striking the end following 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 1901 (6 U.S.C. 957) 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 ‘‘BIOLOGICAL MEDICAL OFFICE’’ 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 ‘‘over- sight of direct patient care, the workforce, public health, and work- force health and safety matters of the De- partment’’;

(ii) in paragraph (1), by striking ‘‘the Admin- istrator of the Federal Emergency Man- agement Agency, the Assistant Secretary, and other Department officials’’ and insert- ing ‘‘and all other Department officials’’;

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

(iv) by redesignating paragraph (5) as para- graph (13); and

(v) by inserting after paragraph (4) the fol- lowing:

‘‘(5) overseeing all medical and public health activities of the Department, includ- ing the delivery, advisement, and oversight of direct patient care and the organization, management, and staffing of component op- erations that deliver direct patient care;

(6) advising the head of each component of the Department that delivers direct pa- tient care regarding the recruitment and appo- intment of a component chief medical offi- cer; and deputy chief medical officer or the employment in the capacities of chief medical officer and deputy chief med- ical officer;

(7) advising the Secretary and the head of each component of the Department that de- liver direct patient care regarding knowl- edge and skill standards for medical per- sonnel and the assessment of that knowledge and skill;

(8) advising the Secretary and the head of each component of the Department that de- liver direct 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 exam- ination as appropriate by such component with respect to any employee solely because such em- ployee identifies a need for psychological health counseling or assistance or re- ceives such assistance;

(B) increasing the availability and num- ber of local psychological health professions with experience providing psycho- logical support services to personnel;

(C) establishing a behavioral health curric- ulum for employees at the beginning of their careers to provide resources early re- garding the importance of psychological health;

(D) establishing periodic management training on crisis intervention and such com- ponent psychological health counseling or assistance program;

(E) improving any associated existing em- ployee 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 vol- untary health assessment program that in- cludes a safe harbor for employees who seek treatment;

(G) including, when appropriate, collabo- rating 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 Infor- mation Officer of the Department—

‘‘(A) identifying methods and technologies for managing, updating, and overseeing pa- tient records; and

(B) setting standards for technology used by the components of the Department re- garding the collection, storage, and over- sight of medical records;

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

(12) performing the Countering Weapons of Mass Destruction Office and other components of the Department as di- rected by the Secretary to enhance the abil- ity of Federal, State, local, Tribal, and terri- torial governments to prevent, detect, pro- tect against, and mitigate the health effects of chemical, biological, radiological, and nu- clear issues; and’’; and

(13) 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

(2) enter into any other transactions.

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

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

(2) ensure privacy protections are inte-grated into all Office of Health Security ac- tivities, subject to the review and approval of the Privacy Officer and 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 Secu- rity, including how best practices were used in the creation of the Office of Health Security.

‘‘(g) by redesigning section 710 (6 U.S.C. 350) section to appear after section 2301, as so redesignated;

(h) in section 2302, as so redesignated—

(A) in the section heading, by striking ‘‘MILITARY SUPPORT’’ and inserting ‘‘SAFETY’’;

(B) in subsection (a), by striking ‘‘Under Secretary for Regional Management’’ and inserting ‘‘Chief Medical Officer’’;

(C) in subsection (b)—

(1) in the matter preceding paragraph (1), by striking ‘‘Secretary for Regional Manage- ment, in coordination with the Chief Medical Officer,’’ and inserting ‘‘Chief Medical Offi- cer’’;

(2) in paragraph (3), by striking ‘‘as deemed appropriate by the Under Sec- retary,’’;

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

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

(9) by the insertion of the following:

‘‘(a) TRANSITION AND TRANSFERS.—

(1) TRANSITION.—The individual appointed pursuant to section 1931 of the Homeland Se- curity Act of 2002 (6 U.S.C. 3302 of the Depart- ment 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 with- out the need for reappointment.

(2) RULE OF CONSTRUCTION.—The rule of construction described in section 2(h) of the Presidential Appointment Efficiency and Streamlining Act of 2011 (5 U.S.C. 3321 note) shall not apply to the Chief Medical Officer of the Department of Homeland Security, as in effect 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 Secu- rity—

(A) all functions, personnel, budget author- ity, 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 author- ity, and assets of the Assistant Secretary for the Countering Weapons of Mass Destruction Office relating to the Chief Medical Officer, including the Medical Operations Direc- torate 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 author- ity, and assets of the Assistant Secretary for the Countering Weapons of Mass Destruction Office associated with the efforts pertaining to the program coordination relating to defending the food, agriculture, and veterinary defenses of the Office, as in exist- ence on the day before the date of enactment of this Act.

