and onerous to navigate and rarely result in permission to return;

Whereas individuals wrongfully or unjustly deported from the United States include—

(1) individuals who have been separated from their children, families, and loved ones after residing in the United States for years or decades;

(2) recipients of deferred action under the Deferred Action for Childhood Arrivals program who lost such status as a result of protracted litigation related to the program;

(3) individuals targeted for deportation as retaliation for exercising their right under the First Amendment to the Constitution of the United States to protest conditions in the immigration system;

(4) individuals who have succeeded in winning their immigration cases after deportation but nevertheless are unable to return to the United States;

(5) individuals deported for past nonviolent criminal convictions who have subsequently demonstrated a commitment to renewal and to their community;

(6) individuals whose criminal convictions that were the basis of deportation have been expunged or pardoned; and

(7) veterans who served the United States;

Whereas, by permanently separating individuals from their children, spouses, and communities, deportation leads to destabilizing and enduring poverty, food and housing insecurity, and irreparable psychological harm to children left behind;

Whereas many deported individuals are sent back to dangerous conditions that pose a significant risk to their lives and wellbeing, or to countries where they have no personal ties at all;

Whereas the harms of deportation disproportionately affect Black and brown immigrant families, who are over-represented within the deportation system;

Whereas the Immigration Nationality Act (8 U.S.C. 1101 et seq.), relevant regulations, and Federal agency policy do include certain legal mechanisms and avenues designed to allow an individual to present a case for return after deportation (including through procedures to reopen a closed immigration court case), to effectuate return upon prevailing on an appeal, and to seek discretionary authority to return; however, such mechanisms intended by Congress and the relevant Federal agencies to remedy wrongful or unjust deportations are largely ineffective and insufficient due to a decentralized review process, associated lengthy wait times, complicated and opaque application procedures, little to no access to counsel, and a lack of resources for line-level decisionmakers with the Department of Homeland Security to meaningfully consider such cases;

Whereas a centralized, dedicated unit within the Department of Homeland Security that offers a fair and independent process for reviewing applications from individuals seeking to return to the United States after a wrongful or unjust deportation would ensure greater fairness and consistency in adjudication, alleviate the burden on individual Government attorneys and immigration courts, and reorient the Department of Homeland Security toward remedying past wrongful or unjust deportation decisions;

Whereas such a unit could exercise the legal and discretionary authority already provided under Federal law to facilitate the return of individuals whose removal orders were contrary to law or justice;

Whereas the Department of Homeland Security has already established a successful central removal review unit, known as ''ImmVets'', for the repatriation of wrongfully or unjustly deported United States veterans, including approximately 100 such veterans who have returned to the United States after deportation, which demonstrates the feasibility and effectiveness of such an approach;

Whereas establishing such a unit is wholly within the broad legal authority of the Department of Homeland Security and would bring fairness and credibility to the United States immigration system; and

Whereas bringing home wrongfully or unjustly deported fathers, mothers, community leaders, and workers is essential for moving toward an immigration system that prioritizes family unity, community wellbeing, economic prosperity, and basic due process: Now, therefore, be it

Resolved by the Senate (the House of Representatives concurring), That it is the sense of Congress that wrongfully or unjustly deported individuals deserve a meaningful chance to come home to the United States and reunite with their loved ones through a centralized unit within the Department of Homeland Security dedicated to reviewing requests for return to the United States.

AMENDMENTS SUBMITTED AND PROPOSED

SA 3207. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 4638, to authorize appropriations for fiscal year 2025 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.

SA 3208. Mr. SCOTT of South Carolina submitted an amendment intended to be proposed by him to the bill S. 4638, supra; which was ordered to lie on the table.

SA 3209. Mr. RUBIO (for Mr. WARNER (for himself and Mr. RUBIO)) submitted an amendment intended to be proposed by Mr. RUBIO to the bill S. 4638, supra; which was ordered to lie on the table.

SA 3210. Mr. HICKENLOOPER (for himself and Ms. LUMMIS) submitted an amendment intended to be proposed by him to the bill S. 4638, supra; which was ordered to lie on the table.

SA 3211. Ms. HIRONO (for herself, Mr. SCHATZ, and Mr. CORNYN) submitted an amendment intended to be proposed by her to the bill S. 4638, supra; which was ordered to lie on the table.

SA 3212. Mr. BROWN submitted an amendment intended to be proposed by him to the bill S. 4638, supra; which was ordered to lie on the table.

SA 3213. Ms. CORTEZ MASTO (for herself and Mr. RISCH) submitted an amendment intended to be proposed by her to the bill S. 4638, supra; which was ordered to lie on the table.

SA 3214. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill H.R. 7024, to make improvements to the child tax credit, to provide tax incentives to promote economic growth, to provide special rules for the taxation of certain residents of Taiwan with income from sources within the United States, to provide tax relief with respect to certain Federal disasters, to make improvements to the low-income housing tax credit, and for other purposes; which was ordered to lie on the table.

SA 3215. Mr. WELCH (for Mr. HEINRICH (for himself and Mr. RISCH)) proposed an amendment to the bill S. 2781, to promote remediation of abandoned hardrock mines, and for other purposes.

TEXT OF AMENDMENTS

SA 3207. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 4638, to authorize appropriations for fiscal year 2025 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

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

SEC. 1239. SPECIAL ENVOY FOR BELARUS.

Section 6406(d) of the Defense of State Authorization Act for Fiscal Year 2023 (division F of Public Law 118–31; 22 U.S.C. 5811 note) is amended by striking paragraphs (1) through (5) and inserting the following:

''(1) shall only exist while United States diplomatic operations in Belarus at the United States Embassy in Minsk, Belarus are suspended; and

''(2) shall oversee the operations and personnel of the Belarus Affairs Unit.''.

SA 3208. Mr. SCOTT of South Carolina submitted an amendment intended to be proposed by him to the bill S. 4638, to authorize appropriations for fiscal year 2025 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

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

SEC. 1272. REPORTS ON FOREIGN BOYCOTTS OF ISRAEL.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter, the head of the Office of Antiboycott Compliance of the Bureau of Industry and Security of the Department of Commerce shall submit to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Foreign Affairs of the House of Representatives a report on boycotts described in section 1773(a) of the Anti-Boycott Act of 2018 (50 U.S.C. 4842(a)) targeted at the State of Israel.

(b) ELEMENTS.—The report required by subsection (a) shall include a description of—

(1) boycotts described in that subsection; and

(2) the steps taken by the Department of Commerce to enforce the provisions of the Anti-Boycott Act of 2018 (50 U.S.C. 4841 et seq.) with respect to those boycotts.

(c) TERMINATION.—The requirement to submit reports under subsection (a) shall terminate on the date that is 5 years after the date of the enactment of this Act.

SA 3209. Mr. RUBIO (for Mr. WARNER (for himself and Mr. RUBIO)) submitted an amendment intended to be proposed by Mr. Rubio to the bill S. 4638, to authorize appropriations for fiscal year 2025 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

DIVISION ____—INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2025

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This division may be cited as the ''Intelligence Authorization Act for Fiscal Year 2025''.

(b) TABLE OF CONTENTS.—The table of contents for this division is as follows:

SEC. 2. DEFINITIONS.

In this Act:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ''congressional intelligence committees'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given such term in such section.

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2025 for the conduct of

the intelligence and intelligence-related activities of the Federal Government.

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) SPECIFICATIONS OF AMOUNTS.—The amounts authorized to be appropriated under section 101 for the conduct of the intelligence activities of the Federal Government are those specified in the classified Schedule of Authorizations prepared to accompany this division.

(b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AUTHORIZATIONS.—

(1) AVAILABILITY.—The classified Schedule of Authorizations referred to in subsection (a) shall be made available to the Committee on Appropriations of the Senate, the Committee on Appropriations of the House of Representatives, and to the President.

(2) DISTRIBUTION BY THE PRESIDENT.—Subject to paragraph (3), the President shall provide for suitable distribution of the classified Schedule of Authorizations referred to in subsection (a), or of appropriate portions of such Schedule, within the executive branch of the Federal Government.

(3) LIMITS ON DISCLOSURE.—The President shall not publicly disclose the classified Schedule of Authorizations or any portion of such Schedule except—

(A) as provided in section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 3306(a));

(B) to the extent necessary to implement the budget; or

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2025 the sum of $656,573,000.

(b) CLASSIFIED AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2025 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a).

SEC. 104. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY LAW.

Appropriations authorized by this division for salary, pay, retirement, and other benefits for Federal employees may be increased by such additional or supplemental amounts as may be necessary for increases in such compensation or benefits authorized by law.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund $514,000,000 for fiscal year 2025.

TITLE III—INTELLIGENCE COMMUNITY MATTERS

SEC. 301. IMPROVEMENTS RELATING TO CONFLICTS OF INTEREST IN THE INTELLIGENCE INNOVATION BOARD.

Section 7506(g) of the Intelligence Authorization Act for Fiscal Year 2024 (Public Law 118–31) is amended—

(1) in paragraph (2)—

(A) in subparagraph (A), by inserting ''active and'' before ''potential'';

(B) in subparagraph (B), by striking ''the Inspector General of the Intelligence Community'' and inserting ''the designated agency ethics official'';

(C) by redesignating subparagraph (C) as subparagraph (D); and

(D) by inserting after subparagraph (B) the following:

''(C) Authority for the designated agency ethics official to grant a waiver for a conflict of interest, except that—

''(i) no waiver may be granted for an active conflict of interest identified with respect to the Chair of the Board;

''(ii) every waiver for a potential conflict of interest requires review and approval by the Director of National Intelligence; and

''(iii) for every waiver granted, the designated agency ethics official shall submit to the congressional intelligence committees notice of the waiver.''; and

(2) by adding at the end the following:

''(3) DEFINITION OF DESIGNATED AGENCY ETHICS OFFICIAL.—In this subsection, the term 'designated agency ethics official' means the designated agency ethics official (as defined in section 13101 of title 5, United States Code) in the Office of the Director of National Intelligence.''.

SEC. 302. NATIONAL THREAT IDENTIFICATION AND PRIORITIZATION ASSESSMENT AND NATIONAL COUNTERINTELLIGENCE STRATEGY.

Section 904(f)(3) of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3383(f)(3)) is amended by striking ''National Counterintelligence Executive'' and inserting ''Director of the National Counterintelligence and Security Center''.

SEC. 303. OPEN SOURCE INTELLIGENCE DIVISION OF OFFICE OF INTELLIGENCE AND ANALYSIS PERSONNEL.

None of the funds authorized to be appropriated by this division for the Office of Intelligence and Analysis of the Department of Homeland Security may be obligated or expended by the Office to increase, above the staffing level in effect on the day before the date of the enactment of this Act, the number of personnel assigned to the Open Source Intelligence Division who work exclusively or predominantly on domestic terrorism issues.

SEC. 304. IMPROVEMENTS TO ADVISORY BOARD OF NATIONAL RECONNAISSANCE OFFICE.

Section 106A(d) of the National Security Act of 1947 (50 U.S.C. 3041a(d)) is amended—

(1) in paragraph (3)(A)—

(A) in clause (i)—

(i) by striking ''five members appointed by the Director'' and inserting ''up to 8 members appointed by the Director''; and

(ii) by inserting '', and who do not present any actual or potential conflict of interest'' before the period at the end;

(B) by redesignating clause (ii) as clause (iii); and

(C) by inserting after clause (i) the following:

''(ii) MEMBERSHIP STRUCTURE.—The Director shall ensure that no more than 2 concurrently serving members of the Board qualify for membership on the Board based predominantly on a single qualification set forth under clause (i).'';

(2) by redesignating paragraphs (5) through (7) as paragraphs (6) through (8), respectively;

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

''(5) CHARTER.—The Director shall establish a charter for the Board that includes the following:

''(A) Mandatory processes for identifying potential conflicts of interest, including the submission of initial and periodic financial disclosures by Board members.

''(B) The vetting of potential conflicts of interest by the designated agency ethics official, except that no individual waiver may be granted for a conflict of interest identified with respect to the Chair of the Board.

''(C) The establishment of a process and associated protections for any whistleblower alleging a violation of applicable conflict of interest law, Federal contracting law, or other provision of law.''; and

(4) in paragraph (8), as redesignated by paragraph (2), by striking ''September 30, 2024'' and inserting ''August 31, 2027''.

SEC. 305. NATIONAL INTELLIGENCE UNIVERSITY ACCEPTANCE OF GRANTS.

(a) IN GENERAL.—Subtitle D of title X of the National Security Act of 1947 (50 U.S.C. 3227 et seq.) is amended by adding at the end the following:

''§ 1035. National Intelligence University acceptance of grants

''(a) AUTHORITY.—The Director of National Intelligence may authorize the President of the National Intelligence University to accept qualifying research grants.

''(b) QUALIFYING GRANTS.—A qualifying research grant under this section is a grant that is awarded on a competitive basis by an entity referred to in subsection (c) for a research project with a scientific, literary, or educational purpose.

''(c) ENTITIES FROM WHICH GRANTS MAY BE ACCEPTED.—A qualifying research grant may be accepted under this section only from a Federal agency or from a corporation, fund, foundation, educational institution, or similar entity that is organized and operated primarily for scientific, literary, or educational purposes.

''(d) ADMINISTRATION OF GRANT FUNDS.—

''(1) ESTABLISHMENT OF ACCOUNT.—The Director shall establish an account for administering funds received as qualifying research grants under this section.

''(2) USE OF FUNDS.—The President of the University shall use the funds in the account established pursuant to paragraph (1) in accordance with applicable provisions of the regulations and the terms and conditions of the grants received.

''(e) RELATED EXPENSES.—Subject to such limitations as may be provided in appropriations Acts, appropriations available for the National Intelligence University may be used to pay expenses incurred by the University in applying for, and otherwise pursuing, the award of qualifying research grants.

''(f) REGULATIONS.—The Director of National Intelligence shall prescribe regulations for the administration of this section.''.

(b) CLERICAL AMENDMENT.—The table of contents preceding section 2 of such Act is amended by inserting after the item relating to section 1034 the following new item:

''Sec. 1035. National Intelligence University acceptance of grants.''.

SEC. 306. LIMITATION ON AVAILABILITY OF FUNDS FOR NEW CONTROLLED ACCESS PROGRAMS.

None of the funds authorized to be appropriated by this division for the National Intelligence Program (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) may be obligated or expended for any controlled access program (as defined in section 501A(d) of the National Security Act of 1947 (50 U.S.C. 3091a(d))), or a compartment or subcompartment therein, that is established on or after the date of the enactment of this Act, until the head of the element of the intelligence community responsible for the establishment of such program, compartment, or subcompartment, submits the notification required by section 501A(b) of the National Security Act of 1947 (50 U.S.C. 3091a(b)).

SEC. 307. LIMITATION ON TRANSFERS FROM CONTROLLED ACCESS PROGRAMS.

Section 501A(b) of the National Security Act of 1947 (50 U.S.C. 3091a(b)) is amended—

(1) in the subsection heading, by striking ''LIMITATION ON ESTABLISHMENT'' and inserting ''LIMITATIONS'';

(2) by striking ''A head'' and inserting the following:

''(1) ESTABLISHMENT.—A head''; and

(3) by adding at the end the following:

''(2) TRANSFERS.—A head of an element of the intelligence community may not transfer a capability from a controlled access program, including from a compartment or subcompartment therein to a compartment or subcompartment of another controlled access program, to a special access program (as defined in section 1152(g) of the National Defense Authorization Act for Fiscal Year 1994 (50 U.S.C. 3348(g))), or to anything else outside the controlled access program, until the head submits to the appropriate congressional committees and congressional leadership notice of the intent of the head to make such transfer.''.

SEC. 308. EXPENDITURE OF FUNDS FOR CERTAIN INTELLIGENCE AND COUNTERINTELLIGENCE ACTIVITIES OF THE COAST GUARD.

