To authorize appropriations for fiscal year 2024 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 22, 2023

Mr. WARNER, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

A BILL

To authorize appropriations for fiscal year 2024 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the “Intelligence Authorization Act for Fiscal Year 2024”.
(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—INTELLIGENCE ACTIVITIES

Sec. 101. Authorization of appropriations.
Sec. 102. Classified Schedule of Authorizations.
Sec. 103. Intelligence Community Management Account.
Sec. 104. Increase in employee compensation and benefits authorized by law.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Sec. 201. Authorization of appropriations.

TITLE III—INTELLIGENCE COMMUNITY MATTERS

Subtitle A—General Intelligence Community Matters

Sec. 301. Post-graduate employment of Department of Defense Cyber and Digital Service Academy scholarship recipients in intelligence community.
Sec. 302. Plan to recruit, train, and retain personnel with experience in financial intelligence and emerging technologies.
Sec. 304. In-State tuition rates for active duty members of the intelligence community.
Sec. 305. Standards, criteria, and guidance for counterintelligence vulnerability assessments and surveys.
Sec. 306. Improving administration of certain post-employment restrictions for intelligence community.
Sec. 307. Mission of the National Counterintelligence and Security Center.
Sec. 308. Prohibition relating to transport of individuals detained at United States Naval Station, Guantanamo Bay, Cuba.
Sec. 309. Department of Energy review of certain foreign visitors and assignees to National Laboratories.
Sec. 310. Congressional oversight of intelligence community risk assessments.
Sec. 311. Inspector General review of dissemination by Federal Bureau of Investigation Richmond, Virginia, field office of certain document.
Sec. 312. Office of Intelligence and Analysis.

Subtitle B—Central Intelligence Agency

Sec. 321. Protection of Central Intelligence Agency facilities and assets from unmanned aircraft.
Sec. 322. Change to penalties and increased availability of mental health treatment for unlawful conduct on Central Intelligence Agency installations.
Sec. 323. Modifications to procurement authorities of the Central Intelligence Agency.
Sec. 324. Establishment of Central Intelligence Agency standard workplace sexual misconduct complaint investigation procedure.

Sec. 325. Pay cap for diversity, equity, and inclusion staff and contract employees of the Central Intelligence Agency.

TITLE IV—MATTERS CONCERNING FOREIGN COUNTRIES

Subtitle A—People’s Republic of China

Sec. 401. Intelligence community coordinator for accountability of atrocities of the People’s Republic of China.

Sec. 402. Interagency working group and report on the malign efforts of the People’s Republic of China in Africa.

Sec. 403. Amendment to requirement for annual assessment by intelligence community working group for monitoring the economic and technological capabilities of the People's Republic of China.

Sec. 404. Assessments of reciprocity in the relationship between the United States and the People’s Republic of China.

Sec. 405. Annual briefing on intelligence community efforts to identify and mitigate Chinese Communist Party political influence operations and information warfare against the United States.

Sec. 406. Assessment of threat posed to United States ports by cranes manufactured by countries of concern.

Subtitle B—Russian Federation

Sec. 411. Assessment of lessons learned by intelligence community with respect to conflict in Ukraine.

Sec. 412. National intelligence estimate on long-term confrontation with Russia.

Subtitle C—Other Foreign Countries

Sec. 421. Report on efforts to capture and detain United States citizens as hostages.

Sec. 422. Sense of Congress on priority of fentanyl in National Intelligence Priorities Framework.

TITLE V—MATTERS PERTAINING TO UNITED STATES ECONOMIC AND EMERGING TECHNOLOGY COMPETITION WITH UNITED STATES ADVERSARIES

Subtitle A—General Matters

Sec. 501. Office of Global Competition Analysis.

Sec. 502. Assignment of detailees from intelligence community to Department of Commerce.

Sec. 503. Threats posed by information and communications technology and services transactions and other activities.

Sec. 504. Revision of regulations defining sensitive national security property for Committee on Foreign Investment in the United States reviews.

Sec. 505. Support of intelligence community for export controls and other missions of the Department of Commerce.

Sec. 506. Review regarding information collection and analysis with respect to economic competition.
Subtitle B—Next-generation Energy, Biotechnology, and Artificial Intelligence

Sec. 511. Expanded annual assessment of economic and technological capabilities of the People’s Republic of China.

Sec. 512. Procurement of public utility contracts.

Sec. 513. Assessment of using civil nuclear energy for intelligence community capabilities.

Sec. 514. Policies established by Director of National Intelligence for artificial intelligence capabilities.

Sec. 515. Strategy for submittal of notice by private persons to Federal agencies regarding certain risks and threats relating to artificial intelligence.

TITLE VI—WHISTLEBLOWER MATTERS

Sec. 601. Submittal to Congress of complaints and information by whistleblowers in the intelligence community.

Sec. 602. Prohibition against disclosure of whistleblower identity as reprisal against whistleblower disclosure by employees and contractors in intelligence community.

Sec. 603. Establishing process parity for adverse security clearance and access determinations.

Sec. 604. Elimination of cap on compensatory damages for retaliatory revocation of security clearances and access determinations.

Sec. 605. Modification and repeal of reporting requirements.

TITLE VII—CLASSIFICATION REFORM

Subtitle A—Classification Reform Act of 2023

CHAPTER 1—SHORT TITLE; DEFINITIONS

Sec. 701. Short title.

Sec. 702. Definitions.

CHAPTER 2—GOVERNANCE AND ACCOUNTABILITY FOR REFORM OF THE SECURITY CLASSIFICATION SYSTEM

Sec. 711. Executive Agent for Classification and Declassification.

Sec. 712. Executive Committee on Classification and Declassification Programs and Technology.

Sec. 713. Advisory bodies for Executive Agent for Classification and Declassification.

Sec. 714. Information Security Oversight Office.

CHAPTER 3—REDUCING OVERCLASSIFICATION

Sec. 721. Classification and declassification of information.

Sec. 722. Declassification working capital funds.

Sec. 723. Transparency officers.

CHAPTER 4—PREVENTING MISHANDLING OF CLASSIFIED INFORMATION

Sec. 731. Security review of certain records of the President and Vice President.

Sec. 732. Mandatory counterintelligence risk assessments.

Sec. 733. Minimum standards for Executive agency insider threat programs.
CHAPTER 5—Other Matters

Sec. 741. Prohibitions.
Sec. 742. Conforming amendment.
Sec. 743. Clerical amendment.

Subtitle B—Sensible Classification Act of 2023

Sec. 751. Short title.
Sec. 752. Definitions.
Sec. 753. Findings and sense of the Senate.
Sec. 754. Classification authority.
Sec. 755. Promoting efficient declassification review.
Sec. 756. Training to promote sensible classification.
Sec. 757. Improvements to Public Interest Declassification Board.
Sec. 758. Implementation of technology for classification and declassification.
Sec. 759. Studies and recommendations on necessity of security clearances.