‘‘(4) SEC. 5145. MEDICAL COUNTERMEASURES PRO- GRAM.

The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by redesign- nating 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 QUAL- ITY ASSURANCE RECORDS.

Title XXIII of the Homeland Security Act of 2002, as amended by the Administrator’s direction 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 contractor to the Department from an- other Federal Agency or contractor to the Department from another Federal Agency;

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

(iv) hired under a contract for services;

(B) in paragraph (1), by striking ‘‘as deemed appropriate by the Under Sec- retary,’’;

(C) in subsection (b)—

(1) in the matter preceding paragraph (1), by striking ‘‘Secretary for Regional Manage- ment, in coordination with the Chief Medical Officer,’’ and inserting ‘‘Chief Medical Offi- cer’’;

(2) in paragraph (3), by striking ‘‘as deemed appropriate by the Under Sec- retary,’’;
"(c) 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 the United States Code (commonly known as the ‘Freedom of Information Act’).

"(d) 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 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.

"(e) 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.

"(f) 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 sub- section (c).

SEC. 5148. TECHNICAL AND CONFORMING AMENDMENTS.


"(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 sub- title C of title XIX and sections 1901 and 1922; and

"(e) by adding at the end the following:—

"TITLE XXIII—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.
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 materials 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 policy documents; and
(4) any other recommendations to ensure the confidentiality, availability, and integrity of data residing in or in transit through commercial satellite systems.
(b) REQUIREMENTS.—The report made under subsection (a) shall be unclassified but may include a classified annex.

SEC. 5141. RECOMMENDATIONS 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 in section 3 of the Small Business Act (15 U.S.C. 632).
(b) ESTABLISHMENT OF SMALL BUSINESS 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; and
(C) shall contain appropriate materials for reference by entities that develop, operate, or maintain commercial satellite systems;
(D) shall contain materials specifically tailored at assisting small business concerns with the secure development, operation, and maintenance of commercial satellite systems; and
(E) shall contain controlled unclassified information distributed to commercial entities through a process determined appropriate by the Director.

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.

SEC. 5154. RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
(a) DEFINITIONS.—In this section:
(1) SMALL BUSINESS CONCERN.—The term "small business concern" has the meaning given in section 3 of the Small Business Act (15 U.S.C. 632).
(2) SMALL BUSINESS CYBERSECURITY AGENCY.—The term "small business cybersecurity agency" has the meaning given in section 3 of the Small Business Act (15 U.S.C. 632).
(b) ESTABLISHMENT OF SMALL BUSINESS 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; and
(C) shall contain appropriate materials for reference by entities that develop, operate, or maintain commercial satellite systems; and

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" means—
(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" means the means given the term in subsection (e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 15504).
(4) CYBERSECURITY RISK.—The term "cybersecurity risk" means the means given the term in section 2200 of the Homeland Security Act of 2002, as added by section 5149 of this Act.
(5) CYBERSECURITY THREAT.—The term "cybersecurity threat" means the means given the term in section 2200 of the Homeland Security Act of 2002, as added by section 5149 of this Act.

SEC. 5153. REPORT ON COMMERCIAL SATELLITE SYSTEMS
(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 materials 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 policy documents; and
(4) any other recommendations to ensure the confidentiality, availability, and integrity of data residing in or in transit through commercial satellite systems.
(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 (b)(1); (B) any consultation with a non-Federal entity described in subsection (d)(3); (C) the coordination carried out pursuant to subsection (d)(3); (D) the establishment and maintenance of the clearinghouse pursuant to subsection (b); (E) the recommendations consolidated pursuant to subsection (b)(1); and (F) any feedback received by the Director on the clearinghouse from non-Federal entities.