The Commandant of the Coast Guard may use up to 1 percent of the amounts made available for the National Intelligence Program (as such term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) for each fiscal year for intelligence and counterintelligence activities of the Coast Guard relating to objects of a confidential, extraordinary, or emergency nature, which amounts may be accounted for solely on the certification of the Commandant and each such certification shall be considered to be a sufficient voucher for the amount contained in the certification.

SEC. 309. STRENGTHENING OF OFFICE OF INTELLIGENCE AND ANALYSIS.

(a) IMPROVEMENTS.—

(1) IN GENERAL.—Section 311 of title 31, United States Code, is amended to read as follows:

''§ 311. Office of Economic Intelligence and Security

''(a) DEFINITIONS.—In this section, the terms 'counterintelligence', 'foreign intelligence', and 'intelligence community' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

''(b) ESTABLISHMENT.—There is established within the Office of Terrorism and Financial Intelligence of the Department of the Treasury, the Office of Economic Intelligence and Security (in this section referred to as the 'Office'), which, subject to the availability of appropriations, shall—

''(1) be responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information relating to the operation and responsibilities of the Department of the Treasury and other Federal agencies executing economic statecraft tools that do not include any elements that are elements of the intelligence community;

''(2) provide intelligence support and economic analysis to Federal agencies implementing United States economic policy, including for purposes of global strategic competition; and

''(3) have such other related duties and authorities as may be assigned by the Secretary for purposes of the responsibilities described in paragraph (1), subject to the authority, direction, and control of the Secretary, in consultation with the Director of National Intelligence.

''(c) ASSISTANT SECRETARY FOR ECONOMIC INTELLIGENCE AND SECURITY.—The Office shall be headed by an Assistant Secretary, who shall be appointed by the President, by and with the advice and consent of the Senate. The Assistant Secretary shall report directly to the Undersecretary for Terrorism and Financial Crimes.''.

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 3 of such title is amended by striking the item relating to section 311 and inserting the following:

''311. Office of Economic Intelligence and Security.''.

(3) CONFORMING AMENDMENT.—Section 3(4)(J) of the National Security Act of 1947 (50 U.S.C. 3003(4)(J)) is amended by striking ''Office of Intelligence and Analysis'' and inserting ''Office of Economic Intelligence and Security''.

(4) REFERENCES.—Any reference in a law, regulation, document, paper, or other record of the United States to the Office of Intelligence and Analysis of the Department of the Treasury shall be deemed a reference to the Office of Economic Intelligence and Security of the Department of the Treasury.

(b) STRATEGIC PLAN AND EFFECTIVE DATE.—

(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

(B) the Committee on Banking, Housing, and Urban Affairs and the Committee on Appropriations of the Senate; and

(C) the Committee on Financial Services and the Committee on Appropriations of the House of Representatives.

(2) IN GENERAL.—Subsection (a) shall take effect on the date that is 180 days after the date on which the Secretary of the Treasury submits to the appropriate committees of Congress a 3-year strategic plan detailing the resources required by the Department of the Treasury.

(3) CONTENTS.—The strategic plan submitted pursuant to paragraph (2) shall include the following:

(A) Staffing and administrative expenses planned for the Department for the 3-year period beginning on the date of the submittal of the plan, including resourcing requirements for each office and division in the Department during such period.

(B) Stuctural changes and resources, including leadership structure and staffing, required to implement subsection (a) during the period described in subparagraph (A).

(c) LIMITATION.—None of the amounts appropriated or otherwise made available before the date of the enactment of this Act for the Office of Foreign Asset Control, the Financial Crimes Enforcement Network, the Office of International Affairs, the Office of Tax Policy, or the Office of Domestic Finance may be transferred or reprogrammed to support the Office of Economic Intelligence and Security established by section 311 of title 31, United States Code, as added by subsection (a).

SEC. 310. REPORT ON COLLECTION OF UNITED STATES LOCATION INFORMATION.

(a) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees;

(B) the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, and the Committee on Commerce, Science, and Transportation of the Senate; and

(C) the Committee on the Judiciary, the Committee on Homeland Security, and the Committee on Energy and Commerce of the House of Representatives.

(2) UNITED STATES LOCATION INFORMATION.—The term ''United States location information'' means information derived or otherwise calculated from the use of technology, including global positioning systems-level latitude and longitude coordinates or other mechanisms, that reveals the past or present approximate or specific location of a customer, subscriber, user, or device in the United States, or, if the customer, subscriber, or user is known to be a United States person, outside the United States.

(3) UNITED STATES PERSON.—The term ''United States person'' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Attorney General, shall issue a report on the collection of United States location information by the intelligence community.

(c) CONTENT.—The report required by subsection (a) shall address the filtering, segregation, use, dissemination, masking, and retention of United States location information by the intelligence community.

(d) FORM; PUBLIC AVAILABILITY.—The report required by subsection (a)—

(1) shall be issued in unclassified form and made available to the public; and

(2) may include a classified annex, which the Director of National Intelligence shall submit to the appropriate committees of Congress.

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as authorizing—

(1) any rulemaking; or

(2) the collection or access of United States location information.

TITLE IV—COUNTERING FOREIGN THREATS

Subtitle A—People's Republic of China

SEC. 401. ASSESSMENT OF CURRENT STATUS OF BIOTECHNOLOGY OF PEOPLE'S REPUBLIC OF CHINA.

(a) ASSESSMENT.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the Director of the National Counterproliferation and Biosecurity Center and such heads of elements of the intelligence community as the Director of National Intelligence considers appropriate, conduct an assessment of the current status of the biotechnology of the People's Republic of China, which shall include an assessment of how the People's Republic of China is supporting the biotechnology sector through both licit and illicit means, such as foreign direct investment, subsidies, talent recruitment, or other efforts.

(b) REPORT.—

(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

(B) the Committee on Finance, the Committee on Foreign Relations, the Committee on the Judiciary, the Committee on Banking, Housing, and Urban Affairs, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(C) the Committee on Ways and Means, the Committee on Foreign Affairs, the Committee on the Judiciary, the Committee on Financial Services, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(2) IN GENERAL.—Not later than 30 days after the date on which the Direct of National Intelligence completes the assessment required by subsection (a), the Director shall submit to the appropriate committees of Congress a report on the findings of the Director with respect to the assessment.

(3) FORM.—The report submitted pursuant to paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

SEC. 402. INTELLIGENCE SHARING WITH LAW ENFORCEMENT AGENCIES ON SYNTHETIC OPIOID PRECURSOR CHEMICALS ORIGINATING IN PEOPLE'S REPUBLIC OF CHINA.

(a) STRATEGY REQUIRED.—The Director of National Intelligence shall, in coordination with the Attorney General, the Secretary of Homeland Security, the Secretary of State, the Secretary of the Treasury, and the heads of such other departments and agencies as the Director considers appropriate, develop a strategy to ensure robust intelligence sharing relating to the illicit trafficking of synthetic opioid precursor chemicals from the People's Republic of China and other source countries.

(b) ELEMENTS.—The strategy developed pursuant to subsection (a) shall include the following:

(1) An assessment of existing intelligence sharing between the intelligence community, the Department of Justice, the Department of Homeland Security, any other relevant Federal departments, and State, local, territorial and tribal law enforcement entities, including any mechanisms that allow subject matter experts with and without security clearances to share and receive information and any gaps identified.

(2) A plan to ensure robust intelligence sharing, including by addressing gaps identified pursuant to subparagraph (1) and identifying additional capabilities and resources needed;

(3) A detailed description of the measures used to ensure the protection of civil rights, civil liberties, and privacy rights in carrying out this strategy.

SEC. 403. REPORT ON EFFORTS OF THE PEOPLE'S REPUBLIC OF CHINA TO EVADE UNITED STATES TRANSPARENCY AND NATIONAL SECURITY REGULATIONS.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Finance, the Committee on Foreign Relations, the Committee on Commerce, Science, and Transportation, the Committee on the Judiciary, the Committee on Banking, Housing, and Urban Affairs, the Committee on Homeland Security and Governmental Affairs, and the Committee on Armed Services of the Senate; and

(3) the Committee on Ways and Means, the Committee on Foreign Affairs, the Committee on Energy and Commerce, the Committee on the Judiciary, the Committee on Financial Services, the Committee on Homeland Security, and the Committee on Armed Services of the House of Representatives.

(b) REPORT REQUIRED.—The Director of National Intelligence shall submit to the appropriate committees of Congress a report on efforts of the People's Republic of China to evade the following:

(1) Identification under section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 10 U.S.C. 113 note).

(2) Restrictions or limitations imposed by any of the following:

(A) Section 805 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118–31).

(B) Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 41 U.S.C. 3901 note prec.).

(C) The list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury (commonly known as the ''SDN list'').

(D) The Entity List maintained by the Bureau of Industry and Security of the Department of Commerce and set forth in Supplement No. 4 to part 744 of title 15, Code of Federal Regulations.

(E) Commercial or dual-use export controls under the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.) and the Export Administration Regulations.

(F) Executive Order 14105 (88 Fed. Reg. 54867; relating to addressing United States investments in certain national security technologies and products in countries of concern), or successor order.

(G) Import restrictions on products made with forced labor implemented by U.S. Customs and Border Protection pursuant to Public Law 117–78 (22 U.S.C. 6901 note).

(c) FORM.—The report submitted pursuant to subsection (b) shall be submitted in unclassified form.

SEC. 404. PLAN FOR RECRUITMENT OF MANDARIN SPEAKERS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate congressional committees a comprehensive plan to prioritize the recruitment and training of individuals who speak Mandarin Chinese for each element of the intelligence community.

(b) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term ''appropriate congressional committees'' means—

(1) the congressional intelligence committees;

(2) the Committee on the Judiciary and the Committee on Appropriations of the Senate; and

(3) the Committee on the Judiciary and the Committee on Appropriations of the House of Representatives.

Subtitle B—The Russian Federation

SEC. 411. REPORT ON RUSSIAN FEDERATION SPONSORSHIP OF ACTS OF INTERNATIONAL TERRORISM.

(a) DEFINITIONS.—In this section—

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

(A) the congressional intelligence committees;

(B) the Committee on Foreign Relations, the Committee on Armed Services, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, and the Committee on Appropriations of the Senate; and

(C) the Committee on Foreign Affairs, the Committee on Armed Services, the Committee on the Judiciary, the Committee on Homeland Security, the Committee on Financial Services, and the Committee on Appropriations of the House of Representatives.

(2) FOREIGN TERRORIST ORGANIZATION.—The term ''foreign terrorist organization'' means an organization that has been designated as a foreign terrorist organization by the Secretary of State, pursuant to section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(3) SPECIALLY DESIGNATED GLOBAL TERRORIST ORGANIZATION.—The term ''specially designated global terrorist organization'' means an organization that has been designated as a specially designated global terrorist by the Secretary of State or the Secretary, pursuant to Executive Order 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism).

(4) STATE SPONSOR OF TERRORISM.—The term ''state sponsor of terrorism'' means a country the government of which the Secretary of State has determined has repeatedly provided support for acts of international terrorism, for purposes of—

(A) section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (50 U.S.C. 4813(c)(1)(A)(i));

(B) section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. 2371);

(C) section 40(d) of the Arms Export Control Act (22 U.S.C. 2780(d)); or

(D) any other provision of law.

(b) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in concurrence with the Secretary of State, conduct and submit to the appropriate congressional committees a report that includes the following:

(1) A list of all instances in which the Russian Federation, or an official of the Russian Federation, has provided financial, material, technical, or lethal support to foreign terrorist organizations, specially designated global terrorist organizations, state sponsors of terrorism, or for acts of international terrorism.

(2) A list of all instances in which the Russian Federation, or an official of the Russian Federation, has willfully aided or abetted—

(A) the international proliferation of nuclear explosive devices to persons;

(B) a person in acquiring unsafeguarded special nuclear material; or

(C) the efforts of a person to use, develop, produce, stockpile, or otherwise acquire chemical, biological, or radiological weapons.

(3) An assessment of threats to the homeland as a result of Russian government assistance to the Russian Imperial Movement.

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

(d) BRIEFINGS.—Not later than 30 days after submittal of the report required by subsection (b), the Director of National Intelligence shall provide a classified briefing to the appropriate congressional committees on the methodology and findings of the report.

SEC. 412. ASSESSMENT OF LIKELY COURSE OF WAR IN UKRAINE.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services, the Committee on Foreign Relations and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services, the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives.

(b) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in collaboration with the Director of the Defense Intelligence Agency and the Director of the Central Intelligence Agency, shall submit to the appropriate committees of Congress an assessment of the likely course of the war in Ukraine through December 31, 2025.

(c) ELEMENTS.—The assessment required by subsection (b) shall include an assessment of each of the following:

(1) The ability of the military of Ukraine to defend against Russian aggression if the United States does, or does not, continue to provide military and economic assistance to Ukraine and does, or does not, maintain policy restrictions on the use of United States weapons during the period described in such subsection.

(2) The likely course of the war during such period if the United States does, or does

not, continue to provide military and economic assistance to Ukraine.

(3) The ability and willingness of countries in Europe and outside of Europe to continue to provide military and economic assistance to Ukraine if the United States does, or does not, do so, including the ability of such countries to make up for any shortfall in United States assistance.

(4) The effects of a potential defeat of Ukraine by the Russian Federation on United States national security and foreign policy interests, including the potential for further aggression from the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, and the Democratic People's Republic of Korea.

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

Subtitle C—International Terrorism

SEC. 421. ASSESSMENT AND REPORT ON THE THREAT OF ISIS-KHORASAN TO THE UNITED STATES.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Foreign Relations, the Committee on Commerce, Science, and Transportation, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(3) the Committee on Foreign Affairs, the Committee on Transportation and Infrastructure, the Committee on the Judiciary, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(b) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Director of the National Counterterrorism Center, in coordination with such elements of the intelligence community as the Director considers relevant, shall—

(1) conduct an assessment of the threats to the United States and United States citizens posed by ISIS-Khorasan; and

(2) submit to the appropriate committees of Congress a written report on the findings of the assessment.

(c) REPORT ELEMENTS.—The report required by subsection (b) shall include the following:

(1) A description of the historical evolution of ISIS-Khorasan, beginning with Al-Qaeda and the attacks on the United States on September 11, 2001.

(2) A description of the ideology and stated intentions of ISIS-Khorasan as related to the United States and the interests of the United States, including the homeland.

(3) A list of all terrorist attacks worldwide attributable to ISIS-Khorasan or for which ISIS-Khorasan claimed credit, beginning on January 1, 2015.

(4) A description of the involvement of ISIS-Khorasan in Afghanistan before, during, and after the withdrawal of United States military and civilian personnel and resources in August 2021.

(5) The recruiting and training strategy of ISIS-Khorasan following the withdrawal described in paragraph (4), including—

(A) the geographic regions in which ISIS-Khorasan is physically present;

(B) regions from which ISIS-Khorasan is recruiting; and

(C) its ambitions for individual actors worldwide and in the United States.

(6) A description of the relationship between ISIS-Khorasan and ISIS core, the Taliban, Al-Qaeda, and other terrorist groups, as appropriate.

(7) A description of the association of members of ISIS-Khorasan with individuals formerly detained at United States Naval Station, Guantanamo Bay, Cuba.

(8) A description of ISIS-Khorasan's development of, and relationships with, travel facilitation networks in Europe, Central Asia, Eurasia, and Latin America.

(9) An assessment of ISIS-Khorasan's understanding of the border and immigration policies of the United States.

(10) An assessment of the known travel of members of ISIS-Khorasan within the Western Hemisphere and specifically across the southern border of the United States.

(11) As assessment of ISIS-Khorasan's intentions and capabilities within the United States.

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

Subtitle D—Other Foreign Threats

SEC. 431. ASSESSMENT OF VISA-FREE TRAVEL TO AND WITHIN WESTERN HEMISPHERE BY NATIONALS OF COUNTRIES OF CONCERN.