TITLE VIII—Security Clearance and Trusted Workforce

Sec. 801. Review of shared information technology services for personnel vetting.
Sec. 802. Timeliness standard for rendering determinations of trust for personnel vetting.
Sec. 803. Annual report on personnel vetting trust determinations.
Sec. 804. Survey to assess strengths and weaknesses of Trusted Workforce 2.0.
Sec. 805. Prohibition on denial of eligibility for access to classified information solely because of past use of cannabis.

TITLE IX—Anomalous Health Incidents

Sec. 901. Improved funding flexibility for payments made by the Central Intelligence Agency for qualifying injuries to the brain.
Sec. 902. Clarification of requirements to seek certain benefits relating to injuries to the brain.
Sec. 903. Intelligence community implementation of HAVANA Act of 2021 authorities.
Sec. 904. Report and briefing on Central Intelligence Agency handling of anomalous health incidents.

TITLE X—Election Security


TITLE XI—Other Matters

Sec. 1101. Modification of reporting requirement for All-domain Anomaly Resolution Office.
Sec. 1102. Modifications to notification on the provision of defense sensitive support.
Sec. 1103. Modification of congressional oversight of special access programs.
Sec. 1104. Funding limitations relating to unidentified anomalous phenomena.
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 2024 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 Act.

(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) D ISTRIBUTION 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) L IMITS 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 2024 the sum of $658,950,000.
(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 2024 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 Act 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 2024.
TITLE III—INTELLIGENCE
COMMUNITY MATTERS
Subtitle A—General Intelligence
Community Matters

SEC. 301. POST-GRADUATE EMPLOYMENT OF DEPARTMENT
OF DEFENSE CYBER AND DIGITAL SERVICE
ACADEMY SCHOLARSHIP RECIPIENTS IN INTELLIGENCE COMMUNITY.

Section 1535(d) of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263) is amended by inserting “or of an element of the intelligence community (as that term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003))” after “missions of the Department”.

SEC. 302. PLAN TO RECRUIT, TRAIN, AND RETAIN PERSONNEL WITH EXPERIENCE IN FINANCIAL INTELLIGENCE AND EMERGING TECHNOLOGIES.

(a) 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 heads of human capital of the Central Intelligence Agency, the National Security Agency, and the Federal Bureau of Investigation, shall submit to the congressional intelligence committees a plan for the intelligence community to recruit, train, and
retain personnel who have skills and experience in financial intelligence and emerging technologies in order to improve analytic tradecraft.

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

(1) An assessment, including measurable benchmarks of progress, of current initiatives of the intelligence community to recruit, train, and retain personnel who have skills and experience in financial intelligence and emerging technologies.

(2) An assessment of whether personnel in the intelligence community who have such skills are currently well integrated into the analytical cadre of the relevant elements of the intelligence community that produce analyses with respect to financial intelligence and emerging technologies.

(3) An identification of challenges to hiring or compensation in the intelligence community that limit progress toward rapidly increasing the number of personnel with such skills, and an identification of hiring or other reforms to resolve such challenges.

(4) A determination of whether the National Intelligence University has the resources and expertise necessary to train existing personnel in financial intelligence and emerging technologies.
(5) A strategy, including measurable benchmarks of progress, to, by January 1, 2025, increase by 10 percent the analytical cadre of personnel with expertise and previous employment in financial intelligence and emerging technologies.

SEC. 303. POLICY AND PERFORMANCE FRAMEWORK FOR MOBILITY OF INTELLIGENCE COMMUNITY WORKFORCE.

(a) In General.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall develop and implement a policy and performance framework to ensure the timely and effective mobility of employees and contractors of the Federal Government who are transferring employment between elements of the intelligence community.

(b) Elements.—The policy and performance framework required by subsection (a) shall include processes with respect to the following:

(1) Human resources.

(2) Medical reviews.

(3) Determinations of suitability or eligibility for access to classified information in accordance with Executive Order 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for Government employment, fitness for contractor
employees, and eligibility for access to classified na-
tional security information).

SEC. 304. IN-STATE TUITION RATES FOR ACTIVE DUTY
MEMBERS OF THE INTELLIGENCE COMMU-
NITY.

(a) In general.—Section 135(d) of the Higher
Education Act of 1965 (20 U.S.C. 1015d(d)), as amended
by section 6206(a)(4) of the Foreign Service Families Act
of 2021 (Public Law 117–81), is further amended—
(1) in paragraph (1), by striking “or” after the
semicolon;
(2) in paragraph (2), by striking the period at
the end and inserting “; or”; and
(3) by adding at the end the following new
paragraph:
“(3) a member of the intelligence community
(as defined in section 3 of the National Security Act
of 1947 (50 U.S.C. 3003)) (other than a member of
the Armed Forces of the United States) who is on
active duty for a period of more than 30 days.”.

(b) Effective date.—The amendments made by
subsection (a) shall take effect at each public institution
of higher education in a State that receives assistance
under the Higher Education Act of 1965 (20 U.S.C. 1001
et seq.) for the first period of enrollment at such institution that begins after July 1, 2026.

SEC. 305. STANDARDS, CRITERIA, AND GUIDANCE FOR COUNTERINTELLIGENCE VULNERABILITY ASSESSMENTS AND SURVEYS.

Section 904(d)(7)(A) of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3383(d)(7)(A)) is amended to read as follows:

“(A) COUNTERINTELLIGENCE VULNERABILITY ASSESSMENTS AND SURVEYS.—To develop standards, criteria, and guidance for counterintelligence risk assessments and surveys of the vulnerability of the United States to intelligence threats, including with respect to critical infrastructure and critical technologies, in order to identify the areas, programs, and activities that require protection from such threats.”.

SEC. 306. IMPROVING ADMINISTRATION OF CERTAIN POST-EMPLOYMENT RESTRICTIONS FOR INTELLIGENCE COMMUNITY.

Section 304 of the National Security Act of 1947 (50 U.S.C. 3073a) is amended—

(1) in subsection (c)(1)—
(A) by striking “A former” and inserting the following:

“(A) IN GENERAL.—A former’’; and

(B) by adding at the end the following:

“(B) PRIOR DISCLOSURE TO DIRECTOR OF NATIONAL INTELLIGENCE.—

“(i) IN GENERAL.—In the case of a former employee who occupies a covered post-service position in violation of subsection (a), whether the former employee voluntarily notified the Director of National Intelligence of the intent of the former employee to occupy such covered post-service position before occupying such post-service position may be used in determining whether the violation was knowing and willful for purposes of subparagraph (A).

“(ii) PROCEDURES AND GUIDANCE.—The Director of National Intelligence may establish procedures and guidance relating to the submittal of notice for purposes of clause (i).’’; and

(2) in subsection (d)—
(A) in paragraph (1), by inserting “the restrictions under subsection (a) and” before “the report requirements”;

(B) in paragraph (2), by striking “ceases to occupy” and inserting “occupies”; and

(C) in paragraph (3)(B), by striking “before the person ceases to occupy a covered intelligence position” and inserting “when the person occupies a covered intelligence position”.