SEC. 5155. STRATEGY.
Not later than 180 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 those terms in section 2220D 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);
(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 of building, including synagogues, mosques, temples, in which congregants practice their religious or spiritual beliefs; and
(4) the term ‘safety and security’, for the purpose of this section, 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.
(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 coordinate the 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) DETAILS.—The Secretary may coordinate details as required for the Clearinghouse.
(C) DESIGNATED POINT OF CONTACT.—There shall be a 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 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, shall 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 TIER.—
(A) IN GENERAL.—In consultation with the Attorney General, in consultation with the Attorney General, 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, in faith-based organizations and houses of worship.
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
SEC. 5161. GRANT PROGRAM OVERVIEW.
(a) DHS GRANTS 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; and
(2) directly link to each grant application and any applicable user guides;
(b) OTHER FEDERAL GRANTS AND RESOURCES.—Each Federal agency notified under section 5164(3) shall provide necessary information on any 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), provide information regarding Department grant programs and houses of worship to the Secretary or the appropriate point of contact for the Clearinghouse; and
(2) IDENTIFICATION OF RESOURCES.—The Clearinghouse shall, to the extent practicable, identify, for each State—
(i) the information collected under subparagraph (A); and
(ii) the recommendations proposed under subparagraph (B)(iii).
(3) any resources or programs, including any Federal, State, local, Tribal, territorial, private sector, and nongovernmental organizations relevant to 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. 5162. APPROVAL OF GRANTS.
(a)izzie the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives.
SEC. 5163. OTHER RESOURCES.
(a) zzice the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives.
SEC. 5164. NOTIFICATION OF CLEARINGHOUSE.
(b) zzice the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives.
SEC. 5165. GRANT PROGRAM OVERVIEW.
(a) DHS GRANTS 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; and
(2) directly link to each grant application and any applicable user guides;
(b) OTHER FEDERAL GRANTS AND RESOURCES.—Each Federal agency notified under section 5164(3) shall provide necessary information on any 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), provide information regarding Department grant programs and houses of worship to the Secretary or the appropriate point of contact for the Clearinghouse; and
(2) IDENTIFICATION OF RESOURCES.—The Clearinghouse shall, to the extent practicable, identify, for each State—
(i) the information collected under subparagraph (A); and
(ii) the recommendations proposed under subparagraph (B)(iii).
(3) any resources or programs, including any Federal, State, local, Tribal, territorial, private sector, and nongovernmental organizations relevant to 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.
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 practicable.

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

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

(iv) 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

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

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

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

(I) in paragraph (A), by striking ‘‘January 31, 2018, and January 31, 2021, the Inspector General of the Department’’ and inserting ‘‘January 31, 2018, and January 31, 2021, the Inspector General of the Department’’;

(II) comply with the procedures developed and implemented pursuant to section 70923(b)(2) of the Build America, Buy America Act of 2002, submit annually to each committee specified in subparagraph (B) a report that—

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

(IV) outlines the progress in implementing outcome-based and other performance metrics referred to in subparagraph (B) (A)(i).’’;

(3) in paragraph (11)(A), by striking the period at the end and inserting the following:

‘‘(i) the mission of each Joint Task Force;’’;

(II) protect against, detect, deter, suppress, and mitigate, to the extent practicable, the verifiable chronology of the origin and proliferation and impact of digital content forgeries, such as the adoption of digital content provenance and technology standards; and

(III) 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

(4) INSTITUTION OF HIGHER EDUCATION.—The Secretary, in consultation with the Commissioner of the Higher Education Act of 1965 (20 U.S.C. 1010), may—

(a) establish a task force, including goals and performance metrics for the Joint Task Force;’’;

(b) establish a strategy and performance measures for the Joint Task Force, including goals and performance metrics for the Joint Task Force;’’; and

(c) establish outcome-based and other performance metrics for the Joint Task Force;’’;

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

(D) the Committee on Science, Space, and Technology 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).

(8) Joint Task Force Reauthorization Act of 2022.—This subtitle may be cited as the ‘‘Joint Task Force Reauthorization Act of 2022’’.

SEC. 5218. 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.


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

(i) 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;’’.’’

(ii) 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); and

(iii) targets for current and future fiscal years; and

’’(C) in subparagraph (A), by striking ‘‘enactment of the DHS Joint Task Forces Reauthorization Act of 2022’’.

SEC. 5191. SHORT TITLE.

This subtitle may be cited as the ‘‘DHS Joint Task Forces Reauthorization Act of 2022’’.
(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 and 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 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 stakeholders, 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 benign or helpful alterations 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 developing policies and standards, for the adoption and effective use of technologies and systems to determine digital content provenance and detect digital content forgeries while promoting 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 technology 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 digital content forgeries, including public-private partnerships that support and collaborate on—

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

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

(iii) research 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 with respect to the 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.