(a) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees;

(B) the Committee on Foreign Relations, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(C) the Committee on Foreign Affairs, the Committee on the Judiciary, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(2) COUNTRIES OF CONCERN.—The term ''countries of concern'' means—

(A) the Russian Federation;

(B) the People's Republic of China;

(C) the Islamic Republic of Iran;

(D) the Syrian Arab Republic;

(E) the Democratic People's Republic of Korea;

(F) the Bolivarian Republic of Venezuela; and

(G) the Republic of Cuba.

(b) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a written assessment of the impacts to national security caused by travel without a visa to and within countries in the Western Hemisphere by nationals of countries of concern.

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

SEC. 432. ASSESSMENT OF THREAT POSED BY CITIZENSHIP-BY-INVESTMENT PROGRAMS.

(a) DEFINITIONS.—In this section:

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

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Appropriations of the Senate; and

(B) the Committee on Homeland Security, the Committee on Foreign Affairs, the Committee on Financial Services, the Permanent Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Appropriations of the House of Representatives.

(2) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury.

(3) CITIZENSHIP-BY-INVESTMENT PROGRAM.—The term ''citizenship-by-investment program'' means an immigration, investment, or other program of a foreign country that, in exchange for a covered contribution, authorizes the individual making the covered contribution to acquire citizenship in such country, including temporary or permanent residence that may serve as the basis for subsequent naturalization.

(4) COVERED CONTRIBUTION.—The term ''covered contribution'' means—

(A) an investment in, or a monetary donation or any other form of direct or indirect capital transfer to, including through the purchase or rental of real estate—

(i) the government of a foreign country; or

(ii) any person, business, or entity in such a foreign country; and

(B) a donation to, or endowment of, any activity contributing to the public good in such a foreign country.

(5) DIRECTOR.—The term ''Director'' means the Director of National Intelligence.

(b) ASSESSMENT OF THREAT POSED BY CITIZENSHIP-BY-INVESTMENT PROGRAMS.—

(1) ASSESSMENT.—Not later than 1 year after the date of the enactment of this Act, the Director and the Assistant Secretary, in coordination with the heads of the other elements of the intelligence community and the head of any appropriate Federal agency, shall complete an assessment of the threat posed to the United States by citizenship-by-investment programs.

(2) ELEMENTS.—The assessment required by paragraph (1) shall include the following:

(A) An identification of each citizenship-by-investment program, including an identification of the foreign country that operates each such program.

(B) With respect to each citizenship-by-investment program identified under subparagraph (A)—

(i) a description of the types of investments required under the program; and

(ii) an identification of the sectors to which an individual may make a covered contribution under the program.

(C) An assessment of the threats posed to the national security of the United States by malign actors that use citizenship-by-investment programs—

(i) to evade sanctions or taxes;

(ii) to facilitate or finance—

(I) crimes relating to national security, including terrorism, weapons trafficking or proliferation, cybercrime, drug trafficking, human trafficking, and espionage; or

(II) any other activity that furthers the interests of a foreign adversary or undermines the integrity of the immigration laws or security of the United States; or

(iii) to undermine the United States and its interests through any other means identified by the Director and the Assistant Secretary.

(D) An identification of the foreign countries the citizenship-by-investment programs of which pose the greatest threat to the national security of the United States.

(3) REPORT AND BRIEFING.—

(A) REPORT.—

(i) IN GENERAL.—Not later than 180 days after completing the assessment required by paragraph (1), the Director and the Assistant Secretary shall jointly submit to the appropriate committees of Congress a report on the findings of the Director and the Assistant Secretary with respect to the assessment.

(ii) ELEMENTS.—The report required by clause (i) shall include the following:

(I) A detailed description of the threats posed to the national security of the United States by citizenship-by-investment programs.

(II) Recommendations for additional resources or authorities necessary to counter such threats.

(III) A description of opportunities to counter such threats.

(iii) FORM.—The report required by clause (i) shall be submitted in unclassified form but may include a classified annex, as appropriate.

(B) BRIEFING.—Not later than 90 days after the date on which the report required by subparagraph (A) is submitted, the Director and Assistant Secretary shall provide the appropriate committees of Congress with a briefing on the report.

SEC. 433. OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE REVIEW OF VISITORS AND ASSIGNEES.

(a) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees;

(B) the Committee on Armed Services, the Committee on Energy and Natural Resources, the Committee on Foreign Relations, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(C) the Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Foreign Affairs, the Committee on the Judiciary, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(2) COUNTRY OF RISK.—The term ''country of risk'' means a country identified in the report submitted to Congress by the Director of National Intelligence in 2024 pursuant to section 108B of the National Security Act of 1947 (50 U.S.C. 3043b) (commonly referred to as the ''Annual Threat Assessment'').

(3) COVERED ASSIGNEE; COVERED VISITOR.—The terms ''covered assignee'' and ''covered visitor'' mean a foreign national from a country of risk that is ''engaging in competitive behavior that directly threatens U.S. national security'', who is not an employee of either the Department of Energy or the management and operations contractor operating a National Laboratory on behalf of the Department of Energy, and has requested access to the premises, information, or technology of a National Laboratory.

(4) DIRECTOR.—The term ''Director'' means the Director of the Office of Intelligence and Counterintelligence of the Department of Energy (or their designee).

(5) FOREIGN NATIONAL.—The term ''foreign national'' has the meaning given the term ''alien'' in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

(6) NATIONAL LABORATORY.—The term ''National Laboratory'' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(7) NONTRADITIONAL COLLECTION THREAT.—The term ''nontraditional collection threat'' means a threat posed by an individual not employed by a foreign intelligence service, who is seeking access to information about a capability, research, or organizational dynamics of the United States to inform a foreign adversary or non-state actor.

(b) FINDINGS.—The Senate finds the following:

(1) The National Laboratories conduct critical, cutting-edge research across a range of scientific disciplines that provide the United States with a technological edge over other countries.

(2) The technologies developed in the National Laboratories contribute to the national security of the United States, including classified and sensitive military technology and dual-use commercial technology.

(3) International cooperation in the field of science is critical to the United States maintaining its leading technological edge.

(4) The research enterprise of the Department of Energy, including the National Laboratories, is increasingly targeted by adversarial nations to exploit military and dual-use technologies for military or economic gain.

(5) Approximately 40,000 citizens of foreign countries, including more than 8,000 citizens from China and Russia, were granted access to the premises, information, or technology of National Laboratories in fiscal year 2023.

(6) The Office of Intelligence and Counterintelligence of the Department of Energy is responsible for identifying counterintelligence risks to the Department, including the National Laboratories, and providing direction for the mitigation of such risks.

(c) SENSE OF THE SENATE.—It is the sense of the Senate that—

(1) before being granted access to the premises, information, or technology of a National Laboratory, citizens of foreign countries identified in the 2024 Annual Threat Assessment of the intelligence community as ''engaging in competitive behavior that directly threatens U.S. national security'' should be appropriately screened by the National Laboratory to which they seek access, and by the Office of Intelligence and Counterintelligence of the Department, to identify risks associated with granting the requested access to sensitive military, or dual-use technologies; and

(2) identified risks should be mitigated.

(d) REVIEW OF COUNTRY OF RISK COVERED VISITOR AND COVERED ASSIGNEE ACCESS REQUESTS.—The Director shall, in consultation with the applicable Under Secretary of the Department of Energy that oversees the National Laboratory, or their designee, promulgate a policy to assess the counterintelligence risk that covered visitors or covered assignees pose to the research or activities undertaken at a National Laboratory.

(e) ADVICE WITH RESPECT TO COVERED VISITORS OR COVERED ASSIGNEES.—

(1) IN GENERAL.—The Director shall provide advice to a National Laboratory on covered visitors and covered assignees when 1 or more of the following conditions are present:

(A) The Director has reason to believe that a covered visitor or covered assignee is a nontraditional intelligence collection threat.

(B) The Director is in receipt of information indicating that a covered visitor or covered assignee constitutes a counterintelligence risk to a National Laboratory.

(2) ADVICE DESCRIBED.—Advice provided to a National Laboratory in accordance with paragraph (1) shall include a description of the assessed risk.

(3) RISK MITIGATION.—When appropriate, the Director shall, in consultation with the applicable Under Secretary of the Department of Energy that oversees the National Laboratory, or their designee, provide recommendations to mitigate the risk as part of the advice provided in accordance with paragraph (1).

(f) REPORTS TO CONGRESS.—Not later than 90 days after the date of the enactment of this Act, and quarterly thereafter, the Secretary of Energy shall submit to the appropriate congressional committees a report, which shall include—

(1) the number of covered visitors or covered assignees permitted to access the premises, information, or technology of each National Laboratory;

(2) the number of instances in which the Director provided advice to a National Laboratory in accordance with subsection (e); and

(3) the number of instances in which a National Laboratory took action inconsistent with advice provided by the Director in accordance with subsection (e).

(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such sums as may be necessary to carry out this section for each of fiscal years 2024 through 2032.

SEC. 434. ASSESSMENT OF THE LESSONS LEARNED BY THE INTELLIGENCE COMMUNITY WITH RESPECT TO THE ISRAEL-HAMAS WAR.

(a) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services, the Committee on Foreign Relations, the Committee on Commerce, Science, and Transportation, and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services, the Committee on Foreign Affairs, the Committee on Transportation and Infrastructure, and the Committee on Appropriations of the House of Representatives.

(b) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with such other heads of elements of the intelligence community as the Director considers appropriate, shall submit to the appropriate committees of Congress a written assessment of the lessons learned from the Israel-Hamas war.

(c) ELEMENTS.—The assessment required by subsection (b) shall include the following:

(1) Lessons learned from the timing and scope of the October 7, 2023 attack by Hamas against Israel, including lessons related to United States intelligence cooperation with Israel and other regional partners.

(2) Lessons learned from advances in warfare, including the use by adversaries of a complex tunnel network.

(3) Lessons learned from attacks by adversaries against maritime shipping routes in the Red Sea.

(4) Lessons learned from the use by adversaries of rockets, missiles, and unmanned aerial systems, including attacks by Iran.

(5) Analysis of the impact of the Israel-Hamas war on the global security environment, including the war in Ukraine.

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

SEC. 435. CENTRAL INTELLIGENCE AGENCY INTELLIGENCE ASSESSMENT ON TREN DE ARAGUA.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Committee on the Judiciary, and the Committee on Appropriations of the Senate; and

(3) the Committee on Foreign Affairs, the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on Appropriations of the House of Representatives.

(b) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency, in consultation with such other

heads of elements of the intelligence community as the Director considers appropriate, shall submit to the appropriate committees of Congress an intelligence assessment on the gang known as ''Tren de Aragua''.

(c) ELEMENTS.—The intelligence assessment required by subsection (b) shall include the following:

(1) A description of the key leaders, organizational structure, subgroups, presence in countries in the Western Hemisphere, and cross-border illicit drug smuggling routes of Tren de Aragua.

(2) A description of the practices used by Tren de Aragua to generate revenue.

(3) A description of the level at which Tren de Aragua receives support from the regime of Nicolás Maduro in Venezuela.

(4) A description of the manner in which Tren de Aragua is exploiting heightened migratory flows out of Venezuela and throughout the Western Hemisphere to expand its operations.

(5) A description of the degree to which Tren de Aragua cooperates or competes with other criminal organizations in the Western Hemisphere.

(6) An estimate of the annual revenue received by Tren de Aragua from the sale of illicit drugs, kidnapping, and human trafficking, disaggregated by activity.

(7) Any other information the Director of the Central Intelligence Agency considers relevant.

(d) FORM.—The intelligence assessment required by subsection (b) may be submitted in classified form.

SEC. 436. ASSESSMENT OF MADURO REGIME'S ECONOMIC AND SECURITY RELATIONSHIPS WITH STATE SPONSORS OF TERRORISM AND FOREIGN TERRORIST ORGANIZATIONS.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

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

(3) the Committee on Foreign Affairs, the Committee on Financial Services, and the Committee on the Judiciary of the House of Representatives.

(b) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a written assessment of the economic and security relationships of the regime of Nicolás Maduro of Venezuela with the countries and organizations described in subsection (c), including formal and informal support to and from such countries and organizations.

(c) COUNTRIES AND ORGANIZATIONS DESCRIBED.—The countries and organizations described in this subsection are the following:

(1) The following countries designated by the United States as state sponsors of terrorism:

(A) The Republic of Cuba.

(B) The Islamic Republic of Iran.

(2) The following organizations designated by the United States as foreign terrorist organizations:

(A) The National Liberation Army (ELN).

(B) The Revolutionary Armed Forces of Colombia–People's Army (FARC-EP).

(C) The Segunda Marquetalia.

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

SEC. 437. CONTINUED CONGRESSIONAL OVERSIGHT OF IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Foreign Relations and the Committee on the Judiciary of the Senate; and

(3) the Committee on Foreign Affairs and the Committee on the Judiciary of the House of Representatives.

(b) UPDATE REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress an update to the report submitted under section 6705 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412) to reflect current occurrences, circumstances, and expenditures.

(c) FORM.—The update submitted pursuant to subsection (b) shall be submitted in unclassified form, but may include a classified annex.

TITLE V—EMERGING TECHNOLOGIES

SEC. 501. STRATEGY TO COUNTER FOREIGN ADVERSARY EFFORTS TO UTILIZE BIOTECHNOLOGIES IN WAYS THAT THREATEN UNITED STATES NATIONAL SECURITY.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, the Committee on Health, Education, Labor, and Pensions, the Committee on Commerce, Science, and Transportation, and the Committee on Appropriations of the Senate; and

(3) the Committee on Foreign Affairs, the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives.

(b) SENSE OF CONGRESS.—It is the sense of Congress that as biotechnologies become increasingly important with regard to the national security interests of the United States, and with the addition of biotechnologies to the biosecurity mission of the National Counterproliferation and Biosecurity Center, the intelligence community must articulate and implement a strategy to identify and assess threats relating to biotechnologies.

(c) STRATEGY FOR BIOTECHNOLOGIES CRITICAL TO NATIONAL SECURITY.—

(1) STRATEGY REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall, acting through the Director of the National Counterproliferation and Biosecurity Center and in coordination with the heads of such other elements of the intelligence community as the Director of National Intelligence considers appropriate, develop and submit to the appropriate committees of Congress a whole-of-government strategy to address concerns relating to biotechnologies.

(2) ELEMENTS.—The strategy developed and submitted pursuant to paragraph (1) shall include the following:

(A) Identification and assessment of threats associated with biotechnologies critical to the national security of the United States, including materials that involve a dependency on foreign adversary nations.

(B) A determination of how best to counter foreign adversary efforts to utilize biotechnologies that threaten the national security of the United States, including threats identified pursuant to paragraph (1).

(C) A plan to support efforts of other Federal departments and agencies to secure United States supply chains of the biotechnologies critical to the national security of the United States, by coordinating—

(i) across the intelligence community;

(ii) the support provided by the intelligence community to other relevant Federal departments and agencies and policymakers;

(iii) the engagement of the intelligence community with private sector entities, in coordination with other relevant Federal departments and agencies, as may be applicable; and

(iv) how the intelligence community, in coordination with other relevant Federal departments and agencies, can support such efforts to secure United States supply chains for and use of biotechnologies.

(D) Proposals for such legislative or administrative action as the Directors consider necessary to support the strategy.

SEC. 502. IMPROVEMENTS TO THE ROLES, MISSIONS, AND OBJECTIVES OF THE NATIONAL COUNTERPROLIFERATION AND BIOSECURITY CENTER.