SEC. 307. MISSION OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER.

(a) In general.—Section 904 of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3383) is amended—

(1) by redesignating subsections (d) through (i) as subsections (e) through (j), respectively; and

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

“(d) MISSION.—The mission of the National Counterintelligence and Security Center shall include organizing and leading strategic planning for counterintelligence activities of the United States Government by integrating instruments of national power as needed to counter foreign intelligence activities.”.

(b) Conforming Amendments.—

(A) in subsection (e), as redesignated by subsection (a)(1), by striking “Subject to subsection (e)” both places it appears and inserting “Subject to subsection (f)”;

(B) in subsection (f), as so redesignated—

(i) in paragraph (1), by striking “subsection (d)(1)” and inserting “subsection (e)(1)”;

(ii) in paragraph (2), by striking “subsection (d)(2)” and inserting “subsection (e)(2)”.

SEC. 308. PROHIBITION RELATING TO TRANSPORT OF INDIVIDUALS DETAINED AT UNITED STATES NAVAL STATION, GUANTANAMO BAY, CUBA.

(a) Definition of Individual Detained at Guantanamo.—In this section, the term “individual detained at Guantanamo” has the meaning given that term in section 1034(f)(2) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 971; 10 U.S.C. 801 note).

(b) Prohibition on Chartering Private or Commercial Aircraft to Transport Individuals Detained at United States Naval Station, Guantanamo Bay, Cuba.—No head of an element of the intelligence community may charter any private or commercial aircraft to transport an individual who is or was an individual detained at Guantanamo.

SEC. 309. DEPARTMENT OF ENERGY REVIEW OF CERTAIN FOREIGN VISITORS AND ASSIGNEES TO NATIONAL LABORATORIES.

(a) Definitions.—In this section:

(1) Appropriate committees of Congress.—The term “appropriate committees of Congress” means—

(A) the Select Committee on Intelligence of the Senate;
(B) the Committee on Energy and Natural Resources of the Senate;

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

and

(D) the Committee on Energy and Commerce of the House of Representatives.

(2) DIRECTOR.—The term “Director” means the Director of the Office of Intelligence and Counterintelligence of the Department of Energy (or a designee).

(3) 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)).

(4) 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).

(5) SENSITIVE COUNTRY.—The term “sensitive country” means a country to which particular consideration is given for policy reasons during the Department of Energy internal review and approval process for visits by, and assignments of, foreign nationals to National Laboratories.
(6) **Sensitive country national.**—The term “sensitive country national” means a foreign national who was born in, is a citizen of, or is employed by a government, employer, institution, or organization of, a sensitive country.

(7) **Sensitive country visitor or assignee.**—

(A) **In general.**—The term “sensitive country visitor or assignee” means a visitor or assignee who is a sensitive country national.

(B) **Associated definitions.**—For purposes of this paragraph:

(i) **Assignee.**—The term “assignee” means an individual who is seeking approval from, or has been approved by, a National Laboratory to access the premises, information, or technology of the National Laboratory for a period of more than 30 consecutive calendar days.

(ii) **Visitor.**—The term “visitor” means an individual who is seeking approval from, or has been approved by, a National Laboratory to access the premises, information, or technology of the National Lab-
oratory for any period other than a period described in clause (i).

(b) RECOMMENDATIONS WITH RESPECT TO SENSITIVE COUNTRY VISITORS OR ASSIGNEES.—

(1) NOTIFICATION AND RECOMMENDATION REQUIREMENT.—On determination that a proposed sensitive country visitor or assignee poses a counterintelligence risk to a National Laboratory, the Director shall—

(A) notify the National Laboratory of the determination; and

(B) provide a recommendation to the National Laboratory on whether to grant or deny the proposed sensitive country visitor or assignee access to the premises, information, or technology of the National Laboratory.

(2) PROHIBITION.—A National Laboratory may not allow a sensitive country visitor or assignee that the Director has identified as a counterintelligence risk under paragraph (1) to have any access to the premises, information, or technology of the National Laboratory until the Director has submitted the notification and recommendation to the National Laboratory as described in paragraph (1).
(3) **APPLICATION TO OTHER NATIONAL LABORATORIES.**—If the Director makes a recommendation under paragraph (1) that a sensitive country visitor or assignee should not be granted access to the premises, information, or technology of a National Laboratory—

(A) the Director shall notify each National Laboratory of that recommendation; and

(B) that recommendation shall apply to each National Laboratory with respect to that sensitive country visitor or assignee.

(c) **NOTIFICATION TO DIRECTOR.**—

(1) **IN GENERAL.**—After receiving a recommendation to deny access under subsection (b)(1)(B), a National Laboratory shall submit to the Director a notification of the decision of the National Laboratory to grant or deny access to the premises, information, or technology of the National Laboratory to the sensitive country visitor or assignee that is the subject of the recommendation.

(2) **TIMING.**—If a National Laboratory decides to grant access to a sensitive country visitor or assignee despite a recommendation to deny access, the notification under paragraph (1) shall be submitted to the Director before the sensitive country visitor or
assignee is granted access to the premises, information, or technology of the National Laboratory.

(d) REPORTS TO CONGRESS.—

(1) IN GENERAL.—The Director shall submit to the appropriate committees of Congress an unclassified quarterly report listing each instance in which a National Laboratory indicates in a notification submitted under subsection (c)(1) that the National Laboratory has decided to grant a sensitive country visitor or assignee access to the premises, information, or technology of the National Laboratory.

(2) REQUIREMENT.—Each quarterly report under paragraph (1) shall include the recommendation of the Director under subsection (b)(1)(B) with respect to the applicable sensitive country visitor or assignee.

SEC. 310. CONGRESSIONAL OVERSIGHT OF INTELLIGENCE COMMUNITY RISK ASSESSMENTS.

(a) RISK ASSESSMENT DOCUMENTS AND MATERIALS.—Except as provided in subsection (b), whenever an element of the intelligence community conducts a risk assessment arising from the mishandling or improper disclosure of classified information, the Director of National Intelligence shall, not later than 30 days after the date of the commencement of such risk assessment—
(1) submit to the congressional intelligence committees copies of such documents and materials as are—

(A) within the jurisdiction of such committees; and

(B) subject to the risk assessment; and

(2) provide such committees a briefing on such documents, materials, and risk assessment.

(b) EXCEPTION.—If the Director determines, with respect to a risk assessment described in subsection (a), that the documents and other materials otherwise subject to paragraph (1) of such subsection (a) are of such a volume that submittal pursuant to such paragraph would be impracticable, the Director shall—

(1) in lieu of submitting copies of such documents and materials, submit a log of such documents and materials; and

(2) pursuant to a request by the Select Committee on Intelligence of the Senate or the Permanent Select Committee on Intelligence of the House of Representatives for a copy of a document or material included in such log, submit to such committee such copy.
SEC. 311. INSPECTOR GENERAL REVIEW OF DISSEMINATION BY FEDERAL BUREAU OF INVESTIGATION RICHMOND, VIRGINIA, FIELD OFFICE OF CERTAIN DOCUMENT.