(k) 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.


(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.

(l) STAFF.—

(1) IN GENERAL.—Staff of the Task Force shall be comprised of detailed from—

(A) the Department of Homeland Security; and

(B) the National Telecommunications and Information Administration.

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

(3) COMMITTEE REPORT.—An interim report containing the findings, conclusions, and recommendations of the Task Force, including the plan developed under subsections (a) and (c), shall be submitted to the President and the relevant congressional committees an interim report containing the findings, conclusions, and recommendations of the Task Force, including the plan developed under subsection (c).
(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 security testing, risk evaluation, threat risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including security, 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) a combination of cybersecurity measures and communication patterns indicating 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 pattern or technical means by which an illegitimate access to an information system or information that is stored on, processed by, or transmitted by a critical infrastructure or information system is thwarted by 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 systems, networks, or facilities 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, assessment, protection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, threat risk management planning, or risk audit; 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 transmitted by a critical infrastructure or 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 occurrences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such occurrences 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, that endangers an information system that may result in an unauthorized use to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transmitted by an information system.

(B) EXCLUSION.—The term ‘cybersecurity threat’ shall not include 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 transmitted by 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, has an adverse effect on an information system or information stored on, processed by, or transmitted by an information system not owned by—

(i) the entity deploying 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 non-governmental 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 or information systems, 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 to—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents; and

(B) facilitating information sharing and operational coordination with threat response; and

(C) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective, and efficient manner to speed recovery from cybersecurity risks.

(15) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’—

(A) means the ‘intelligence community’ as that term is defined in section 3502 of title 44, United States Code; and

(B) does not include the National Security Agency.

(16) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given in section 101 of the National Security Act of 1947 (50 U.S.C. 3000(a)).

(17) MONITOR.—The term ‘monitor’ means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transmitted by 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, and efficient manner to speed recovery from cybersecurity risks.

(19) NATIONAL SECURITY SYSTEM.—The term ‘national security system’ has the meaning given in the term in section 11013 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, operation, maintenance, or administration of a federal information system or information and any security assessment that could enable or facilitate the defeat of a security control.

(22) SECURITY VULNERABILITY.—The term ‘security vulnerability’ means any attribute of a federal information system or information that could be exploited to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transmitted by an information system.

(23) SHARING.—The term ‘sharing’ includes transferring or conveying, by any means, software, process, or procedure that could enable or facilitate the defeat of a security control.

IN GENERAL.—In this subtitle, the term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

SEC. 2201. DEFINITION—

In this subtitle, the term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

(B) in section 2202 (6 U.S.C. 652) —

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

(ii) in paragraph (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

SEC. 2202. CYBERSECURITY ADVISORY COMMITTEE—

In general.—The term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

(a) Membership.—The term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

(b) Term.—The term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

(c) Authorization.—The term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

(d) Purpose.—The term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

(e) Authorization.—The term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

(f) Authorization.—The term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

IN GENERAL.—In this subtitle, the term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2230a of this title.

(B) in section 2202 (6 U.S.C. 652) —

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

(ii) in paragraph (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

SEC. 2203. CRYPTOGRAPHY STANDARDS—

In general.—The term ‘Cryptography Standards’ means the standards established under section 2203 of this title.

(b) Term.—The term ‘Cryptography Standards’ means the standards established under section 2203 of this title.

(c) Authority.—The term ‘Cryptography Standards’ means the standards established under section 2203 of this title.

(d) Authorization.—The term ‘Cryptography Standards’ means the standards established under section 2203 of this title.

(e) Authorization.—The term ‘Cryptography Standards’ means the standards established under section 2203 of this title.

(f) Authorization.—The term ‘Cryptography Standards’ means the standards established under section 2203 of this title.

IN GENERAL.—In this subtitle, the term ‘Cryptography Standards’ means the standards established under section 2203 of this title.