Section 119A of the National Security Act of 1947 (50 U.S.C. 3057) is amended—

(1) in subsection (a)(4), by striking ''biosecurity and'' and inserting ''counterproliferation, biosecurity, and''; and

(2) in subsection (b)—

(A) in paragraph (1)—

(i) in subparagraph (A), by striking ''analyzing and'';

(ii) in subparagraph (C), by striking ''Establishing'' and inserting ''Coordinating the establishment of'';

(iii) in subparagraph (D), by striking ''Disseminating'' and inserting ''Overseeing the dissemination of'';

(iv) in subparagraph (E), by inserting ''and coordinating'' after ''Conducting''; and

(v) in subparagraph (G), by striking ''Conducting'' and inserting ''Coordinating and advancing''; and

(B) in paragraph (2)—

(i) in subparagraph (B), by striking ''and analysis'';

(ii) by redesignating subparagraphs (C) through (E) as subparagraphs (D) through (F), respectively;

(iii) by inserting after subparagraph (B) the following:

''(C) Overseeing and coordinating the analysis of intelligence on biosecurity and foreign biological threats in support of the intelligence needs of Federal departments and agencies responsible for public health, including by providing analytic priorities to elements of the intelligence community and by conducting and coordinating net assessments.'';

(iv) in subparagraph (D), as redesignated by clause (ii), by inserting ''on matters relating to biosecurity and foreign biological threats'' after ''public health'';

(v) in subparagraph (F), as redesignated by clause (ii), by inserting ''and authorities'' after ''capabilities''; and

(vi) by adding at the end the following:

''(G) Enhancing coordination between elements of the intelligence community and private sector entities on information relevant to biosecurity, biotechnology, and foreign biological threats, and coordinating such information with relevant Federal departments and agencies, as applicable.''.

SEC. 503. ENHANCING CAPABILITIES TO DETECT FOREIGN ADVERSARY THREATS RELATING TO BIOLOGICAL DATA.

(a) DEFINITION OF BIOLOGICAL DATA.—The term ''biological data'' means information,

including associated descriptors, derived from the structure, function, or process of a biological system that is either measured, collected, or aggregated for analysis.

(b) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with relevant heads of Federal departments and agencies, take the following steps to standardize the use by the intelligence community of biological data and the ability of the intelligence community to detect foreign adversary threats relating to biological data:

(1) Standardize the processes and procedures for the collection, analysis, and dissemination of information relating to foreign adversary use of biological data, particularly in ways that threaten or could threaten the national security of the United States.

(2) Issue policy guidance within the intelligence community—

(A) to standardize the data security practices for biological data maintained by the intelligence community, including security practices for the handling and processing of biological data, including with respect to protecting the civil rights, liberties, and privacy of United States persons;

(B) to standardize intelligence engagements with foreign allies and partners with respect to biological data; and

(C) to standardize the creation of metadata relating to biological data maintained by the intelligence community.

(3) Ensure coordination with such Federal departments and agencies and entities in the private sector as the Director considers appropriate to understand how foreign adversaries are accessing and using biological data stored within the United States.

SEC. 504. NATIONAL SECURITY PROCEDURES TO ADDRESS CERTAIN RISKS AND THREATS RELATING TO ARTIFICIAL INTELLIGENCE.

(a) DEFINITION OF ARTIFICIAL INTELLIGENCE.—In this section, the term ''artificial intelligence''—

(1) has the meaning given that term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401); and

(2) includes the artificial systems and techniques described in paragraphs (1) through (5) of section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 4061 note prec.)

(b) FINDINGS.—Congress finds the following:

(1) Artificial intelligence systems demonstrate increased capabilities in the generation of synthetic media and computer programming code, as well as areas such as object recognition, natural language processing, and workflow orchestration.

(2) The growing capabilities of artificial intelligence systems in the areas described in paragraph (1), as well as the greater accessibility of large-scale artificial intelligence models and advanced computation capabilities to individuals, businesses, and governments, have dramatically increased the adoption of artificial intelligence products in the United States and globally.

(3) The advanced capabilities of the systems described in paragraph (1), and their accessibility to a wide-range of users, have increased the likelihood and effect of foreign misuse or malfunction of these systems, such as to assist foreign actors to generate synthetic media for disinformation campaigns, develop or refine malware for computer network exploitation activity by foreign actors, enhance foreign surveillance capabilities in ways that undermine the privacy of citizens of the United States, and increase the risk of foreign exploitation or malfunction of information technology systems incorporating artificial intelligence systems in mission-critical fields such as health care, critical infrastructure, and transportation.

(c) PROCEDURES REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the President shall develop and issue procedures to facilitate and promote mechanisms by which—

(1) vendors of advanced computation capabilities, vendors and commercial users of artificial intelligence systems, as well as independent researchers and other third parties, may effectively notify appropriate elements of the United States Government of—

(A) information security risks emanating from artificial intelligence systems, such as the use of an artificial intelligence system by foreign actors to develop or refine malicious software;

(B) information security risks such as indications of compromise or other threat information indicating a compromise to the confidentiality, integrity, or availability of an artificial intelligence system, or to the supply chain of an artificial intelligence system, including training or test data, frameworks, computing environments, or other components necessary for the training, management, or maintenance of an artificial intelligence system posed by foreign actors;

(C) biosecurity risks emanating from artificial intelligence systems, such as the use of an artificial intelligence system by foreign actors to design, develop, or acquire dual-use biological entities such as putatively toxic small molecules, proteins, or pathogenic organisms;

(D) suspected foreign malign influence (as defined by section 119C of the National Security Act of 1947 (50 U.S.C. 3059(f))) activity that appears to be facilitated by an artificial intelligence system;

(E) chemical security risks emanating from artificial intelligence systems, such as the use of an artificial intelligence system to design, develop, or acquire chemical weapons or their analogues, or other hazardous chemical compounds; and

(F) any other unlawful activity by foreign actors facilitated by, or directed at, an artificial intelligence system;

(2) elements of the Federal Government may provide threat briefings to vendors of advanced computation capabilities and vendors of artificial intelligence systems, alerting them, as may be appropriate, to potential or confirmed foreign exploitation of their systems, as well as malign foreign plans and intentions; and

(3) an inter-agency process is convened to identify appropriate Federal agencies to assist in the private sector engagement described in this subsection and to coordinate with respect to risks that implicate multiple sectors and Federal agencies, including leveraging Sector Risk Management Agencies (as defined in section 2200 of the Homeland Security Act of 20002 (6 U.S.C. 650)) where appropriate.

(d) BRIEFING REQUIRED.—

(1) APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, the Committee on Health, Education, Labor, and Pensions, the Committee on the Judiciary, the Committee on Commerce, Science, and Transportation, and the Committee on Appropriations of the Senate; and

(C) the Committee on Homeland Security, the Committee on Foreign Affairs, the Committee on the Judiciary, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives.

(2) IN GENERAL.—The President shall provide the appropriate committees of Congress a briefing on procedures developed and issued pursuant to subsection (c).

(3) ELEMENTS.—The briefing provided pursuant to paragraph (2) shall include the following:

(A) A clear specification of which Federal agencies are responsible for leading outreach to affected industry and the public with respect to the matters described in subparagraphs (A) through (E) of paragraph (1) of subsection (c) and paragraph (2) of such subsection.

(B) An outline of a plan for industry outreach and public education regarding risks posed by, and directed at, artificial intelligence systems associated with foreign actors.

(C) Use of research and development, stakeholder outreach, and risk management frameworks established pursuant to—

(i) provisions of law in effect on the day before the date of the enactment of this Act; or

(ii) Federal agency guidelines.

SEC. 505. ESTABLISHMENT OF ARTIFICIAL INTELLIGENCE SECURITY CENTER.

(a) DEFINITION OF COUNTER-ARTIFICIAL INTELLIGENCE.—In this section, the term ''counter-artificial intelligence'' means techniques or procedures to extract information about the behavior or characteristics of an artificial intelligence system, or to learn how to manipulate an artificial intelligence system, in order to subvert the confidentiality, integrity, or availability of an artificial intelligence system or adjacent system.

(b) ESTABLISHMENT.—Not later than 90 days after the date of the enactment of this Act, the Director of the National Security Agency shall establish an Artificial Intelligence Security Center within the Cybersecurity Collaboration Center of the National Security Agency.

(c) FUNCTIONS.—The functions of the Artificial Intelligence Security Center shall be as follows:

(1) Developing guidance to prevent or mitigate counter-artificial intelligence techniques.

(2) Promoting secure artificial intelligence adoption practices for managers of national security systems (as defined in section 3552 of title 44, United States Code) and elements of the defense industrial base.

(3) Such other functions as the Director considers appropriate.

SEC. 506. SENSE OF CONGRESS ENCOURAGING INTELLIGENCE COMMUNITY TO INCREASE PRIVATE SECTOR CAPITAL PARTNERSHIPS AND PARTNERSHIP WITH OFFICE OF STRATEGIC CAPITAL OF DEPARTMENT OF DEFENSE TO SECURE ENDURING TECHNOLOGICAL ADVANTAGES.

It is the sense of Congress that—

(1) acquisition leaders in the intelligence community should further explore the strategic use of private capital partnerships to secure enduring technological advantages for the intelligence community, including through the identification, development, and transfer of promising technologies to full-scale programs capable of meeting intelligence community requirements; and

(2) the intelligence community should undertake regular consultation with Federal partners, such as the Office of Strategic Capital of the Office of the Secretary of Defense, on best practices and lessons learned from their experiences integrating these resources so as to accelerate attainment of national security objectives.

SEC. 507. INTELLIGENCE COMMUNITY TECHNOLOGY BRIDGE PROGRAM.

(a) DEFINITIONS.—In this section:

(1) NONPROFIT ORGANIZATION.—The term ''nonprofit organization'' means an organization that is described in section 501(c)(3) of the Internal Revenue Code of 1986 and that is exempt from tax under section 501(a) of such Code.

(2) WORK PROGRAM.—The term ''work program'' means any agreement between In-Q-Tel and a third-party company, where such third-party company furnishes or is furnishing a product or service for use by any of In-Q-Tel's government customers to address those customers' technology needs or requirements.

(b) ESTABLISHMENT OF PROGRAM.—

(1) IN GENERAL.—The Director of National Intelligence shall establish within the Office of the Director of National Intelligence a program to assist in the transitioning of products or services from the research and development phase to the contracting and production phase, subject to the extent and in such amounts as specifically provided in advance in appropriations Acts for such purposes.

(2) DESIGNATION.—The program established pursuant to paragraph (1) shall be known as the ''Intelligence Community Technology Bridge Program'' (in this subsection referred to as the ''Program'').

(c) PROVISION OF ASSISTANCE.—

(1) IN GENERAL.—Subject to paragraph (3), the Director shall, in consultation with In-Q-Tel, carry out the Program by providing assistance to businesses or nonprofit organizations that are transitioning products or services.

(2) TYPES OF ASSISTANCE.—Assistance provided under paragraph (1) may be provided in the form of a grant or a payment for a product or service.

(3) REQUIREMENTS FOR ASSISTANCE.—Assistance may be provided under paragraph (1) to a business or nonprofit organization that is transitioning a product or service only if—

(A) the business or nonprofit organization—

(i) has participated or is participating in a work program; or

(ii) is engaged with an element of the intelligence community or Department of Defense for research and development; and

(B) the Director or the head of an element of the intelligence community attests that the product or service will be utilized by an element of the intelligence community for a mission need, such as because it would be valuable in addressing a needed capability, fill or complement a technology gap, or increase the supplier base or price-competitiveness for the Federal Government.

(4) PRIORITY FOR SMALL BUSINESS CONCERNS AND NONTRADITIONAL DEFENSE CONTRACTORS.—In providing assistance under paragraph (1), the Director shall prioritize the provision of assistance to small business concerns (as defined under section 3(a) of the Small Business Act (15 U.S.C. 632(a))) and nontraditional defense contractors (as defined in section 3014 of title 10, United States Code).

(d) ADMINISTRATION OF PROGRAM.—

(1) IN GENERAL.—The Program shall be administered by the Director.

(2) CONSULTATION.—In administering the Program, the Director—

(A) shall consult with the heads of the elements of the intelligence community; and

(B) may consult with In-Q-Tel, the Defense Advanced Research Project Agency, the North Atlantic Treaty Organization Investment Fund, and the Defense Innovation Unit.

(e) SEMIANNUAL REPORTS.—

(1) IN GENERAL.—Not later than September 30, 2025, and not less frequently than twice each fiscal year thereafter in which amounts are available for the provision of assistance under the Program, the Director shall submit to the congressional intelligence committees a semiannual report on the Program.

(2) CONTENTS.—Each report submitted pursuant to paragraph (1) shall include, for the period covered by the report, information about the following:

(A) How much was expended or obligated by the Program in the provision of assistance under subsection (c).

(B) For what the amounts were expended or obligated.

(C) The effects of such expenditures and obligations, including a timeline for expected milestones for operational use.

(D) A summary of annual transition activities and outcomes of such activities for the intelligence community.

(E) A description of why products and services were chosen for transition, including a description of milestones achieved.

(3) FORM.—Each report submitted pursuant to paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Office of the Director of National Intelligence to carry out the Program $75,000,000 for fiscal year 2025.

SEC. 508. ENHANCEMENT OF AUTHORITY FOR INTELLIGENCE COMMUNITY PUBLIC-PRIVATE TALENT EXCHANGES.

(a) FOCUS AREAS.—Subsection (a) of section 5306 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334) is amended—

(1) by striking ''Not later than'' and inserting the following:

''(1) IN GENERAL.—Not later than''; and

(2) by adding at the end the following:

''(2) FOCUS AREAS.—The Director shall ensure that the policies, processes, and procedures developed pursuant to paragraph (1) require exchanges under this section relate to intelligence or counterintelligence with a focus on rotations described in such paragraph with private-sector organizations in the following fields:

''(A) Finance.

''(B) Acquisition.

''(C) Biotechnology.

''(D) Computing.

''(E) Artificial intelligence.

''(F) Business process innovation and entrepreneurship.

''(G) Cybersecurity.

''(H) Materials and manufacturing.

''(I) Any other technology or research field the Director determines relevant to meet evolving national security threats in technology sectors.''.

(b) DURATION OF TEMPORARY DETAILS.—Subsection (e) of section 5306 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334) is amended—

(1) in paragraph (1), by striking ''3 years'' and inserting ''5 years''; and

(2) in paragraph (2), by striking ''3 years'' and inserting ''5 years''.

(c) TREATMENT OF PRIVATE-SECTOR EMPLOYEES.—Subsection (g) of such section is amended—

(1) in paragraph (5), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (6), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(7) shall not be considered to have a conflict of interest with an element of the intelligence community solely because of being detailed to an element of the intelligence community under this section.''.

(d) HIRING AUTHORITY.—Such section is amended—

(1) by redesignating subsection (j) as subsection (k); and

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

''(j) HIRING AUTHORITY.—

''(1) IN GENERAL.—The Director may hire, under section 213.3102(r) of title 5, Code of Federal Regulations, or successor regulations, an individual who is an employee of a private-sector organization who is detailed to an element of the intelligence community under this section.

''(2) NO PERSONNEL BILLET REQUIRED.—Hiring an individual under paragraph (1) shall not require a personnel billet.''.

(e) ANNUAL REPORTS.—

(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

(B) the Committee on Appropriations of the Senate; and

(C) the Committee on Appropriations of the House of Representatives.

(2) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act and annually thereafter for 2 more years, the Director of National Intelligence shall submit to the appropriate committees of Congress an annual report on—

(A) the implementation of the policies, processes, and procedures developed pursuant to subsection (a) of such section 5306 (50 U.S.C. 3334) and the administration of such section;

(B) how the heads of the elements of the intelligence community are using or plan to use the authorities provided under such section; and

(C) recommendations for legislative or administrative action to increase use of the authorities provided under such section.

SEC. 509. ENHANCING INTELLIGENCE COMMUNITY ABILITY TO ACQUIRE EMERGING TECHNOLOGY THAT FULFILLS INTELLIGENCE COMMUNITY NEEDS.