(a) Review Required.—Not later than 120 days after the date of the enactment of this Act, the Inspector General of the Department of Justice shall conduct a review of the actions and events, including any underlying policy direction, that served as a basis for the January 23, 2023, dissemination by the field office of the Federal Bureau of Investigation located in Richmond, Virginia, of a document titled “Interest of Racially or Ethnically Motivated Violent Extremists in Radical-Traditionalist Catholic Ideology Almost Certainly Presents New Mitigation Opportunities.”

(b) Submittal to Congress.—The Inspector General of the Department of Justice shall submit to the congressional intelligence committees the findings of the Inspector General with respect to the review required by subsection (a).

SEC. 312. OFFICE OF INTELLIGENCE AND ANALYSIS.

Section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) is amended by adding at the end the following:

“(h) Prohibition.—
“(1) DEFINITION.—In this subsection, the term ‘United States person’ means a United States citizen, an alien known by the Office of Intelligence and Analysis to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by 1 or more foreign governments.

“(2) COLLECTION OF INFORMATION FROM UNITED STATES PERSONS.—

“(A) IN GENERAL.—Notwithstanding any other provision of law, the Office of Intelligence and Analysis may not engage in the collection of information or intelligence targeting any United States person except as provided in subparagraph (B).

“(B) EXCEPTION.—Subparagraph (A) shall not apply to any employee, officer, or contractor of the Office of Intelligence and Analysis who is responsible for collecting information from individuals working for a State, local, or Tribal territory government or a private employer.”.
Subtitle B—Central Intelligence Agency

SEC. 321. PROTECTION OF CENTRAL INTELLIGENCE AGENCY FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT.

The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.) is amended by inserting after section 15 the following new section:

"SEC. 15A. PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT.

“(a) DEFINITIONS.—In this section:

“(1) BUDGET.—The term ‘budget’, with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31, United States Code.

“(2) 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).

“(3) CONGRESSIONAL JUDICIARY COMMITTEES.—The term ‘congressional judiciary committees’ means—
“(A) the Committee on the Judiciary of the Senate; and

“(B) the Committee on the Judiciary of the House of Representatives.

“(4) CONGRESSIONAL TRANSPORTATION AND INFRASTRUCTURE COMMITTEES.—The term ‘congressional transportation and infrastructure committees’ means—

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

“(B) the Committee on Transportation and Infrastructure of the House of Representatives.

“(5) COVERED FACILITY OR ASSET.—The term ‘covered facility or asset’ means the headquarters compound of the Agency and the property controlled and occupied by the Federal Highway Administration located immediately adjacent to such compound (subject to a risk-based assessment as defined for purposes of this section), or any other installation and protected property of the Agency where the facility or asset—

“(A) is identified as high risk and a potential target for unlawful unmanned aircraft activity by the Director, in coordination with the
Secretary of Transportation, with respect to potentially affected airspace, through a risk-based assessment for purposes of this section;

“(B) is located in the United States; and

“(C) directly relates to one or more functions authorized to be performed by the Agency, pursuant to the National Security Act of 1947 (50 U.S.C. 3001 et seq.) or this Act.

“(6) ELECTRONIC COMMUNICATION.—The term ‘electronic communication’ has the meaning given such term in section 2510 of title 18, United States Code.

“(7) INTERCEPT.—The term ‘intercept’ has the meaning given such term in section 2510 of title 18, United States Code.

“(8) RADIO COMMUNICATION.—The term ‘radio communication’ has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

“(9) RISK-BASED ASSESSMENT.—The term ‘risk-based assessment’ includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential effects on the safety and efficiency of the national airspace system and the needs of national security at each covered
facility or asset identified by the Director, an evaluation of each of the following factors:

“(A) Potential effects on safety, efficiency, and use of the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services relating to the use of any system or technology for carrying out the actions described in subsection (c)(1).

“(B) Options for mitigating any identified effects on the national airspace system relating to the use of any system or technology, including minimizing when possible the use of any system or technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

“(C) Potential consequences of any actions taken under subsection (c)(1) to the national airspace system and infrastructure, if not mitigated.

“(D) The ability to provide reasonable advance notice to aircraft operators consistent
with the safety of the national airspace system
and the needs of national security.

“(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, and any potential for interference with wireless communications or for injury or damage to persons or property.

“(F) Potential consequences to national security if threats posed by unmanned aircraft systems or unmanned aircraft are not mitigated or defeated.

“(10) Oral communication.—The term ‘oral communication’ has the meaning given such term in section 2510 of title 18, United States Code.

“(11) United States.—The term ‘United States’ has the meaning given such term in section 5 of title 18, United States Code.

“(12) Unmanned aircraft and unmanned aircraft system.—The terms ‘unmanned aircraft’ and ‘unmanned aircraft system’ have the meanings given such terms in section 44801 of title 49, United States Code.
“(13) Wire communication.—The term ‘wire communication’ has the meaning given such term in section 2510 of title 18, United States Code.

“(b) Authority.—Notwithstanding section 46502 of title 49, United States Code, section 32, 1030, or 1367 of title 18, United States Code, or chapter 119 or 206 of such title, the Director may take, and may authorize personnel of the Agency with assigned duties that include the security or protection of people, facilities, or assets within the United States, to take—

“(1) such actions described in subsection (c)(1) that are necessary to detect, identify, monitor, track, or mitigate a credible threat (as defined by the Director, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset; and

“(2) such actions described in subsection (c)(2).

“(c) Actions.—

“(1) Actions described.—The actions described in this paragraph are the following:

“(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, in-
cluding by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

“(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by doing so passively or actively, and by direct or indirect physical, electronic, radio, and electromagnetic means.

“(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering with, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

“(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

“(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

“(F) Use reasonable force, if necessary, to seize or otherwise disable, damage, or destroy
the unmanned aircraft system or unmanned aircraft.

“(2) RESEARCH, TESTING, TRAINING, AND EVALUATION.—The Director shall conduct research, testing, and training on, and evaluation of, any equipment, including any electronic equipment, to determine the capability and utility of the equipment prior to the use of the equipment for any action described in paragraph (1). Personnel and contractors who do not have duties that include the safety, security, or protection of people, facilities, or assets may engage in research, testing, training, and evaluation activities pursuant to this section.

“(3) COORDINATION.—

“(A) SECRETARY OF TRANSPORTATION.—

The Director shall develop the actions described in paragraph (1) in coordination with the Secretary of Transportation.

“(B) ADMINISTRATOR OF FEDERAL AVIATION ADMINISTRATION.—The Director shall coordinate with the Administrator of the Federal Aviation Administration on any action described in paragraphs (1) and (3) so the Administrator may ensure that unmanned aircraft system detection and mitigation systems do not adversely
affect or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

“(d) FORFEITURE.—Any unmanned aircraft system or unmanned aircraft described in subsection (b) that is seized by the Director is subject to forfeiture to the United States.