(B) in section 2202 (6 U.S.C. 652) —

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

(ii) in paragraph (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’’;
(C) in section 2209 (6 U.S.C. 659)—
(i) by striking subsection (a);
(ii) by redesigning subsections (b) through subsection (o) as subsections (a) through subsection (r), respectively;
(iii) in subsection (c)(1), as so redesignated;
(iv) in paragraphs (A)(ii) and (F), as so redesignated—
(I) in the matter preceding paragraph (1), by striking “subsection (c)” and inserting “subsection (b)”;
(II) in paragraph (2)(A), by striking “subsection (c)(1)” and inserting “subsection (b)(1)”;
(v) in subsection (i), as so redesignated, by striking “subsection (c)(8)” and inserting “subsection (c)(12)”;
(vi) by redesigning the first subsections (p) and second subsections (q) and (r) 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)”;
(II) in paragraph (5)(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 redesigning subsections (b) through (e) as subsections (a) through (d), respectively; and
(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 2290”;
(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 (b); and
(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) in redesigning 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 redesigned, in the matter preceding paragraph (1), by striking “subsection (b)” and inserting “subsection (a)”;
(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)”;
(cc) in paragraph (B), by striking “subsection (c)(2)” and inserting “subsection (b)(2)”;
(D) in paragraph (2), by striking “subsection (c)(2)” and inserting “subsection (b)(2)”;
(E) in paragraph (3), by striking “subsection (c)” and inserting “subsection (b)”;
(F) 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”;
(ii) by striking subsection (f) and inserting the following:
“(C) 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. 665p)—
(i) in subsection (a)—
(I) by striking paragraphs (1), (2), (5), and (6); and
(II) by redesigning paragraphs (3), (4), (7), (8), (9), (10), (11), and (12) as paragraphs (1) through (8), respectively;
(ii) in subsection (c)(2)(B)(xv)(ii)(aa), by striking “information sharing and analysis organization” and inserting “Information Sharing and Analysis Organization”; and
(v) in subsection (i), as so redesignated, by striking “appropriate committees of Congress and inserting ‘appropriate congressional committees’”;
(vi) in subsection (q)(4), in the matter preceding clause (i), by striking “appropriate committees of Congress and inserting ‘appropriate congressional committees’”;
(K) in section 2220B (6 U.S.C. 665j)—
(i) by striking paragraph (1);
(ii) by redesigning 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; 130 Stat. 1501)” and inserting “(6 U.S.C. 1501)”;
(L) in section 2222 (6 U.S.C. 671)—
(i) by striking paragraphs (3), (5), and (8); and
(ii) by redesigning paragraph (4) as paragraph (3); and
(iii) by redesigning 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 subtitile A of title XXII the following:
“Sec. 2200. Definitions.”;
(B) by striking the item relating to section 2201 and inserting 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—
(I) in subsection (a)—
(A) by striking paragraphs (4) through (7) and inserting the following:
“(B) The term ‘cybersecurity’ purpose has the meaning given the term in section 2200 of the Homeland Security Act of 2002.”;
“(G) The term ‘cybersecurity threat’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.”;
“(H) The term ‘cyber threat indicator’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.”;
“(I) The term ‘defensive measure’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.”;
“(J) The term ‘security vulnerability’ 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, as added by this section and inserting “section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)”.
(7) DEFENSIVE MEASURE.—The term ‘defensive measure’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002, as added by this section and inserting “section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)”.
(8) CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 is amended by striking “small business” and inserting “the Small Business Act (6 U.S.C. 668(a)(8))”.
(9) SMALL BUSINESS ACT.—Section 21(a) (8)(B) of the Small Business Act (15 U.S.C. 668(a)(8)) is amended by striking...
CHAPTER 79—FEDERAL RESEARCH SECURITY COUNCIL

SEC. 7901. SHORT TITLE.

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

SEC. 7902. 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.


"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 malicious 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 security 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 existing products or processes or improving existing products or processes; and

"(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 at Executive agencies;

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

"(C) research and development centers at institutions of higher education (as defined in section 101(a) of the Higher Education Act of 1965 (34 U.S.C. 1001(a)));

"(D) research and development centers of States, United States territories, Indian tribes, and municipalities;

"(E) the Department of Agriculture, the Department of Commerce, the Department of Energy, the Department of Health and Human Services, the Department of Homeland Security, the Department of Justice, the Department of Energy, the Department of Commerce, the Department of Health and Human Services, and the Department of Transportation;

"(F) The Department of Energy.

"(G) The Department of State.

"(H) The Department of the Interior.

"(I) The Department of Defense.


"(K) The Office of the Director of National Intelligence.

"(L) The Department of Justice.

"(2) UNIFORM APPLICATION PROCESS.—The term ‘uniform application process’ means a process for the receipt of applications for federal research and development funding.
(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 conflict of interest policy for grants in accordance with subsection (c).