(a) DEFINITION OF WORK PROGRAM.—The term ''work program'' means any agreement between In-Q-Tel and a third-party company, where such third-party company furnishes or is furnishing a property, product, or service for use by any of In-Q-Tel's government customers to address those customers' technology needs or requirements.

(b) IN GENERAL.—In addition to the exceptions listed under section 3304(a) of title 41, United States Code, and under section 3204(a) of title 10, United States Code, for the use of competitive procedures, the Director of National Intelligence or the head of an element of the intelligence community may use procedures other than competitive procedures to acquire a property, product, or service if—

(1) the property, product, or service is a work program; and

(2) the Director of National Intelligence or the head of an element of the intelligence community certifies that such property, product, or service has been shown to meet an identified need of the intelligence community.

(c) JUSTIFICATION FOR USE OF PROCEDURES OTHER THAN COMPETITIVE PROCEDURES.—

(1) IN GENERAL.—A property, product, or service may not be acquired by the Director or the head of an element of the intelligence community under subsection (b) using procedures other than competitive procedures unless the acquiring officer for the acquisition justifies, at the directorate level, the use of such procedures in writing.

(2) CONTENTS.—A justification in writing described in paragraph (1) for an acquisition using procedures other than competitive procedures shall include the following:

(A) A description of the need of the element of the intelligence community that the property, product, or service satisfies.

(B) A certification that the anticipated costs will be fair and reasonable.

(C) A description of the market survey conducted or a statement of the reasons a market survey was not conducted.

(D) Such other matters as the Director or the head, as the case may be, determines appropriate.

SEC. 510. SENSE OF CONGRESS ON HOSTILE FOREIGN CYBER ACTORS.

It is the sense of Congress that foreign ransomware organizations, and foreign affiliates associated with them, constitute hostile foreign cyber actors, that covered nations abet and benefit from the activities of these actors, and that such actors should be treated as hostile foreign cyber actors by the United States. Such actors include the following:

(1) DarkSide.

(2) Conti.

(3) REvil.

(4) BlackCat, also known as ''ALPHV''.

(5) LockBit.

(6) Rhysida, also known as ''Vice Society''.

(7) Royal.

(8) Phobos, also known as ''Eight'' and also known as ''Joanta''.

(9) C10p.

(10) Hackers associated with the SamSam ransomware campaigns.

(11) Play.

(12) BianLian.

(13) Killnet.

(14) Akira.

(15) Ragnar Locker, also known as ''Dark Angels''.

(16) Blacksuit.

(17) INC.

(18) Black Basta.

SEC. 511. DEEMING RANSOMWARE THREATS TO CRITICAL INFRASTRUCTURE A NATIONAL INTELLIGENCE PRIORITY.

(a) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees;

(B) the Committee on Commerce, Science, and Transportation, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(C) the Committee on Energy and Commerce, the Committee on the Judiciary, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

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

(b) RANSOMWARE THREATS TO CRITICAL INFRASTRUCTURE AS NATIONAL INTELLIGENCE PRIORITY.—The Director of National Intelligence, pursuant to the provisions of the National Security Act of 1947 (50 U.S.C. 3001 et seq.), the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), section 1.3(b)(17) of Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), as in effect on the day before the date of the enactment of this Act, and National Security Presidential Directive–26 (February 24, 2003; relating to intelligence priorities), as in effect on the day before the date of the enactment of this Act, shall deem ransomware threats to critical infrastructure a national intelligence priority component to the National Intelligence Priorities Framework.

(c) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, submit to the appropriate committees of Congress a report on the implications of the ransomware threat to United States national security.

(2) CONTENTS.—The report submitted under paragraph (1) shall address the following:

(A) Identification of individuals, groups, and entities who pose the most significant threat, including attribution to individual ransomware attacks whenever possible.

(B) Locations from which individuals, groups, and entities conduct ransomware attacks.

(C) The infrastructure, tactics, and techniques ransomware actors commonly use.

(D) Any relationships between the individuals, groups, and entities that conduct ransomware attacks and their governments or countries of origin that could impede the ability to counter ransomware threats.

(E) Intelligence gaps that have impeded, or currently are impeding, the ability to counter ransomware threats.

(3) FORM.—The report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

SEC. 512. ENHANCING PUBLIC-PRIVATE SHARING ON MANIPULATIVE ADVERSARY PRACTICES IN CRITICAL MINERAL PROJECTS.

(a) STRATEGY REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the heads of such Federal agencies as the Director considers appropriate, develop a strategy to improve the sharing between the Federal Government and private entities of information and intelligence to mitigate the threat that foreign adversary illicit activities and tactics pose to United States persons in foreign jurisdictions on projects relating to energy generation and storage, including with respect to critical minerals inputs.

(b) ELEMENTS.—The strategy required by subsection (a) shall cover—

(1) how best to assemble and transmit information to United States persons—

(A) to protect against foreign adversary illicit tactics and activities relating to critical mineral projects abroad, including foreign adversary efforts to undermine such projects abroad;

(B) to mitigate the risk that foreign adversary government involvement in the ownership and control of entities engaging in deceptive or illicit activities targeting critical mineral supply chains pose to the interests of the United States; and

(C) to inform on economic espionage and other threats from foreign adversaries to the rights of owners of intellectual property, including owners of patents, trademarks, copyrights, and trade secrets, and other sensitive information, with respect to such property that is dependent on critical mineral inputs; and

(2) how best to receive information from United States persons on threats to United States interests in the critical mineral supply chains, resources, mines, and products, including disinformation campaigns abroad or other suspicious malicious activity.

(c) IMPLEMENTATION PLAN REQUIRED.—

(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

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

(C) the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives.

(2) IN GENERAL.—Not later than 30 days after the date on which the Director completes developing the strategy pursuant to subsection (a), the Director shall submit to the appropriate committees of Congress, or provide such committees a briefing on, a plan for implementing the strategy.

TITLE VI—CLASSIFICATION REFORM

SEC. 601. CLASSIFICATION AND DECLASSIFICATION OF INFORMATION.

(a) IN GENERAL.—The President may, in accordance with this section, protect from unauthorized disclosure any information owned by, produced by or for, or under the control of the executive branch of the Federal Government when there is a demonstrable need to do so to protect the national security of the United States.

(b) ESTABLISHMENT OF STANDARDS, CATEGORIES, AND PROCEDURES FOR CLASSIFICATION AND DECLASSIFICATION.—

(1) GOVERNMENTWIDE PROCEDURES.—

(A) CLASSIFICATION.—The President shall, to the extent necessary, establish categories of information that may be classified and procedures for classifying information under subsection (a).

(B) DECLASSIFICATION.—At the same time the President establishes categories and procedures under subparagraph (A), the President shall establish procedures for declassifying information that was previously classified.

(C) MINIMUM REQUIREMENTS.—The procedures established pursuant to subparagraphs (A) and (B) shall—

(i) be the exclusive means for classifying information on or after the effective date established by subsection (c), except with respect to information classified pursuant to the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.);

(ii) ensure that no information is classified unless there is a demonstrable need to do so to protect the national security and there is a reasonable basis to believe that means other than classification will not provide sufficient protection;

(iii) ensure that no information may remain classified indefinitely;

(iv) ensure that no information shall be classified, continue to be maintained as classified, or fail to be declassified in order—

(I) to conceal violations of law, inefficiency, or administrative error;

(II) to prevent embarrassment to a person, organization, or agency;

(III) to restrain competition; or

(IV) to prevent or delay the release of information that does not require protection in the interest of the national security;

(v) ensure that basic scientific research information not clearly related to the national security shall not be classified;

(vi) ensure that information may not be reclassified after being declassified and released to the public under proper authority unless personally approved by the President based on a determination that such reclassification is required to prevent significant and demonstrable damage to the national security;

(vii) establish standards and criteria for the classification of information;

(viii) establish standards, criteria, and timelines for the declassification of information classified under this section;

(ix) provide for the automatic declassification of classified records with permanent historical value;

(x) provide for the timely review of materials submitted for pre-publication;

(xi) ensure that due regard is given for the public interest in disclosure of information;

(xii) ensure that due regard is given for the interests of departments and agencies in sharing information at the lowest possible level of classification;

(D) SUBMITTAL TO CONGRESS.—The President shall submit to Congress the categories and procedures established under subsection (b)(1)(A) and the procedures established under subsection (b)(1)(B) at least 60 days prior to their effective date.

(2) AGENCY STANDARDS AND PROCEDURES.—

(A) IN GENERAL.—The head of each Federal agency shall establish a single set of consolidated standards and procedures to permit such agency to classify and declassify information created by such agency in accordance with the categories and procedures established by the President under this section and otherwise to carry out this section.

(B) SUBMITTAL TO CONGRESS.—Each agency head shall submit to Congress the standards and procedures established by such agency head under subparagraph (A).

(c) EFFECTIVE DATE.—

(1) IN GENERAL.—Subsections (a) and (b) shall take effect on the date that is 180 days after the date of the enactment of this Act.

(2) RELATION TO PRESIDENTIAL DIRECTIVES.—Presidential directives regarding classifying, safeguarding, and declassifying national security information, including Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), in effect on the day before the date of the enactment of this Act, as well as procedures issued pursuant to such Presidential directives, shall remain in effect until superseded by procedures issued pursuant to subsection (b).

(d) CONFORMING AMENDMENT.—Section 805(2) of the National Security Act of 1947 (50 U.S.C. 3164(2)) is amended by inserting ''section 603 of the Intelligence Authorization Act for Fiscal Year 2025,'' before ''Executive Order''.

SEC. 602. MINIMUM STANDARDS FOR EXECUTIVE AGENCY INSIDER THREAT PROGRAMS.

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' means any Executive agency as defined in section 105 of title 5, United States Code, any military department as defined in section 102 of such title, and any other entity in the executive branch of the Federal Government that comes into the possession of classified information.

(2) CLASSIFIED INFORMATION.—The term ''classified information'' means information that has been determined to require protection from unauthorized disclosure pursuant to Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or predecessor or successor order, to protect the national security of the United States.

(b) ESTABLISHMENT OF INSIDER THREAT PROGRAMS.—Each head of an agency with access to classified information shall establish an insider threat program to protect classified information from unauthorized disclosure.

(c) MINIMUM STANDARDS.—In carrying out an insider threat program established by the head of an agency pursuant to subsection (b), the head of the agency shall—

(1) designate a senior official of the agency who shall be responsible for management of the program;

(2) monitor user activity on all classified networks to detect activity indicative of insider threat behavior;

(3) build and maintain an insider threat analytic and response capability to review, assess, and respond to information obtained pursuant to paragraph (2); and

(4) provide insider threat awareness training to all cleared employees within 30 days of entry-on-duty or granting of access to classified information and annually thereafter.

(d) ANNUAL REPORTS.—Not less frequently than once each year, the Director of National Intelligence shall, serving as the Security Executive Agent under section 803 of the National Security Act of 1947 (50 U.S.C. 3162a), submit to Congress an annual report on the compliance of agencies with respect to the requirements of this section.

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to revoke or diminish any right of an individual provided by section 2303 or 7211 of title 5, United States Code, or under any other applicable protections for whistleblowers provided by law.

TITLE VII—SECURITY CLEARANCES AND INTELLIGENCE COMMUNITY WORKFORCE IMPROVEMENTS

SEC. 701. SECURITY CLEARANCES HELD BY CERTAIN FORMER EMPLOYEES OF INTELLIGENCE COMMUNITY.

(a) ISSUANCE OF GUIDELINES AND INSTRUCTIONS REQUIRED.—Section 803(c) of the National Security Act of 1947 (50 U.S.C. 3162a(c)) is amended—

(1) in paragraph (3), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (4), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(5) issue guidelines and instructions to the heads of Federal agencies to ensure that any individual who was appointed by the President to a position in an element of the intelligence community but is no longer employed by the Federal Government shall maintain a security clearance only in accordance with Executive Order 12968 (50 U.S.C. 3161 note; relating to access to classified information), or successor order.''.

(b) SUBMITTAL OF GUIDELINES AND INSTRUCTIONS TO CONGRESS REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in the Director's capacity as the Security Executive Agent pursuant to subsection (a) of section 803 of the National Security Act of 1947 (50 U.S.C. 3162a), submit to the congressional intelligence committees and the congressional defense committees the guidelines and instructions required by subsection (c)(5) of such Act, as added by subsection (a) of this section.

(c) ANNUAL REPORT REQUIRED.—

(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

(B) the congressional defense committees;

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

(D) the Committee on Oversight and Accountability of the House of Representatives.

(2) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than once each year thereafter, the Director of National Intelligence shall, in the Director's capacity as the Security Executive Agent pursuant to section 803(a) of the National Security Act of 1947 (50 U.S.C. 3162a(a)), submit to the appropriate committees of Congress an annual report on the eligibility status of former senior employees of the intelligence community to access classified information.

(3) CONTENTS.—Each report submitted pursuant to paragraph (2) shall include, for the period covered by the report, the following:

(A) A list of individuals who were appointed by the President to a position in an element of the intelligence community who currently hold security clearances.

(B) The number of such former employees who still hold security clearances.

(C) For each former employee described in subparagraph (B)—

(i) the position in the intelligence community held by the former employee;

(ii) the years of service in such position; and

(iii) the individual's current employment position and employer.

(D) The Federal entity authorizing and adjudicating the former employees' need to know classified information.

SEC. 702. POLICY FOR AUTHORIZING INTELLIGENCE COMMUNITY PROGRAM OF CONTRACTOR-OWNED AND CONTRACTOR-OPERATED SENSITIVE COMPARTMENTED INFORMATION FACILITIES.

(a) POLICY.—The Director of National Intelligence shall establish a standardized policy for the intelligence community that authorizes a program of contractor-owned and contractor-operated sensitive compartmented information facilities as a service to the national security and intelligence enterprises.

(b) REQUIREMENTS.—The policy established pursuant to subsection (a) shall—

(1) authorize the head of an element of the intelligence community to approve and accredit contractor-owned and contractor-operated sensitive compartmented information facilities; and

(2) designate an element of the intelligence community as a service of common concern (as defined in Intelligence Community Directive 122, or successor directive) to serve as an accrediting authority (in accordance with Intelligence Community Directive 705, or successor directive) on behalf of other elements of the intelligence community for contractor-owned and contractor-operated sensitive compartmented information facilities.

(c) COST CONSIDERATIONS.—In establishing the policy required by subsection (a), the Director shall consider existing demonstrated models where a contractor acquires, outfits, and manages a facility pursuant to an agreement with the Federal Government such that no funding from the Federal Government is required to carry out the agreement.

(d) BRIEFING REQUIRED.—

(1) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

(B) the Committee on Appropriations of the Senate; and

(C) the Committee on Appropriations of the House of Representatives.

(2) IN GENERAL.—Not later than 1 year after the date on which the Director establishes the policy pursuant to subsection (a), the Director shall brief the appropriate committees of Congress on—

(A) additional opportunities to leverage contractor-owned and contractor-operated sensitive compartmented information facilities; and

(B) recommendations to address barriers, including resources or authorities needed.

SEC. 703. ENABLING INTELLIGENCE COMMUNITY INTEGRATION.

(a) IN GENERAL.—The National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended by inserting after section 113B the following new section:

''SEC. 113C. ENABLING INTELLIGENCE COMMUNITY INTEGRATION.

''(a) PROVISION OF GOODS OR SERVICES.—Subject to and in accordance with any guidance and requirements developed by the Director of National Intelligence, the head of an element of the intelligence community may provide goods or services to another element of the intelligence community without reimbursement or transfer of funds for

hoteling initiatives for intelligence community employees and affiliates defined in any such guidance and requirements issued by the Director of National Intelligence.

''(b) APPROVAL.—Prior to the provision of goods or services pursuant to subsection (a), the head of the element of the intelligence community providing such goods or services and the head of the element of the intelligence community receiving such goods or services shall approve such provision.''.