“(e) REGULATIONS AND GUIDANCE.—

“(1) ISSUANCE.—The Director and the Secretary of Transportation may each prescribe regulations, and shall each issue guidance, to carry out this section.

“(2) COORDINATION.—

“(A) REQUIREMENT.—The Director shall coordinate the development of guidance under paragraph (1) with the Secretary of Transportation.

“(B) AVIATION SAFETY.—The Director shall coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section, so the Administrator may ensure that unmanned aircraft system detection and mitiga-
tion systems do not adversely affect or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

“(f) PRIVACY PROTECTION.—The regulations prescribed or guidance issued under subsection (e) shall ensure that—

“(1) the interception or acquisition of, access to, or maintenance or use of, communications to or from an unmanned aircraft system or unmanned aircraft under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law;

“(2) communications to or from an unmanned aircraft system or unmanned aircraft are intercepted or acquired only to the extent necessary to support an action described in subsection (c);

“(3) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Director determines that maintenance of such records for a longer period is required under Federal law or necessary for the investigation or prosecution of a violation of
law, to fulfill a duty, responsibility, or function of
the Agency, or for the purpose of any litigation;

“(4) such communications are not disclosed
outside the Agency unless the disclosure—

“(A) is necessary to investigate or pros-
cecute a violation of law;

“(B) would support the Agency, the De-
partment of Defense, a Federal law enforce-
ment, intelligence, or security agency, or a
State, local, tribal, or territorial law enforce-
ment agency, or other relevant person or entity
if such entity or person is engaged in a security
or protection operation;

“(C) is necessary to support a department
or agency listed in subparagraph (B) in inves-
tigating or prosecuting a violation of law;

“(D) would support the enforcement activi-
ties of a regulatory agency of the Federal Gov-
ernment in connection with a criminal or civil
investigation of, or any regulatory, statutory, or
other enforcement action relating to, an action
described in subsection (c) that is necessary to
fulfill a duty, responsibility, or function of the
Agency;
“(E) is necessary to protect against danger- 
gerous or unauthorized activity by unmanned 
aircraft systems or unmanned aircraft;

“(F) is necessary to fulfill a duty, respon-
sibility, or function of the Agency; or

“(G) is otherwise required by law.

“(g) Budget.—

“(1) In General.—The Director shall submit 
to the congressional intelligence committees, as a 
part of the budget requests of the Agency for each 
fiscal year after fiscal year 2024, a consolidated 
funding display that identifies the funding source for 
the actions described in subsection (c)(1) within the 
Agency.

“(2) Form.—The funding display shall be in 
unclassified form, but may contain a classified 
annex.

“(h) Semiannual Briefings and Notifications.—

“(1) Briefings.—Not later than 180 days 
after the date of the enactment of this section, and 
semiannually thereafter, the Director shall provide 
the congressional intelligence committees, the con- 
gressional judiciary committees, and the congress-
ional transportation and infrastructure committees
a briefing on the activities carried out pursuant to this section during the period covered by the briefing.

“(2) REQUIREMENT.—Each briefing under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

“(3) CONTENTS.—Each briefing under paragraph (1) shall include the following:

“(A) Policies, programs, and procedures to mitigate or eliminate effects of such activities on the national airspace system and other critical national transportation infrastructure.

“(B) A description of instances in which actions described in subsection (c)(1) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property.

“(C) A description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues implicated by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights, or civil liberties.
“(D) A description of options considered and steps taken to mitigate any identified effects on the national airspace system relating to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

“(E) A description of instances in which communications intercepted or acquired during the course of operations of an unmanned aircraft system or unmanned aircraft were maintained for more than 180 days or disclosed outside the Agency.

“(F) How the Director and the Secretary of Transportation have informed the public as to the possible use of authorities under this section.

“(G) How the Director and the Secretary of Transportation have engaged with Federal, State, local, territorial, or tribal law enforcement agencies to implement and use such authorities.

“(H) An assessment of whether any gaps or insufficiencies remain in laws, regulations,
and policies that impede the ability of the Agency to counter the threat posed by the malicious use of unmanned aircraft systems or unmanned aircraft, and any recommendations to remedy such gaps or insufficiencies.

“(4) FORM.—Each briefing under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified report.

“(5) NOTIFICATIONS.—

“(A) COVERED FACILITIES AND ASSETS.—

Not later than 30 days before exercising any authority under this section at a covered facility or asset for the first time doing so at such covered facility or asset, the Director shall submit to the congressional intelligence committees—

“(i) notice that the Director intends to exercise authority under this section at such covered facility or asset; and

“(ii) a list of every covered facility and asset.

“(B) DEPLOYMENT OF NEW TECHNOLOGIES.—

“(i) IN GENERAL.—Not later than 30 days after deploying any new technology to carry out the actions described in sub-
section (c)(1), the Director shall submit to the congressional intelligence committees a notification of the use of such technology.

“(ii) CONTENTS.—Each notice submitted pursuant to clause (i) shall include a description of options considered to mitigate any identified effects on the national airspace system relating to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

“(i) RULE OF CONSTRUCTION.—Nothing in this section may be construed—

“(1) to vest in the Director any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration; or

“(2) to vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Director.

“(j) SCOPE OF AUTHORITY.—Nothing in this section shall be construed to provide the Director or the Secretary of Transportation with additional authorities beyond those described in subsections (b) and (d).
“(k) TERMINATION.—

“(1) IN GENERAL.—The authority to carry out this section with respect to the actions specified in subparagraphs (B) through (F) of subsection (c)(1) shall terminate on the date that is 10 years after the date of enactment of the Intelligence Authorization Act for Fiscal Year 2024.

“(2) EXTENSION.—The President may extend by 1 year the termination date specified in paragraph (1) if, before termination, the President certifies to Congress that such extension is in the national security interests of the United States.”.

SEC. 322. CHANGE TO PENALTIES AND INCREASED AVAILABILITY OF MENTAL HEALTH TREATMENT FOR UNLAWFUL CONDUCT ON CENTRAL INTELLIGENCE AGENCY INSTALLATIONS.

Section 15(b) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3515(b)) is amended, in the second sentence, by striking “those specified in section 1315(c)(2) of title 40, United States Code” and inserting “the maximum penalty authorized for a Class B misdemeanor under section 3559 of title 18, United States Code”.

S 2103 RS
SEC. 323. MODIFICATIONS TO PROCUREMENT AUTHORITIES OF THE CENTRAL INTELLIGENCE AGENCY.

Section 3 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3503) is amended—

(1) in subsection (a), by striking “sections” and all that follows through “session)” and inserting “sections 3201, 3203, 3204, 3206, 3207, 3302 through 3306, 3321 through 3323, 3801 through 3808, 3069, 3134, 3841, and 4752 of title 10, United States Code” and

(2) in subsection (d), by striking “in paragraphs” and all that follows through “1947” and inserting “in sections 3201 through 3204 of title 10, United States Code, shall not be delegable. Each determination or decision required by sections 3201 through 3204, 3321 through 3323, and 3841 of title 10, United States Code”.