(2) Developing and implementing policies and providing guidance to prevent conflict of interest, while reducing administrative burden for researchers and research institutions.

(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 from 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 13387 (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 and grant recipient institutions accurately report conflicts of interest and conflicts of commitment in accordance with subsection (c)(1). Such programs shall include—

(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 affiliated with, Federal agencies, while 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 Foundation 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.

(12) 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 support 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 grants; 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.

(13) REQUIREMENTS FOR TIMELINESS OF SHARING CRITERIA.—In identifying or developing criteria and procedures for sharing information with respect to Federal research security risks, the Council shall ensure that such criteria address, at a minimum—

(i) the information to be shared;

(ii) the circumstances under which it is appropriate for an Executive agency to rely on information made available through such sharing in exercising the authorities and responsibilities of the agency under applicable laws relating to the award of grants;

(iii) the science and technology of that foreign country that do not adhere to the United States scientific values of openness, transparency, reciprocity, integrity, and merit-based competition;

(iv) the impact of such support and affiliations, appointments, or participation in talent programs on United States national security and economic interests; and

(v) the procedures for protecting intellectual capital that may be present in such information; and

(14) 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 and 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, law enforcement, 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) providing employees of Executive agencies with awareness training with respect to insider threats and the responsibilities of employees to report such threats; and

(B) gathering information for a centralized analysis, reporting, and response capability.

(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 science, technology, 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 or foreign government-related organizations, 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; and

(ii) federally funded research and development; and

(C) practices within the research enterprise of a foreign country that 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 Science and Technology Policy and the Director of the Office of Science and Technology Policy that detail—

(1) the number of ongoing investigations by the Council Members related to Federal research security that may result, or have resulted, in agency pre-notice letters, suspensions, proposed debarments, and debarments; and

(2) the procedures for sharing information 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. 

(2) REPORT.—Nothing in this section may be construed— 
"(1) to alter or diminish the authority of any Executive agency; or 
"(2) to alter any procedural requirements or remedies that were in place before the date of enactment of the Safeguarding America’s 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 risk posed by persons participating in federally funded research and development; 
"(2) integrating 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) on the applicability and relevance of the research and development to the national security and economic competitiveness of the United States; 
"(4) identifying initiatives impacting Federally funded research grant making policy and management to protect the national and economic security interests of the United States, that 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. 2000 et seq.).

(b) INCLUSIONS.—The responsibility of the head of an Executive agency for assessing Federally funded grantees 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 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.

(2) C LERICAL 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:


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

"(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’ means—

"(A) a grant awarded by a Federal agency; 
"(B) includes a grant 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 GOVERNMENT.—The term ‘foreign government’ includes a foreign entity owned by, subject to the control of, or subject to regulation by a foreign government.

"(5) FOREIGN GOVERNMENT INSTITUTION.—The term ‘foreign government institution’ means an entity over which a foreign government directly or indirectly exercises a dominant influence.

"(6) LAW ENFORCEMENT AGENCY.—The term ‘law enforcement agency’ includes—

"(A) a Federal, State, local, or Tribal law enforcement agency; and 
"(B) includes—

"(i) the Office of Inspector General of an Executive agency; 
"(ii) the Office of Inspector General, or a designated Federal entity (as defined in section 6(b) of the Inspector General Act of 1978 (5 U.S.C. App.)); or 
"(iii) the Inspector General of the Department of Homeland Security (as defined in section 8(a) of the Inspector General Act of 1978 (5 U.S.C. App.)); and 
"(iv) the Inspector General, or similar office, of a State or unit of local government.

"(7) 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.

"(8) PROHIBITION.—It shall be unlawful for any individual to knowingly—

"(1) prepare or submit, or assist in the submission of a Federal grant application.

"(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 misrepresentation; or 
"(B) contains a material misrepresenta—

"(c) EXCEPTION.—Subsection (b) does not apply to an activity—

"(1) carried out in connection with a lawful authority, that is, investigatory, protective, or intelligence activity of—

"(A) a law enforcement agency; or 
"(B) a Federal intelligence agency; or 
"(2) authorized under chapter 234. 

"(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) C LERICAL 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 AGENTS

(a) IN GENERAL.—The Secretary of State—

"(1) 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). 