(b) CLERICAL AMENDMENT.—The table of contents of the National Security Act of 1947 is amended by inserting after the item relating to section 113B the following:

''Sec. 113C. Enabling intelligence community integration.''.

SEC. 704. APPOINTMENT OF SPOUSES OF CERTAIN FEDERAL EMPLOYEES.

(a) IN GENERAL.—Section 3330d of title 5, United States Code, is amended—

(1) in the section heading, by striking ''**military and Department of Defense civilian spouses**'' and inserting ''**military and Department of Defense, Department of State, and intelligence community spouses**'';

(2) in subsection (a)—

(A) by redesignating the second paragraph (4) (relating to a spouse of an employee of the Department of Defense) as paragraph (7);

(B) by striking paragraph (5);

(C) by redesignating paragraph (4) (relating to the spouse of a disabled or deceased member of the Armed Forces) as paragraph (6);

(D) by striking paragraph (3) and inserting the following:

''(3) The term 'covered spouse' means an individual who is married to an individual who—

''(A)(i) is an employee of the Department of State or an element of the intelligence community; or

''(ii) is a member of the Armed Forces who is assigned to an element of the intelligence community; and

''(B) is transferred in the interest of the Government from one official station within the applicable agency to another within the agency (that is outside of normal commuting distance) for permanent duty.

''(4) The term 'intelligence community' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

''(5) The term 'remote work' refers to a work flexibility arrangement under which an employee—

''(A) is not expected to physically report to the location from which the employee would otherwise work, considering the position of the employee; and

''(B) performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite—

''(i) other than the location from which the employee would otherwise work;

''(ii) that may be inside or outside the local commuting area of the location from which the employee would otherwise work; and

''(iii) that is typically the residence of the employee.''; and

(E) by adding at the end the following:

''(8) The term 'telework' has the meaning given the term in section 6501.''; and

(3) in subsection (b)—

(A) in paragraph (2), by striking ''or'' at the end;

(B) in the first paragraph (3) (relating to a spouse of a member of the Armed Forces on active duty), by striking the period at the end and inserting a semicolon;

(C) by redesignating the second paragraph (3) (relating to a spouse of an employee of the Department of Defense) as paragraph (4);

(D) in paragraph (4), as so redesignated—

(i) by inserting '', including to a position in which the spouse will engage in remote work'' after ''Department of Defense''; and

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

(E) by adding at the end the following:

''(5) a covered spouse to a position in which the covered spouse will engage in remote work.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for subchapter I of chapter 33 of title 5, United States Code, is amended by striking the item relating to section 3330d and inserting the following:

''3330d. Appointment of military and Department of Defense, Department of State, and intelligence community civilian spouses.''.

(c) REPORT.—

(1) DEFINITION OF APPROPRIATION COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

(B) the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(C) the Committee on Armed Services, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(2) IN GENERAL.—Not later than 5 years after the date of the enactment of this Act, the Secretary of Defense shall submit to the appropriate committees of Congress a report detailing the use of the authority provided pursuant to the amendments made by subsection (a) and the impacts on recruitment, retention, and job opportunities created by such amendments.

(d) RULE OF CONSTRUCTION.—Nothing in this section or an amendment made by this section shall be construed to revoke or diminish any right of an individual provided by title 5, United States Code.

(e) SUNSET AND SNAPBACK.—On the date that is 5 years after the date of the enactment of this Act—

(1) section 3330d of title 5, United States Code, as amended by subsection (a), is amended to read as it read on the day before the date of the enactment of this Act; and

(2) the item for such section in the table of sections for subchapter I of chapter 33 of title 5, United States Code, as amended by subsection (b), is amended to read as it read on the day before the date of the enactment of this Act.

SEC. 705. PLAN FOR STAFFING THE INTELLIGENCE COLLECTION POSITIONS OF THE CENTRAL INTELLIGENCE AGENCY.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall submit to the congressional intelligence committees a plan for ensuring that the Directorate of Operations of the Agency has staffed every civilian full-time equivalent position authorized for that Directorate under the Intelligence Authorization Act for Fiscal Year 2024 (division G of Public Law 118–31).

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

(1) Specific benchmarks and timelines for accomplishing the goal described in such subsection by September 30, 2025.

(2) An assessment of the appropriate balance of staffing between the Directorate of Operations and the Directorate of Analysis consistent with the responsibilities of the Director of the Central Intelligence Agency under section 104A(d) of the National Security Act of 1947 (50 U.S.C. 3036(d)).

SEC. 706. SENSE OF CONGRESS ON GOVERNMENT PERSONNEL SUPPORT FOR FOREIGN TERRORIST ORGANIZATIONS.

It is the sense of Congress that for the purposes of adjudicating the eligibility of an individual for access to classified information, renewal of a prior determination of eligibility for such access, or continuous vetting of an individual for eligibility for such access, including on form SF–86 or any successor form, each of the following should be considered an action advocating for an act of terrorism:

(1) Advocating for violence by an organization designated as a foreign terrorist organization under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(2) Soliciting funds for or contributing funds to an organization described in paragraph (1).

TITLE VIII—WHISTLEBLOWERS

SEC. 801. IMPROVEMENTS REGARDING URGENT CONCERNS SUBMITTED TO INSPECTORS GENERAL OF THE INTELLIGENCE COMMUNITY.

(a) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—Section 103H(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)) is amended—

(1) in subparagraph (A)—

(A) by inserting ''(i)'' before ''An employee of'';

(B) by inserting ''in writing'' before ''to the Inspector General''; and

(C) by adding at the end the following:

''(ii) The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this subparagraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or information and treat such written record as a written submission.'';

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

''(B)(i)(I) Not later than the end of the period specified in subclause (II), the Inspector General shall determine whether the written complaint or information submitted under subparagraph (A) appears credible. Upon making such a determination, the Inspector General shall transmit to the Director notice of that determination, together with the complaint or information.

''(II) The period specified in this subclause is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subparagraph (A) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subparagraph.

''(ii) The Inspector General may transmit a complaint or information submitted under subparagraph (A) directly to the congressional intelligence committees—

''(I) without transmittal to the Director if the Inspector General determines that transmittal to the Director could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(II) following transmittal to the Director if the Director does not transmit the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C).'';

(3) in subparagraph (D)—

(A) in clause (i), by striking ''or does not transmit the complaint or information to the Director in accurate form under subparagraph (B),'' and inserting ''does not transmit the complaint or information to the Director in accurate form under subparagraph (B)(i)(I), or makes a determination pursuant

to subparagraph (B)(ii)(I) but does not transmit the complaint or information to the congressional intelligence committees within 21 calendar days of receipt,''; and

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

''(ii) An employee may contact the congressional intelligence committees directly as described in clause (i) only if—

''(I) the employee, before making such a contact—

''(aa) transmits to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

''(bb) obtains and follows from the Director, through the Inspector General, direction on how to contact the congressional intelligence committees in accordance with appropriate security practices; or

''(II) the Inspector General—

''(aa) determines that—

''(AA) a transmittal under subclause (I) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(BB) the Director has failed to provide adequate direction pursuant to item (bb) of subclause (I) within 7 calendar days of a transmittal under such subclause; and

''(bb) provides the employee direction on how to contact the congressional intelligence committees in accordance with appropriate security practices.''; and

(4) by adding at the end the following:

''(J) In this paragraph, the term 'employee', with respect to an employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community who may submit a complaint or information to the Inspector General under subparagraph (A), means—

''(i) a current employee at the time of such submission; or

''(ii) a former employee at the time of such submission, if such complaint or information arises from and relates to the period of employment as such an employee.''.

(b) INSPECTOR GENERAL OF THE CENTRAL INTELLIGENCE AGENCY.—Section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)) is amended—

(1) in subparagraph (A)—

(A) by inserting (i) before ''An employee'';

(B) by inserting ''in writing'' before ''to the Inspector General''; and

(C) by adding at the end the following:

''(ii) The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this subparagraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or information and treat such written record as a written submission.'';

(2) in subparagraph (B)—

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

''(i)(I) Not later than the end of the period specified in subclause (II), the Inspector General shall determine whether the written complaint or information submitted under subparagraph (A) appears credible. Upon making such a determination, the Inspector General shall transmit to the Director notice of that determination, together with the complaint or information.

''(II) The period specified in this subclause is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subparagraph (A) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subparagraph.''; and

(B) by adding at the end the following:

''(iii) The Inspector General may transmit a complaint or information submitted under subparagraph (A) directly to the congressional intelligence committees—

''(I) without transmittal to the Director if the Inspector General determines that transmittal to the Director could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information;

''(II) following transmittal to the Director if the Director does not transmit the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C) and has not made a determination regarding a conflict of interest pursuant to clause (ii); or

''(III) following transmittal to the Director and a determination by the Director that a conflict of interest exists pursuant to clause (ii) if the Inspector General determines that—

''(aa) transmittal to the Director of National Intelligence could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(bb) the Director of National Intelligence has not transmitted the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C).'';

(3) in subparagraph (D)—

(A) in clause (i), by striking ''or does not transmit the complaint or information to the Director in accurate form under subparagraph (B),'' and inserting ''does not transmit the complaint or information to the Director in accurate form under subparagraph (B)(i)(I), or makes a determination pursuant to subparagraph (B)(iii)(I) but does not transmit the complaint or information to the congressional intelligence committees within 21 calendar days of receipt,''; and

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

''(ii) An employee may contact the congressional intelligence committees directly as described in clause (i) only if—

''(I) the employee, before making such a contact—

''(aa) transmits to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

''(bb) obtains and follows from the Director, through the Inspector General, direction on how to contact the congressional intelligence committees in accordance with appropriate security practices; or

''(II) the Inspector General—

''(aa) determines that—

''(AA) the transmittal under subclause (I) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(BB) the Director has failed to provide adequate direction pursuant to item (bb) of subclause (I) within 7 calendar days of a transmittal under such subclause; and

''(bb) provides the employee direction on how to contact the congressional intelligence committees in accordance with appropriate security practices.''; and

(4) by adding at the end the following:

''(I) In this paragraph, the term 'employee', with respect to an employee of the Agency, or of a contractor to the Agency, who may submit a complaint or information to the Inspector General under subparagraph (A), means—

''(i) a current employee at the time of such submission; or

''(ii) a former employee at the time of such submission, if such complaint or information arises from and relates to the period of employment as such an employee.''.

(c) OTHER INSPECTORS GENERAL OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.—Section 416 of title 5, United States Code, is amended—

(1) in subsection (a)—

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

(B) by inserting before paragraph (2), as redesignated by paragraph (1), the following:

''(1) EMPLOYEE.—The term 'employee', with respect to an employee of an element of the Federal Government covered by subsection (b), or of a contractor to such an element, who may submit a complaint or information to an Inspector General under such subsection, means—

''(A) a current employee at the time of such submission; or

''(B) a former employee at the time of such submission, if such complaint or information arises from and relates to the period of employment as such an employee.'';

(2) in subsection (b)—

(A) in paragraph (1)—

(i) in the paragraph heading, by inserting ''; SUPPORT FOR WRITTEN SUBMISSION''; after ''MADE'';

(ii) by inserting ''in writing'' after ''may report the complaint or information'' each place it appears; and

(iii) in subparagraph (B), by inserting ''in writing'' after ''such complaint or information''; and

(B) by adding at the end the following:

''(E) SUPPORT FOR WRITTEN SUBMISSION.—The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this paragraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or information and treat such written record as a written submission.'';

(3) in subsection (c)—

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

''(1) CREDIBILITY.—

''(A) DETERMINATION.—Not later than the end of the period specified in subparagraph (B), the Inspector General shall determine whether the written complaint or information submitted under subsection (b) appears credible. Upon making such a determination, the Inspector General shall transmit to the head of the establishment notice of that determination, together with the complaint or information.

''(B) PERIOD SPECIFIED.—The period specified in this subparagraph is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subsection (b) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subsection.''; and

(B) by adding at the end the following:

''(3) TRANSMITTAL DIRECTLY TO INTELLIGENCE COMMITTEES.—The Inspector General may transmit the complaint or information directly to the intelligence committees—

''(A) without transmittal to the head of the establishment if the Inspector General determines that transmittal to the head of the establishment could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information;

''(B) following transmittal to the head of the establishment if the head of the establishment does not transmit the complaint or information to the intelligence committees within the time period specified in subsection (d) and has not made a determination regarding a conflict of interest pursuant to paragraph (2); or

''(C) following transmittal to the head of the establishment and a determination by the head of the establishment that a conflict of interest exists pursuant to paragraph (2) if the Inspector General determines that—

''(i) transmittal to the Director of National Intelligence or the Secretary of Defense could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(ii) the Director of National Intelligence or the Secretary of Defense has not transmitted the complaint or information to the intelligence committees within the time period specified in subsection (d).'';

(4) in subsection (e)(1), by striking ''or does not transmit the complaint or information to the head of the establishment in accurate form under subsection (c),'' and inserting ''does not transmit the complaint or information to the head of the establishment in accurate form under subsection (c)(1)(A), or makes a determination pursuant to subsection (c)(3)(A) but does not transmit the complaint or information to the intelligence committees within 21 calendar days of receipt,''; and

(5) in subsection (e), by striking paragraph (2) and inserting the following:

''(2) LIMITATION.—An employee may contact the intelligence committees directly as described in paragraph (1) only if—

''(A) the employee, before making such a contact—

''(i) transmits to the head of the establishment, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the intelligence committees directly; and

''(ii) obtains and follows from the head of the establishment, through the Inspector General, direction on how to contact the intelligence committees in accordance with appropriate security practices; or

''(B) the Inspector General—

''(i) determines that the transmittal under subparagraph (A) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(ii) determines that the head of the establishment has failed to provide adequate direction pursuant to clause (ii) of subparagraph (A) within 7 calendar days of a transmittal under such subparagraph; and

''(iii) provides the employee direction on how to contact the intelligence committees in accordance with appropriate security practices.''.

(d) RULE OF CONSTRUCTION.—Nothing in this section or an amendment made by this section shall be construed to revoke or diminish any right of an individual provided by section 2303 or 7211 of title 5, United States Code, to make a protected disclosure to any congressional committee.

SEC. 802. PROHIBITION AGAINST DISCLOSURE OF WHISTLEBLOWER IDENTITY AS ACT OF REPRISAL.

(a) IN GENERAL.—Section 1104(a) of the National Security Act of 1947 (50 U.S.C. 3234(a)) is amended—

(1) in paragraph (3)—

(A) in subparagraph (I), by striking ''; or'' and inserting a semicolon;

(B) by redesignating subparagraph (J) as subparagraph (K); and

(C) by inserting after subparagraph (I) the following:

''(J) an unauthorized whistleblower identity disclosure;''; and

(2) by adding at the end the following:

''(5) UNAUTHORIZED WHISTLEBLOWER IDENTITY DISCLOSURE.—The term 'unauthorized whistleblower identity disclosure' means, with respect to an employee or a contractor employee described in paragraph (3), a knowing and willful disclosure revealing the identity or other personally identifiable information of the employee or contractor employee so as to identify the employee or contractor employee as an employee or contractor employee who has made a lawful disclosure described in subsection (b) or (c), but does not include such a knowing and willful disclosure that meets any of the following criteria:

''(A) Such disclosure was made with the express consent of the employee or contractor employee.

''(B) Such disclosure was made during the course of reporting or remedying the subject of the lawful disclosure of the whistleblower through management, legal, or oversight processes, including such processes relating to human resources, equal opportunity, security, or an Inspector General.

''(C) An Inspector General with oversight responsibility for the relevant covered intelligence community element determines that such disclosure—

''(i) was unavoidable under section 103H of this Act (50 U.S.C. 3033), section 17 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517), section 407 of title 5, United States Code, or section 420(b)(2)(B) of such title;

''(ii) was made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken; or

''(iii) was required by statute or an order from a court of competent jurisdiction.''.