SEC. 324. ESTABLISHMENT OF CENTRAL INTELLIGENCE AGENCY STANDARD WORKPLACE SEXUAL MISCONDUCT COMPLAINT INVESTIGATION PROCEDURE.

(a) WORKPLACE SEXUAL MISCONDUCT DEFINED.—

The term “workplace sexual misconduct”—
(1) means unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature when—

(A) submission to such conduct is made either explicitly or implicitly a term or condition of an individual’s employment;

(B) submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual; or

(C) such conduct has the purpose or effect of unreasonably interfering with an individual’s work performance or creating an intimidating, hostile, or offensive working environment; and

(2) includes sexual harassment and sexual assault.

(b) Standard Complaint Investigation Procedure.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall—

(1) establish a standard workplace sexual misconduct complaint investigation procedure;

(2) implement the standard workplace sexual misconduct complaint investigation procedure
through clear workforce communication and edu-
cation on the procedure; and

(3) submit the standard workplace sexual mis-
conduct complaint investigation procedure to the
congressional intelligence committees.

(c) MINIMUM REQUIREMENTS.—The procedure es-
tablished pursuant to subsection (b)(1) shall, at a min-
imum—

(1) identify the individuals and offices of the
Central Intelligence Agency to which an employee of
the Agency may bring a complaint of workplace sex-
ual misconduct;

(2) detail the steps each individual or office
identified pursuant to paragraph (1) shall take upon
receipt of a complaint of workplace sexual mis-
conduct and the timeframes within which those steps
shall be taken, including—

(A) documentation of the complaint;

(B) referral or notification to another indi-
vidual or office;

(C) measures to document or preserve wit-
ness statements or other evidence; and

(D) preliminary investigation of the com-
plaint;
(3) set forth standard criteria for determining whether a complaint of workplace sexual misconduct will be referred to law enforcement and the timeframe within which such a referral shall occur; and 

(4) for any complaint not referred to law enforcement, set forth standard criteria for determining—

(A) whether a complaint has been substantiated; and

(B) for any substantiated complaint, the appropriate disciplinary action.

(d) Annual Reports.—On or before April 30 of each year, the Director shall submit to the congressional intelligence committees an annual report that includes, for the preceding calendar year, the following:

(1) The number of workplace sexual misconduct complaints brought to each individual or office of the Central Intelligence Agency identified pursuant to subsection (c)(1), disaggregated by—

(A) complaints referred to law enforcement; and

(B) complaints substantiated.

(2) For each complaint described in paragraph (1) that is substantiated, a description of the disciplinary action taken by the Director.
SEC. 325. PAY CAP FOR DIVERSITY, EQUITY, AND INCLUSION STAFF AND CONTRACT EMPLOYEES OF THE CENTRAL INTELLIGENCE AGENCY.

(a) IN GENERAL.—Notwithstanding any other provision of law—

(1) the annual rate of basic pay for a staff employee of the Central Intelligence Agency with the duties described in subsection (b) shall not exceed the annual rate of basic pay for an officer of the Directorate of Operations in the Clandestine Service Trainee program of the Agency; and

(2) the Director of the Central Intelligence Agency shall ensure that no contract employee performing duties described in subsection (b) under an Agency contract receives an annual amount for performing such duties that exceeds the annual rate of basic pay described in paragraph (1).

(b) DUTIES DESCRIBED.—The duties described in this subsection are as follows:

(1) Developing, refining, and implementing diversity, equity, and inclusion policy.

(2) Leading working groups and councils to develop diversity, equity, and inclusion goals and objectives to measure performance and outcomes.
(3) Creating and implementing diversity, equity, and inclusion education, training courses, and workshops for staff and contract employees.

(c) ApPLICABILITY TO CURRENT EMPLOYEES.—

(1) Staff Employees.—Any staff employee of the Central Intelligence Agency in a position with duties described in subsection (b) receiving an annual rate of basic pay as of the date of the enactment of this Act that exceeds the rate allowed under subsection (a) shall be reassigned to another position not later than 180 days after such date.

(2) Contract Employees.—Any contract employee of the Central Intelligence Agency performing duties described in subsection (b) receiving an annual amount under an Agency contract for performing such duties as of the date of the enactment of this Act that exceeds the rate allowed under subsection (b) shall be reassigned to another position not later than 180 days after such date.
TITLE IV—MATTERS CONCERNING FOREIGN COUNTRIES

Subtitle A—People’s Republic of China

SEC. 401. INTELLIGENCE COMMUNITY COORDINATOR FOR ACCOUNTABILITY OF ATROCITIES OF THE PEOPLE’S REPUBLIC OF CHINA.

(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 and the Subcommittee on Defense of the Committee on Appropriations of the Senate; and

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

(2) ATROCITY.—The term “atrocity”—

(A) means a crime against humanity, genocide, or a war crime; and
(B) when used with respect to the People’s Republic of China, means an atrocity that is committed by an individual who is—

(i) a member of People’s Liberation Army, or the security or other defense services, including the Ministry of State Security, the Ministry of Public Security, and the United Front Work Department, of the People’s Republic of China;

(ii) an employee of any other element of the Government of the People’s Republic of China, including the regional governments of Xinjiang, Tibet, and Hong Kong;

(iii) a member of the Chinese Communist Party; or

(iv) an agent or contractor of an individual specified in subparagraph (A), (B), or (C).

(3) COMMIT.—The term “commit”, with respect to an atrocity, includes the planning, committing, aiding, and abetting of such atrocity.

(4) FOREIGN PERSON.—The term “foreign person” means—

(A) any person or entity that is not a United States person; or
(B) any entity not organized under the laws of the United States or of any jurisdiction within the United States.

(5) UNITED STATES PERSON.—The term “United States person” has the meaning given that term in section 105A(c) of the National Security Act of 1947 (50 U.S.C. 3039).

(b) INTELLIGENCE COMMUNITY COORDINATOR FOR ACCOUNTABILITY OF ATROCITIES OF THE PEOPLE’S REPUBLIC OF CHINA.—

(1) DESIGNATION.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall designate a senior official of the Office of the Director of National Intelligence to serve as the intelligence community coordinator for accountability of atrocities of the People’s Republic of China (in this section referred to as the “Coordinator”).

(2) DUTIES.—The Coordinator shall lead the efforts of and coordinate and collaborate with the intelligence community with respect to the following:

(A) Identifying and addressing any gaps in intelligence collection relating to atrocities of the People’s Republic of China, including by recommending the modification of the priorities
of the intelligence community with respect to intelligence collection and by utilizing informal processes and collaborative mechanisms with key elements of the intelligence community to increase collection on atrocities of the People’s Republic of China.