"(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) C LERICAL 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. 
(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 whether the visa or other entry documentation is or was issued.

(B) IMMEDIATE EFFECT.—A revocation under clause (A) shall take effect immediately and may be effectuated even if admitting 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.

(c) REQUIREMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of 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, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Governmental 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 consultation 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.

(d) 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 Senate 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, 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 under this subsection 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 of 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 of the Senate, the Committee on Homeland Security and Governmental Affairs 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.

(a) REQUIREMENT.—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) include in the report on 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. PURPOSE.

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 the development of artificial intelligence that builds on the strengths of the United States in innovation and entrepreneurship;

(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 3052 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 Governmental Reform of the House of Representatives.

(3) ARTIFICIAL INTELLIGENCE.—The term “artificial intelligence” has the meaning given the term in section 261 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” means—

(A) 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 research, 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.

(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 261 of the AI appropriation 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”, published in April 2018;

(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 individual or entity the Director determines to be appropriate.

(b) DEPARTMENT POLICIES AND PROCESSES FOR PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES.—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 retraining of artificial intelligence-enabled systems; and

(2) the Chief Privacy Officer and the Chief Information Officers Council, the Chief Acquisition Officers Council, or the Director, in consultation with a working group consisting of members selected by the Director, in consultation with 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) the use of artificial intelligence by the Inspector General to enhance audit and investigatory capabilities, including actions—

(A) ensure the integrity of audit and investigatory 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 plan 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; and

(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 retraining as determined appropriate; 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—

(A) ensure that contracts for the acquisition of artificial intelligence systems; 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.

(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 on a quarterly basis thereafter, on the status of implementing 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, the Director, in coordination with the Chief Information Officers Council, the Chief Data Officers Council, and other interagency bodies as determined appropriate by the Director, shall identify 4 use cases for the application of artificial intelligence-enabled systems to support interagency or intragency modernization initiatives that require linking multiple systems, internal and external data sets, 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.—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 exist 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—

(A) prepare and maintain an inventory of the artificial intelligence use cases of the agencies, including current and planned uses; and

(B) develop a plan for the implementation of the inventory.

(3) USE CASE MODERNIZATION PLAN.—In carrying out paragraph (2), the Director shall—

(A) develop a risk mitigation plan to address 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 deployed artificial intelligence system to unauthorized manipulation or misuse.

(B) 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 at least 1 from each of the following categories:

(A) Applied artificial intelligence to drive agency productivity efficiencies in predicate supply chain and logistics, such as—

(i) predictive food demand and optimized supply;

(ii) predictive medical supplies and equipment management, including optimal third-party logistics; and

(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; 
(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 estimate economic and social benefits.

(6) MEASUREMENT. 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 agencies make faster and better decisions; 
(C) organizes data for meaningful data visualization and analysis so the Government has predictive awareness for situational awareness to improve use case outcomes; 
(D) is rapidly configurable to support multiple applications and automatically adapts to evolving conditions and 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) EARLIEST. 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.

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 INNOVATIONS.

(a) INNOVATIVE COMMERCIAL ITEMS.—Section 803 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 2101 of the Federal Acquisition Regulation; and 

‘‘(B) includes a commercial product or a commercial service, as defined in sections 1001 and 101, 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 inserting ‘‘2027’’.

(b) DHS OTHER TRANSACTION AUTHORITY.—Section 831 of the Homeland Security Act of 2002 (42 U.S.C. 7101 note) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking ‘‘September 30, 2027’’ 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 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. STRATEGIC PLAN FOR FEDERAL ELECTRIC VEHICLE FLEET.

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.

(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 develop and submit to the Congress a strategic plan for Federal electric vehicle fleet planning, budgeting, and operations.

(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) guidance on 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 determine to be necessary based on new information relating to electric vehicle battery technologies 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; and 

(3) the Chair of the Council on Environmental Quality; and 

(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.

SEC. 5244. STUDY OF FEDERAL FLEET VEHICLES.

(a) STUDY.—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 include the part of the Comptroller General’s annual reporting to committees of Congress—

(1) consolidate Matters for Congressional Accountability Office in one report organized by policy topic that includes the amount of time such Matters have been unimplemented and the status of such report in congressional leadership and the oversight committees of each House; and 

(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.

(b) PUBLICATION OF INFORMATION.—(1) The Comptroller General shall make publicly available the information described in paragraphs (1) and (2); and 

(2) 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 submit to either House of Congress or any committee of Congress or subcommittee thereof.