(b) HARMONIZATION OF ENFORCEMENT.—Subsection (f) of such section is amended to read as follows:

''(f) ENFORCEMENT.—

''(1) IN GENERAL.—Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section.

''(2) HARMONIZATION WITH OTHER ENFORCEMENT.—To the fullest extent possible, the President shall provide for enforcement of this section in a manner that is consistent with the enforcement of section 2302(b)(8) of title 5, United States Code, especially with respect to policies and procedures used to adjudicate alleged violations of such section.''.

SEC. 803. PROTECTION FOR INDIVIDUALS MAKING AUTHORIZED DISCLOSURES TO INSPECTORS GENERAL OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.

(a) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—Section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 3033(g)(3)) is amended—

(1) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively;

(2) by adding at the end the following new subparagraph:

''(B) An individual may disclose classified information to the Inspector General in accordance with the applicable security standards and procedures established under Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or section 803, chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.), or any applicable provision of law. Such a disclosure of classified information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

''(i) any otherwise applicable nondisclosure agreement;

''(ii) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information) or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

''(iii) section 798 of title 18, United States Code, or any other provision of law relating to the unauthorized disclosure of national security information.''; and

(3) in the paragraph enumerator, by striking ''(3) '' and inserting ''(3)(A)''.

(b) INSPECTOR GENERAL OF THE CENTRAL INTELLIGENCE AGENCY.—Section 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(e)(3)) is amended—

(1) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively;

(2) by adding at the end the following new subparagraph:

''(B) An individual may disclose classified information to the Inspector General in accordance with the applicable security standards and procedures established under Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or 803 of the National Security Act of 1947 (50 U.S.C. 3024; 3162a), or chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.). Such a disclosure of classified information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

''(i) any otherwise applicable nondisclosure agreement;

''(ii) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

''(iii) section 798 of title 18, United States Code, or any other provision of law relating to the unauthorized disclosure of national security information.''; and

(3) in the paragraph enumerator, by striking ''(3) '' and inserting ''(3)(A)''.

(c) OTHER INSPECTORS GENERAL OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.—Section 416 of title 5, United States Code, is amended by adding at the end the following new subsection:

''(i) PROTECTION FOR INDIVIDUALS MAKING AUTHORIZED DISCLOSURES.—An individual may disclose classified information to an Inspector General of an element of the intelligence community in accordance with the applicable security standards and procedures established under Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or 803 of the National Security Act of 1947 (50 U.S.C. 3024; 3162a), or chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.). Such a disclosure of classified information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

''(1) any otherwise applicable nondisclosure agreement;

''(2) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

''(3) section 798 of title 18, or any other provision of law relating to the unauthorized disclosure of national security information.''.

SEC. 804. CLARIFICATION OF AUTHORITY OF CERTAIN INSPECTORS GENERAL TO RECEIVE PROTECTED DISCLOSURES.

Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subsection (b)(1), by inserting ''or covered intelligence community element'' after ''the appropriate inspector general of the employing agency''; and

(2) in subsection (c)(1)(A), by inserting ''or covered intelligence community element'' after ''the appropriate inspector general of the employing or contracting agency''.

SEC. 805. WHISTLEBLOWER PROTECTIONS RELATING TO PSYCHIATRIC TESTING OR EXAMINATION.

(a) PROHIBITED PERSONNEL PRACTICES.—Section 1104(a)(3) of the National Security Act of 1947 (50 U.S.C. 3234(a)(3)) is amended—

(1) in subparagraph (I), by striking ''; or'' and inserting a semicolon;

(2) by redesignating subparagraph (J) as subparagraph (K); and

(3) by inserting after subparagraph (I) the following new subparagraph:

''(J) a decision to order psychiatric testing or examination; or''.

(b) APPLICATION.—The amendments made by this section shall apply with respect to matters arising under section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) on or after the date of the enactment of this Act.

SEC. 806. ESTABLISHING PROCESS PARITY FOR ADVERSE SECURITY CLEARANCE AND ACCESS DETERMINATIONS.

Subparagraph (C) of section 3001(j)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(4)) is amended to read as follows:

''(C) CONTRIBUTING FACTOR.—

''(i) IN GENERAL.—Subject to clause (iii), in determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if the individual has demonstrated that a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual.

''(ii) CIRCUMSTANTIAL EVIDENCE.—An individual under clause (i) may demonstrate that the disclosure was a contributing factor in the adverse security clearance or access determination taken against the individual through circumstantial evidence, such as evidence that—

''(I) the official making the determination knew of the disclosure; and

''(II) the determination occurred within a period such that a reasonable person could conclude that the disclosure was a contributing factor in the determination.

''(iii) DEFENSE.—In determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall not find that paragraph (1) was violated if, after a finding that a disclosure was a contributing factor, the agency demonstrates by clear and convincing evidence that it would have made the same security clearance or access determination in the absence of such disclosure.''.

SEC. 807. ELIMINATION OF CAP ON COMPENSATORY DAMAGES FOR RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.

Section 3001(j)(4)(B) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(4)(B)) is amended, in the second sentence, by striking ''not to exceed $300,000''.

TITLE IX—ANOMALOUS HEALTH INCIDENTS

SEC. 901. MODIFICATION OF AUTHORITY FOR SECRETARY OF STATE AND HEADS OF OTHER FEDERAL AGENCIES TO PAY COSTS OF TREATING QUALIFYING INJURIES AND MAKE PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN.

Section 901(e) of division J of the Further Consolidated Appropriations Act, 2020 (22 U.S.C. 2680b(e)) is amended—

(1) in paragraph (1)—

(A) in the matter before subparagraph (A), by striking ''a employee who, on or after January 1, 2016'' and inserting ''an employee who, on or after September 11, 2001''; and

(B) in subparagraph (A), by inserting '', or duty station in the United States'' before the semicolon;

(2) in paragraph (2)—

(A) by striking ''January 1, 2016'' and inserting ''September 11, 2001''; and

(B) by inserting '', or duty station in the United States,'' after ''pursuant to subsection (f)'';

(3) in paragraph (3)—

(A) in the matter before subparagraph (A), by striking ''January 1, 2016'' and inserting ''September 11, 2001''; and

(B) in subparagraph (A), by inserting '', or duty station in the United States'' before the semicolon; and

(4) in paragraph (4)—

(A) in subparagraph (A)(i), by inserting '', or duty station in the United States'' before the semicolon; and

(B) in subparagraph (B)(i), by inserting '', or duty station in the United States'' before the semicolon.

TITLE X—UNIDENTIFIED ANOMALOUS PHENOMENA

SEC. 1001. COMPTROLLER GENERAL OF THE UNITED STATES REVIEW OF ALL-DOMAIN ANOMALY RESOLUTION OFFICE.

(a) DEFINITIONS.—In this section, the terms ''congressional defense committees'', ''congressional leadership'', and ''unidentified anomalous phenomena'' have the meanings given such terms in section 1683(n) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(n)).

(b) REVIEW REQUIRED.—The Comptroller General of the United States shall conduct a review of the All-domain Anomaly Resolution Office (in this section referred to as the ''Office'').

(c) ELEMENTS.—The review conducted pursuant to subsection (b) shall include the following:

(1) A review of the implementation by the Office of the duties and requirements of the Office under section 1683 of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373), such as the process for operational unidentified anomalous phenomena reporting and coordination with the Department of Defense, the intelligence community, and other departments and agencies of the Federal Government and non-Government entities.

(2) A review of such other matters relating to the activities of the Office that pertain to unidentified anomalous phenomena as the Comptroller General considers appropriate.

(d) REPORT.—Following the review required by subsection (b), in a timeframe mutually agreed upon by the congressional intelligence committees, the congressional defense committees, congressional leadership, and the Comptroller General, the Comptroller General shall submit to such committees and congressional leadership a report on the findings of the Comptroller General with respect to the review conducted under subsection (b).

SEC. 1002. SUNSET OF REQUIREMENTS RELATING TO AUDITS OF UNIDENTIFIED ANOMALOUS PHENOMENA HISTORICAL RECORD REPORT.

Section 6001 of the Intelligence Authorization Act for Fiscal Year 2023 (50 U.S.C. 3373 note) is amended—

(1) in subsection (b)(2), by inserting ''until April 1, 2025'' after ''quarterly basis''; and

(2) in subsection (c), by inserting ''until June 30, 2025'' after ''semiannually thereafter''.

SEC. 1003. FUNDING LIMITATIONS RELATING TO UNIDENTIFIED ANOMALOUS PHENOMENA.

(a) DEFINITIONS.—In this section:

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

(A) the Select Committee on Intelligence, the Committee on Armed Services, the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Armed Services, the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term ''congressional leadership'' means—

(A) the majority leader of the Senate;

(B) the minority leader of the Senate;

(C) the Speaker of the House of Representatives; and

(D) the minority leader of the House of Representatives.

(3) NATIONAL INTELLIGENCE PROGRAM.—The term ''National Intelligence Program'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(4) UNIDENTIFIED ANOMALOUS PHENOMENA.—The term ''unidentified anomalous phenomena'' has the meaning given such term in section 1683(n) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(n)).

(b) LIMITATIONS.—None of the funds authorized to be appropriated by this division for the National Intelligence Program may be obligated or expended in support of any activity involving unidentified anomalous phenomena protected under any form of special access or restricted access limitation unless the Director of National Intelligence has provided the details of the activity to the appropriate committees of Congress and congressional leadership, including for any activities described in a report released by the All-domain Anomaly Resolution Office in fiscal year 2024.

(c) LIMITATION REGARDING INDEPENDENT RESEARCH AND DEVELOPMENT.—Independent research and development funding relating to unidentified anomalous phenomena shall not be allowable as indirect expenses for purposes of contracts covered by such instruction, unless such material and information is made available to the appropriate congressional committees and leadership.

TITLE XI—OTHER MATTERS

SEC. 1101. LIMITATION ON DIRECTIVES UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 RELATING TO CERTAIN ELECTRONIC COMMUNICATION SERVICE PROVIDERS.

Section 702(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(i)) is amended by adding at the end the following:

''(7) LIMITATION RELATING TO CERTAIN ELECTRONIC COMMUNICATION SERVICE PROVIDERS.—

''(A) DEFINITIONS.—In this paragraph:

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

''(I) the congressional intelligence committees;

''(II) the Committee on the Judiciary and the Committee on Appropriations of the Senate; and

''(III) the Committee on the Judiciary and the Committee on Appropriations of the House of Representatives.

''(ii) COVERED ELECTRONIC COMMUNICATION SERVICE PROVIDER.—

''(I) IN GENERAL.—Subject to subclause (II), the term 'covered electronic communication service provider' means—

''(aa) a service provider described in section 701(b)(4)(E);

''(bb) a custodian of an entity as defined in section 701(b)(4)(F); or

''(cc) an officer, employee, or agent of a service provider described in section 701(b)(4)(E).

''(II) EXCLUSION.—The term 'covered electronic communication service provider' does not include—

''(aa) an electronic communication service provider described in subparagraph (A), (B), (C), or (D) of section 701(b)(4); or

''(bb) an officer, employee, or agent of an electronic communication service provider described in subparagraph (A), (B), (C), or (D) of section 701(b)(4).

''(iii) COVERED OPINIONS.—The term 'covered opinions' means the opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review authorized for public release on August 23, 2023 (Opinion and Order, In re Petition to Set Aside or Modify Directive Issued to [REDACTED], No. [REDACTED], (FISA Ct. [REDACTED] 2022) (Contreras J.); Opinion, In re Petition to Set Aside or Modify Directive Issued to [REDACTED], No. [REDACTED], (FISA Ct. Rev. [REDACTED] 2023) (Sentelle, J.; Higginson, J.; Miller J.)).

''(B) LIMITATION.—A directive may not be issued under paragraph (1) to a covered electronic communication service provider unless the covered electronic communication service provider is a provider of the type of service at issue in the covered opinions.

''(C) REQUIREMENTS FOR DIRECTIVES TO COVERED ELECTRONIC COMMUNICATION SERVICE PROVIDERS.—

''(i) IN GENERAL.—Subject to clause (ii), any directive issued under paragraph (1) on or after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025 to a covered electronic communication service provider that is not prohibited by subparagraph (B) of this paragraph shall include a summary description of the services at issue in the covered opinions.

''(ii) DUPLICATE SUMMARIES NOT REQUIRED.—A directive need not include a summary description of the services at issue in the covered opinions if such summary was included in a prior directive issued to the covered electronic communication service provider and the summary has not materially changed.

''(D) FOREIGN INTELLIGENCE SURVEILLANCE COURT NOTIFICATION AND REVIEW.—

''(i) NOTIFICATION.—

''(I) IN GENERAL.—Subject to subclause (II), on or after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025, each time the Attorney General and the Director of National Intelligence serve a directive under paragraph (1) to a covered electronic communication service provider that is not prohibited by subparagraph (B) and each time the Attorney General and the Director materially change a directive under paragraph (1) served on a covered electronic communication service provider that is not prohibited by subparagraph (B), the Attorney General shall provide the directive to the Foreign Intelligence Surveillance Court on or before the date that is 7 days after the date on which the Attorney General and the Director served the directive, along with a description of the covered electronic communication service provider to whom the directive is issued and the services at issue.

''(II) DUPLICATION NOT REQUIRED.—The Attorney General does not need to provide a directive or description to the Foreign Intelligence Surveillance Court under subclause (I) if a directive and description concerning the covered electronic communication service provider was previously provided to the Court and the directive or description has not materially changed.

''(ii) ADDITIONAL INFORMATION.—As soon as feasible and not later than the initiation of collection, the Attorney General shall, for each directive described in subparagraph (i), provide the Foreign Intelligence Surveillance Court a summary description of the type of equipment to be accessed, the nature of the access, and the form of assistance required pursuant to the directive.

''(iii) REVIEW.—

''(I) IN GENERAL.—The Foreign Intelligence Surveillance Court may review a directive received by the Court under clause (i) to determine whether the directive is consistent with subparagraph (B) and affirm, modify, or set aside the directive.

''(II) NOTICE OF INTENT TO REVIEW.—Not later than 10 days after the date on which the Court receives information under clause (ii) with respect to a directive, the Court shall provide notice to the Attorney General and cleared counsel for the covered electronic communication service provider indicating whether the Court intends to undertake a review under subclause (I) of this clause.

''(III) COMPLETION OF REVIEWS.—In a case in which the Court provides notice under subclause (II) indicating that the Court intends to review a directive under subclause (I), the Court shall, not later than 30 days after the date on which the Court provides notice under subclause (II) with respect to the directive, complete the review.

''(E) CONGRESSIONAL OVERSIGHT.—

''(i) NOTIFICATION.—

''(I) IN GENERAL.—Subject to subclause (II), on or after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025, each time the Attorney General and the Director of National Intelligence serve a directive under paragraph (1) on a covered electronic communication service provider that is not prohibited by subparagraph (B) and each time the Attorney General and the Director materially change a directive under paragraph (1) served on a covered electronic communication service provider that is not prohibited by subparagraph (B), the Attorney General shall submit to the appropriate committees of Congress the directive on or before the date that is 7 days after the date on which the Attorney General and the Director serve the directive, along with a description of the covered electronic communication service provider to whom the directive is issued and the services at issue.

''(II) DUPLICATION NOT REQUIRED.—The Attorney General does not need to submit a directive or description to the appropriate committees of Congress under subclause (I) if a directive and description concerning the covered electronic communication service provider was previously submitted to the appropriate committees of Congress and the directive or description has not materially changed.

''(ii) ADDITIONAL INFORMATION.—As soon as feasible and not later than the initiation of collection, the Attorney General shall, for each directive described in subparagraph (i), provide the appropriate committees of Congress a summary description of the type of equipment to be accessed, the nature of the access, and the form of assistance required pursuant to the directive.