(B) Prioritizing and expanding the intelligence analysis with respect to ongoing atrocities of the People’s Republic of China and disseminating within the United States Government intelligence relating to the identification and activities of foreign persons suspected of being involved with or providing support to atrocities of the People’s Republic of China, including genocide and forced labor practices in Xinjiang, in order to support the efforts of other Federal agencies, including the Department of State, the Department of the Treasury, the Office of Foreign Assets Control, the Department of Commerce, the Bureau of Industry and Security, U.S. Customs and Border Protection, and the National Security Council, to hold the People’s Republic of China accountable for such atrocities.
(C) Increasing efforts to declassify and share with the people of the United States and the international community information regarding atrocities of the People’s Republic of China in order to expose such atrocities and counter the disinformation and misinformation campaign by the People’s Republic of China to deny such atrocities.

(D) Documenting and storing intelligence and other unclassified information that may be relevant to preserve as evidence of atrocities of the People’s Republic of China for future accountability, and ensuring that other relevant Federal agencies, including the Atrocities Early Warning Task Force, receive appropriate support from the intelligence community with respect to the collection, analysis, preservation, and, as appropriate, dissemination, of intelligence related to atrocities of the People’s Republic of China, which may include the information from the annual report required by section 6504 of the Intelligence Authorization Act for Fiscal Year 2023 (Public Law 117–263).

(E) Sharing information with the Forced Labor Enforcement Task Force, established
under section 741 of the United States-Mexico-
Canada Agreement Implementation Act (19
U.S.C. 4681), the Department of Commerce,
and the Department of the Treasury for the
purposes of entity listings and sanctions.

(3) PLAN REQUIRED.—Not later than 120 days
after the date of the enactment of this Act, the Di-
rector shall submit to the appropriate committees of
Congress—

(A) the name of the official designated as
the Coordinator pursuant to paragraph (1); and

(B) the strategy of the intelligence commu-
nity for the collection and dissemination of in-
telligence relating to ongoing atrocities of the
People’s Republic of China, including a detailed
description of how the Coordinator shall sup-
port, and assist in facilitating the implementa-
tion of, such strategy.

(4) ANNUAL REPORT TO CONGRESS.—

(A) REPORTS REQUIRED.—Not later than
May 1, 2024, and annually thereafter until May
1, 2034, the Director shall submit to the appro-
priate committees of Congress a report detail-
ing, for the year covered by the report—
(i) the analytical findings, changes in collection, and other activities of the intelligence community with respect to ongoing atrocities of the People’s Republic of China;

(ii) the recipients of information shared pursuant to this section for the purpose of—

(I) providing support to Federal agencies to hold the People’s Republic of China accountable for such atrocities; and

(II) sharing information with the people of the United States to counter the disinformation and misinformation campaign by the People’s Republic of China to deny such atrocities; and

(iii) with respect to clause (ii), the date of any such sharing.

(B) FORM.—Each report submitted under subparagraph (A) may be submitted in classified form, consistent with the protection of intelligence sources and methods.
(c) **SUNSET.**—This section shall cease to have effect on the date that is 10 years after the date of the enactment of this Act.

**SEC. 402. INTERAGENCY WORKING GROUP AND REPORT ON THE MALIGN EFFORTS OF THE PEOPLE'S REPUBLIC OF CHINA IN AFRICA.**

(a) **ESTABLISHMENT.**—

(1) **IN GENERAL.**—The Director of National Intelligence, in consultation with such heads of elements of the intelligence community as the Director considers appropriate, shall establish an interagency working group within the intelligence community to analyze the tactics and capabilities of the People’s Republic of China in Africa.

(2) **ESTABLISHMENT FLEXIBILITY.**—The working group established under paragraph (1) may be—

(A) independently established; or

(B) to avoid redundancy, incorporated into existing working groups or cross-intelligence efforts within the intelligence community.

(b) **REPORT.**—

(1) **IN GENERAL.**—Not later than 120 days after the date of the enactment of this Act, and twice annually thereafter, the working group established under subsection (a) shall submit to the con-
gressional intelligence committees a report on the specific tactics and capabilities of the People’s Rep-
public of China in Africa.

(2) ELEMENTS.—Each report required by para-
graph (1) shall include the following elements:

(A) An assessment of efforts by the Gov-
ernment of the People’s Republic of China to exploit mining and reprocessing operations in Africa.

(B) An assessment of efforts by the Gov-
ernment of the People’s Republic of China to provide or fund technologies in Africa, includ-
ing—

   (i) telecommunications and energy technologies, such as advanced reactors, transportation, and other commercial prod-
   ucts; and

   (ii) by requiring that the People’s Re-
   public of China be the sole provider of such technologies.

(C) An assessment of efforts by the Gov-
ernment of the People’s Republic of China to expand intelligence capabilities in Africa.

(D) A description of actions taken by the intelligence community to counter such efforts.
(E) An assessment of additional resources needed by the intelligence community to better counter such efforts.

(3) FORM.—Each report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex if necessary.

(e) SUNSET.—The requirements of this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

SEC. 403. AMENDMENT TO REQUIREMENT FOR ANNUAL ASSESSMENT BY INTELLIGENCE COMMUNITY WORKING GROUP FOR MONITORING THE ECONOMIC AND TECHNOLOGICAL CAPABILITIES OF THE PEOPLE’S REPUBLIC OF CHINA.

Section 6503(c)(3)(D) of the Intelligence Authorization Act for Fiscal Year 2023 (division F of Public Law 117–263) is amended by striking “the top 200” and inserting “all the known”.

SEC. 404. ASSESSMENTS OF RECIPROCITY IN THE RELATIONSHIP BETWEEN THE UNITED STATES AND THE PEOPLE’S REPUBLIC OF CHINA.

(a) In General.—Not later than 1 year after the date of the enactment of this Act, the Assistant Secretary of State for Intelligence and Research, in consultation with the Director of National Intelligence and such other
heads of elements of the intelligence community as the Assistant Secretary considers relevant, shall submit to the congressional intelligence committees the following:

(1) A comprehensive assessment that identifies critical areas in the security, diplomatic, economic, financial, technological, scientific, commercial, academic, and cultural spheres in which the United States does not enjoy a reciprocal relationship with the People’s Republic of China.

(2) A comprehensive assessment that describes how the lack of reciprocity between the People’s Republic of China and the United States in the areas identified in the assessment required by paragraph (1) provides advantages to the People’s Republic of China.

(b) FORM OF ASSESSMENTS.—

(1) CRITICAL AREAS.—The assessment required by subsection (a)(1) shall be submitted in unclassified form.

(2) ADVANTAGES.—The assessment required by subsection (a)(2) shall be submitted in classified form.
SEC. 405. ANNUAL BRIEFING ON INTELLIGENCE COMMUNITY EFFORTS TO IDENTIFY AND MITIGATE CHINESE COMMUNIST PARTY POLITICAL INFLUENCE OPERATIONS AND INFORMATION WARFARE AGAINST THE UNITED STATES.