(B) EXCLUSIONS.—

(1) 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:

(A) the select committee on intelligence, the committee on armed services, the committee on appropriations, or the committee on foreign relations of the senate.

(B) 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.

(C) the term “director” means the director of the government publishing office.

(D) federal agency.—the term “federal agency” has the meaning given in the term “federal agency” under section 102 of title 44, United States code, but does not include the government accountability office or an element of the intelligence community.

(E) intelligence community.—the term “intelligence community” has the meaning given in that term in section 3 of the national security act of 1947 (50 u.s.c. 3003).

(f) portal.—

(A) establishment of online portal for congressionally mandated reports.—

(i) requirement to establish online portal.—

(A) 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.

(B) 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.

(ii) 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:

(A) a citation to the statute requiring the report.

(B) an electronic copy of the report, including any transmittal letter associated with 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) which of the 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 text search.

(x) full text search.

(xi) any other relevant information specified by the director.

(C) for congressionally mandated report on the online portal.

(i) 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) means for bulk download of all congressionally mandated reports.

(3) 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 fails to 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)(3)(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 not 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 date 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, which is not submitted to or published on the reports online portal if the chairman of a committee or subcommittee to which the report is submitted notifies the director that the report is to be withheld from submission and publication under this subtitle.

(f) 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 statement that the federal agency has withheld at the request of a committee or subcommittee involved; and

(g) free access.—the director may not charge a fee, require registration, or impose other limitation on exchange for access to the reports online portal.

(h) upgrade capability.—the reports online portal shall be enhanced and updated as necessary to carry out the purposes of this subtitle.

(i) 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 reports 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 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 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) WITHHOLDING INFORMATION.—In the case of congressional mandated reports submitted to Congress by a statute enacted before the date of the enactment of this Act, published on the reports online portal under this subtitle, 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 (2) be withheld under section 552a of title 5, United States Code, or that are required to be withheld under section 552a of title 5, United States Code.

(b) WITHHOLDING OF INFORMATION.—In the case of congressional mandated reports submitted for withholding information pursuant to the requirements of this section.

(c) ACCESS FOR CONGRESSIONAL LEADERSHIP.—Nothing in this subtitle or section 5256 shall preclude the congressional leadership from having access to the reports online portal.

(d) 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 which is enacted on or after the date of 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 submitted notifies the Director in writing that the report is to be withheld from publication; or (B) the Director publishes the notification on the reports online portal.

SEC. 5257. IMPLEMENTATION.

(a) REPORTS SUBMITTED TO CONGRESS.—In general.

(b) REPORT REQUIRED.—In the case of congressional mandated reports submitted to Congress by a statute enacted before the date of enactment of this Act, published on the reports online portal under 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.—In the case of congressional mandated information that is classified, or the public release of which could have a harmful effect on national security.

(b) LAW ENFORCEMENT SENSITIVE.—Nothing in this subtitle or any other provision of law, congressional committee a report including the following:

(1) The number of such members and their dependents described in subsection (a)(4).

(2) The number of such members and their dependents described in subsection (a)(4).

(3) The number of such members and their dependents described in subsection (a)(4).

(4) The number of such members and their dependents described in subsection (a)(4).

(5) The number of such members and their dependents described in subsection (a)(4).

(6) The number of such members and their dependents described in subsection (a)(4).

(b) REPORT REQUIRED.—In the case of congressional mandated reports submitted to Congress by a statute enacted before the date of enactment of this Act, published on the reports online portal under 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.—In the case of congressional mandated reports submitted to Congress by a statute enacted before the date of enactment of this Act, published on the reports online portal under 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.—In the case of congressional mandated reports submitted to Congress by a statute enacted before the date of enactment of this Act, published on the reports online portal under 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.—In the case of congressional mandated reports submitted to Congress by a statute enacted before the date of enactment of this Act, published on the reports online portal under 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.—In the case of congressional mandated reports submitted to Congress by a statute enacted before the date of enactment of this Act, published on the reports online portal under 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.—In the case of congressional mandated reports submitted to Congress by a statute enacted before the date of enactment of this Act, published on the reports online portal under this subtitle, the head of each Federal agency shall be responsible for withholding information pursuant to the requirements of this section.

SEC. 5257. IMPLEMENTATION.