''(iii) REPORTING.—

''(I) QUARTERLY REPORTS.—Not later than 90 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025 and not less frequently than once each quarter thereafter, the Attorney General shall submit to the appropriate committees of Congress a report on the number of directives served, during the period covered by the report, under paragraph (1) to a covered electronic communication service provider and the number of directives provided during the same period to the Foreign Intelligence Surveillance Court under subparagraph (D)(i).

''(II) FORM OF REPORTS.—Each report submitted pursuant to subclause (I) shall be submitted in unclassified form, but may include a classified annex.

''(III) SUBMITTAL OF COURT OPINIONS.—Not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues an opinion relating to a directive issued to a covered electronic communication service provider under paragraph (1), the Attorney General shall submit to the appropriate committees of Congress a copy of the opinion.''.

SEC. 1102. STRENGTHENING ELECTION CYBERSECURITY TO UPHOLD RESPECT FOR ELECTIONS THROUGH INDEPENDENT TESTING ACT OF 2024.

(a) SHORT TITLE.—This section may be cited as the ''Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2024'' or the ''SECURE IT Act of 2024''.

(b) REQUIRING PENETRATION TESTING AS PART OF THE TESTING AND CERTIFICATION OF VOTING SYSTEMS.—Section 231 of the Help America Vote Act of 2002 (52 U.S.C. 20971) is amended by adding at the end the following new subsection:

''(e) REQUIRED PENETRATION TESTING.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, the Commission shall provide for the conduct of penetration testing as part of the testing, certification, decertification, and recertification of voting system hardware and software by the Commission based on accredited laboratories under this section.

''(2) ACCREDITATION.—The Commission shall develop a program for the acceptance of the results of penetration testing on election systems. The penetration testing required by this subsection shall be required for Commission certification. The Commission shall vote on the selection of any entity identified. The requirements for such selection shall be based on consideration of an entity's competence to conduct penetration testing under this subsection. The Commission may consult with the National Institute of Standards and Technology or any other appropriate Federal agency on lab selection criteria and other aspects of this program.''.

(c) INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS.—

(1) IN GENERAL.—Subtitle D of title II of the Help America Vote Act of 2002 (42 U.S.C. 15401 et seq.) is amended by adding at the end the following new part:

"PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PILOT PROGRAM FOR ELECTION SYSTEMS

"SEC. 297. INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PILOT PROGRAM FOR ELECTION SYSTEMS.

''(a) IN GENERAL.—

''(1) ESTABLISHMENT.—The Commission, in consultation with the Secretary, shall establish an Independent Security Testing and Coordinated Vulnerability Disclosure Pilot Program for Election Systems (VDP–E) (in this section referred to as the 'program') to test for and disclose cybersecurity vulnerabilities in election systems.

''(2) DURATION.—The program shall be conducted for a period of 5 years.

''(3) REQUIREMENTS.—In carrying out the program, the Commission, in consultation with the Secretary, shall—

''(A) establish a mechanism by which an election systems vendor may make their election system (including voting machines and source code) available to cybersecurity researchers participating in the program;

''(B) provide for the vetting of cybersecurity researchers prior to their participation in the program, including the conduct of background checks;

''(C) establish terms of participation that—

''(i) describe the scope of testing permitted under the program;

''(ii) require researchers to—

''(I) notify the vendor, the Commission, and the Secretary of any cybersecurity vulnerability they identify with respect to an election system; and

''(II) otherwise keep such vulnerability confidential for 180 days after such notification;

''(iii) require the good faith participation of all participants in the program;

''(iv) require an election system vendor, within 180 days after validating notification of a critical or high vulnerability (as defined by the National Institute of Standards and Technology) in an election system of the vendor, to—

''(I) send a patch or propound some other fix or mitigation for such vulnerability to the appropriate State and local election officials, in consultation with the researcher who discovered it; and

''(II) notify the Commission and the Secretary that such patch has been sent to such officials;

''(D) in the case where a patch or fix to address a vulnerability disclosed under subparagraph (C)(ii)(I) is intended to be applied to a system certified by the Commission, provide—

''(i) for the expedited review of such patch or fix within 90 days after receipt by the Commission; and

''(ii) if such review is not completed by the last day of such 90-day period, that such patch or fix shall be deemed to be certified by the Commission, subject to any subsequent review of such determination by the Commission; and

''(E) 180 days after the disclosure of a vulnerability under subparagraph (C)(ii)(I), notify the Director of the Cybersecurity and Infrastructure Security Agency of the vulnerability for inclusion in the database of Common Vulnerabilities and Exposures.

''(4) VOLUNTARY PARTICIPATION; SAFE HARBOR.—

''(A) VOLUNTARY PARTICIPATION.—Participation in the program shall be voluntary for election systems vendors and researchers.

''(B) SAFE HARBOR.—When conducting research under this program, such research and subsequent publication shall be—

''(i) authorized in accordance with section 1030 of title 18, United States Code (commonly known as the 'Computer Fraud and Abuse Act'), (and similar State laws), and the election system vendor will not initiate or support legal action against the researcher for accidental, good faith violations of the program; and

''(ii) exempt from the anti-circumvention rule of section 1201 of title 17, United States Code (commonly known as the 'Digital Millennium Copyright Act'), and the election system vendor will not bring a claim against a researcher for circumvention of technology controls.

''(C) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to limit or otherwise affect any exception to the general prohibition against the circumvention of technological measures under subparagraph (A) of section 1201(a)(1) of title 17, United States Code, including with respect to any use that is excepted from that general prohibition by the Librarian of Congress under subparagraphs (B) through (D) of such section 1201(a)(1).

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

''(A) CYBERSECURITY VULNERABILITY.—The term 'cybersecurity vulnerability' means, with respect to an election system, any security vulnerability that affects the election system.

''(B) ELECTION INFRASTRUCTURE.—The term 'election infrastructure' means—

''(i) storage facilities, polling places, and centralized vote tabulation locations used to support the administration of elections for public office; and

''(ii) related information and communications technology, including—

''(I) voter registration databases;

''(II) election management systems;

''(III) voting machines;

''(IV) electronic mail and other communications systems (including electronic mail and other systems of vendors who have entered into contracts with election agencies to support the administration of elections, manage the election process, and report and display election results); and

''(V) other systems used to manage the election process and to report and display election results on behalf of an election agency.

''(C) ELECTION SYSTEM.—The term 'election system' means any information system that is part of an election infrastructure, including any related information and communications technology described in subparagraph (B)(ii).

''(D) ELECTION SYSTEM VENDOR.—The term 'election system vendor' means any person providing, supporting, or maintaining an election system on behalf of a State or local election official.

''(E) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

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

''(G) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).''.

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended by adding at the end of the items relating to subtitle D of title II the following:

''PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS

''Sec. 297. Independent security testing and coordinated cybersecurity vulnerability disclosure program for election systems.''.

SEC. 1103. PARITY IN PAY FOR STAFF OF THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD AND THE INTELLIGENCE COMMUNITY.

Section 1061(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(j)(1)) is amended by striking ''except that'' and all that follows through the period at the end and inserting ''except that no rate of pay fixed under this subsection may exceed the highest amount paid by any element of the intelligence community for a comparable position, based on salary information provided to the chairman of the Board by the Director of National Intelligence.''.

SEC. 1104. MODIFICATION AND REPEAL OF REPORTING REQUIREMENTS.

(a) BRIEFING ON IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.—Section 6705(a)(1) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412(a)(1)) is amended by striking '', and not less frequently than once each year thereafter provide a briefing to Congress,''.

(b) REPORTS AND BRIEFINGS ON NATIONAL SECURITY EFFECTS OF GLOBAL WATER INSECURITY AND EMERGING INFECTIOUS DISEASES AND PANDEMICS.—Section 6722(b) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3024 note; division E of Public Law 116–92) is amended by—

(1) striking paragraph (2); and

(2) redesignating paragraphs (3) and (4) as paragraphs (2) and (3), respectively.

(c) REPEAL OF REPORT ON REMOVAL OF SATELLITES AND RELATED ITEMS FROM THE UNITED STATES MUNITIONS LIST.—Section 1261(e) of the National Defense Authorization Act for Fiscal Year 2013 (22 U.S.C. 2778 note; Public Law 112–239) is repealed.

(d) BRIEFING ON REVIEW OF INTELLIGENCE COMMUNITY ANALYTIC PRODUCTION.—Section 1019(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3364(c)) is amended by striking ''December 1'' and inserting ''February 1''.

(e) REPEAL OF REPORT ON OVERSIGHT OF FOREIGN INFLUENCE IN ACADEMIA.—Section 5713 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3369b) is repealed.

(f) REPEAL OF BRIEFING ON IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.—Section 6705 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412) is amended—

(1) by striking subsection (b);

(2) by striking the enumerator and heading for subsection (a);

(3) by redesignating paragraphs (1) and (2) as subsections (a) and (b), respectively, and moving such subsections, as so redesignated, 2 ems to the left;

(4) in subsection (a), as so redesignated, by redesignating subparagraphs (A) and (B) as paragraphs (1) and (2), respectively, and moving such paragraphs, as so redesignated, 2 ems to the left; and

(5) in paragraph (1), as so redesignated, by redesignating clauses (i) through (v) as subparagraphs (A) through (E), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the left.

(g) REPEAL OF REPORT ON FOREIGN INVESTMENT RISKS.—Section 6716 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3370a) is repealed.

(h) REPEAL OF REPORT ON INTELLIGENCE COMMUNITY LOAN REPAYMENT PROGRAMS.—Section 6725(c) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334g(c)) is repealed.

(i) REPEAL OF REPORT ON DATA COLLECTION ON ATTRITION IN INTELLIGENCE COMMUNITY.—Section 306(c) of the Intelligence Authorization Act for Fiscal Year 2021 (50 U.S.C. 3334h(c)) is repealed.

SEC. 1105. TECHNICAL AMENDMENTS.

(a) REQUIREMENTS RELATING TO CONSTRUCTION OF FACILITIES TO BE USED PRIMARILY BY INTELLIGENCE COMMUNITY.—Section 602(a) of the Intelligence Authorization Act for Fiscal Year 1995 (50 U.S.C. 3304(a)) is amended—

(1) in paragraph (1), by striking ''$6,000,000'' and inserting ''$9,000,000''; and

(2) in paragraph (2)—

(A) by striking ''$2,000,000'' each place it appears and inserting ''$4,000,000''; and

(B) by striking ''$6,000,000'' and inserting ''$9,000,000''.

(b) COPYRIGHT PROTECTION FOR CIVILIAN FACULTY OF CERTAIN ACCREDITED INSTITUTIONS.—Section 105 of title 17, United States Code, is amended to read as follows:

''§ 105. Subject matter of copyright: United States Government works

''(a) IN GENERAL.—Copyright protection under this title is not available for any work of the United States Government, but the United States Government is not precluded from receiving and holding copyrights transferred to it by assignment, bequest, or otherwise.

''(b) COPYRIGHT PROTECTION OF CERTAIN WORKS.—Subject to subsection (c), the covered author of a covered work owns the copyright to that covered work.

''(c) USE BY FEDERAL GOVERNMENT.—

''(1) SECRETARY OF DEFENSE AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at a covered institution described in subparagraphs (A) through (K) of subsection (d)(2), the Secretary of Defense may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

''(2) SECRETARY OF HOMELAND SECURITY AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(L), the Secretary of Homeland Security may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

''(3) DIRECTOR OF NATIONAL INTELLIGENCE AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(M), the Director of National Intelligence may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

''(4) SECRETARY OF TRANSPORTATION AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(N), the Secretary of Transportation may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

''(d) DEFINITIONS.—In this section:

''(1) COVERED AUTHOR.—The term 'covered author' means a civilian member of the faculty of a covered institution.

''(2) COVERED INSTITUTION.—The term 'covered institution' means the following:

''(A) National Defense University.

''(B) United States Military Academy.

''(C) Army War College.

''(D) United States Army Command and General Staff College.

''(E) United States Naval Academy.

''(F) Naval War College.

''(G) Naval Postgraduate School.

''(H) Marine Corps University.

''(I) United States Air Force Academy.

''(J) Air University.

''(K) Defense Language Institute.

''(L) United States Coast Guard Academy.

''(M) National Intelligence University.

''(N) United States Merchant Marine Academy.

''(3) COVERED WORK.—The term 'covered work' means a literary work produced by a covered author in the course of employment at a covered institution for publication by a scholarly press or journal.''.

SA 3210. Mr. HICKENLOOPER (for himself, Ms. SINEMA, and Ms. LUMMIS) submitted an amendment intended to be proposed by him to the bill S. 4638, to authorize appropriations for fiscal year 2025 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XV, add the following:

Subtitle E—Orbital Sustainability Act of 2024

SEC. 1551. SHORT TITLE.

This subtitle may be cited as the ''Orbital Sustainability Act of 2024'' or the ''ORBITS Act of 2024''.

SEC. 1552. FINDINGS; SENSE OF CONGRESS.

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

(1) The safety and sustainability of operations in low-Earth orbit and nearby orbits in outer space have become increasingly endangered by a growing amount of orbital debris.

(2) Exploration and scientific research missions and commercial space services of critical importance to the United States rely on continued and secure access to outer space.

(3) Efforts by nongovernmental space entities to apply lessons learned through standards and best practices will benefit from government support for implementation both domestically and internationally.

(b) SENSE OF CONGRESS.—It is the sense of Congress that to preserve the sustainability of operations in space, the United States Government should—

(1) to the extent practicable, develop and carry out programs, establish or update regulations, and commence initiatives to minimize orbital debris, including initiatives to demonstrate active debris remediation of orbital debris generated by the United States Government or other entities under the jurisdiction of the United States;

(2) lead international efforts to encourage other spacefaring countries to mitigate and remediate orbital debris under their jurisdiction and control; and

(3) encourage space system operators to continue implementing best practices for space safety when deploying satellites and constellations of satellites, such as transparent data sharing and designing for system reliability, so as to limit the generation of future orbital debris.

SEC. 1553. DEFINITIONS.

In this subtitle:

(1) ACTIVE DEBRIS REMEDIATION.—The term ''active debris remediation''—

(A) means the deliberate process of facilitating the de-orbit, repurposing, or other disposal of orbital debris, which may include moving orbital debris to a safe position, using an object or technique that is external or internal to the orbital debris; and

(B) does not include de-orbit, repurposing, or other disposal of orbital debris by passive means.

(2) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the National Aeronautics and Space Administration.

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

(A) the Committee on Appropriations, the Committee on Commerce, Science, and Transportation, the Committee on Foreign Relations, and the Committee on Armed Services of the Senate; and

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

(4) DEMONSTRATION PROJECT.—The term ''demonstration project'' means the active orbital debris remediation demonstration project carried out under section 1554(b).

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

(A) a United States-based—

(i) non-Federal, commercial entity;

(ii) institution of higher education (as defined in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a))); or

(iii) nonprofit organization;

(B) any other United States-based entity the Administrator considers appropriate; and

(C) a partnership of entities described in subparagraphs (A) and (B).

(6) ORBITAL DEBRIS.—The term ''orbital debris'' means any human-made space object orbiting Earth that—

(A) no longer serves an intended purpose; and

(B)(i) has reached the end of its mission; or

(ii) is incapable of safe maneuver or operation.

(7) PROJECT.—The term ''project'' means a specific investment with defined requirements, a life-cycle cost, a period of duration with a beginning and an end, and a management structure that may interface with other projects, agencies, and international partners to yield new or revised technologies addressing strategic goals.

(8) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

(9) SPACE TRAFFIC COORDINATION.—The term ''space traffic coordination'' means the planning, coordination, and on-orbit synchronization of activities to enhance the safety and sustainability of operations in the space environment.

SEC. 1554. ACTIVE DEBRIS REMEDIATION.

(a) PRIORITIZATION OF ORBITAL DEBRIS.—

(1) LIST.—Not later than 90 days after the date of the enactment of this Act, the Secretary, in consultation with the Administrator, the Secretary of Defense, the Secretary of State, the National Space Council, and representatives of the commercial space