(a) DEFINITIONS.—In this section:

(1) Chinese entities engaged in political influence operations and information warfare.—The term “Chinese entities engaged in political influence operations and information warfare” means all of the elements of the Government of the People's Republic of China and the Chinese Communist Party involved in information warfare operations, such as—

(A) the Ministry of State Security;
(B) the intelligence services of the People’s Republic of China;
(C) the United Front Work Department and other united front organs;
(D) state-controlled media systems, such as the China Global Television Network (CGTN); and
(E) any entity involved in information warfare operations by demonstrably and intentionally disseminating false information and propaganda of the Government of the People’s
Republic of China or the Chinese Communist Party.

(2) Political influence operation.—The term “political influence operation” means a coordinated and often concealed application of disinformation, press manipulation, economic coercion, targeted investments, corruption, or academic censorship, which are often intended—

(A) to coerce and corrupt United States interests, values, institutions, or individuals; and

(B) to foster attitudes, behavior, decisions, or outcomes in the United States that support the interests of the Government of the People’s Republic of China or the Chinese Communist Party.

(b) Briefing Required.—Not later than 120 days after the date of the enactment of this Act and annually thereafter until the date that is 5 years after the date of the enactment of this Act, the Director of the Foreign Malign Influence Center shall, in collaboration with the heads of the elements of the intelligence community, provide the congressional intelligence committees a classified briefing on the ways in which the relevant elements of the intelligence community are working internally and coordinating across the intelligence community to identify and
mitigate the actions of Chinese entities engaged in political influence operations and information warfare against the United States, including against United States persons.

(c) ELEMENTS.—The classified briefing required by subsection (b) shall cover the following:

(1) The Government of the People’s Republic of China and the Chinese Communist Party tactics, tools, and entities that spread disinformation, misinformation, and malign information and conduct influence operations, information campaigns, or other propaganda efforts.

(2) The actions of the Foreign Malign Influence Center relating to early-warning, information sharing, and proactive risk mitigation systems, based on the list of entities identified in subsection (a)(1), to detect, expose, deter, and counter political influence operations of, and information warfare waged by, the Government of the People’s Republic of China or the Chinese Communist Party, against the United States.

(3) The actions of the Foreign Malign Influence Center to conduct outreach to identify and counter tactics, tools, and entities described in paragraph (1) by sharing information with allies and partners of the United States, State and local governments, the
business community, and civil society that exposes the political influence operations and information operations of the Government of the People’s Republic of China or the Chinese Communist Party carried out against individuals and entities in the United States.

SEC. 406. ASSESSMENT OF THREAT POSED TO UNITED STATES PORTS BY CRANES MANUFACTURED BY COUNTRIES OF CONCERN.

(a) Definition of Country of Concern.—In this section, the term “country of concern” has the meaning given that term in section 1(m)(1) of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a(m)(1)).

(b) Assessment.—The Director of National Intelligence, in coordination with such other heads of the elements of the intelligence community as the Director considers appropriate and the Secretary of Defense, shall conduct an assessment of the threat posed to United States ports by cranes manufactured by countries of concern and commercial entities of those countries, including the Shanghai Zhenhua Heavy Industries Co. (ZPMC).

(c) Report and Briefing.—

(1) In general.—Not later than 180 days after the date of the enactment of this Act, the Di-
rector of National Intelligence shall submit a report
and provide a briefing to Congress on the findings
of the assessment required by subsection (b).

(2) ELEMENTS.—The report and briefing re-
quired by paragraph (1) shall outline the potential
for the cranes described in subsection (b) to collect
intelligence, disrupt operations at United States
ports, and impact the national security of the United
States.

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

Subtitle B—Russian Federation

SEC. 411. ASSESSMENT OF LESSONS LEARNED BY INTEL-
LIGENCE COMMUNITY WITH RESPECT TO
CONFLICT IN UKRAINE.

(a) IN GENERAL.—Not later than 180 days after the
date of the enactment of this Act and semiannually there-
after for 3 years, the Director of National Intelligence
shall produce and submit to the congressional intelligence
committees an assessment of the lessons learned by the
intelligence community with respect to the ongoing war
in Ukraine, particularly in regards to the quality and time-
liness of the information and intelligence support provided
by the United States to Ukraine.
(b) Form.—The assessment submitted pursuant to subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 412. NATIONAL INTELLIGENCE ESTIMATE ON LONG-TERM CONFRONTATION WITH RUSSIA.

(a) National Intelligence Estimate Required.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall produce and submit to the congressional intelligence committees a national intelligence estimate on the implications of the ongoing war in Ukraine with respect to a long-term United States and North Atlantic Treaty Organization confrontation with Russia, including the continued threat to the United States, the North Atlantic Treaty Organization, and other allies of the United States from the conventional and strategic military forces, the intelligence activities, and the malign influence campaigns of Russia.

(b) Elements.—The national intelligence estimate produced pursuant to subsection (a) shall include the following:

(1) An assessment of the efficacy of the sanctions regime in effect on the day before the date of the enactment of this Act that is imposed upon Rus-
sia as a result of its illegal and unjustified invasion
of Ukraine, including—

(A) the effect that such sanctions have had
on the economy of Russia, the defense indus-
trial base of Russia, and the ability of Russia
to maintain its war on Ukraine; and

(B) the expected effect such sanctions
would have on a potential long-term confronta-
tion between Russia and the members of the
North Atlantic Treaty Organization and other
allies of the United States.

(2) An updated assessment of the convergence
of interests between Russia and China, an assess-
ment of the assistance that China is providing to
Russia’s economy and war effort, and an assessment
of other collaboration between the two countries.

(3) An assessment of potential friction points
between China and Russia.

(4) An assessment of assistance and potential
assistance from other countries to Russia, including
assistance from Iran and North Korea.

(5) An assessment of other significant countries
that have not joined the sanctions regime against
Russia, why they have not done so, and what might
induce them to change this policy.
(c) Form.—The national intelligence estimate submitted pursuant to subsection (a) shall be submitted in unclassified form, but may include a classified annex.

Subtitle C—Other Foreign Countries

SEC. 421. REPORT ON EFFORTS TO CAPTURE AND DETAIN UNITED STATES CITIZENS AS HOSTAGES.

(a) In General.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on efforts by the Maduro regime in Venezuela to detain United States citizens and lawful permanent residents.

(b) Elements.—The report required by subsection (a) shall include, regarding the arrest, capture, detention, or imprisonment of United States citizens and lawful permanent residents, the following:

(1) The names, positions, and institutional affiliation of Venezuelan individuals, or those acting on their behalf, who have engaged in such activities.

(2) A description of any role played by transnational criminal organizations, and an identification of such organizations.
(3) Where relevant, an assessment of whether and how United States citizens and lawful permanent residents have been lured to Venezuela.

(4) An analysis of the motive for the arrest, capture, detention, or imprisonment of United States citizens and lawful permanent residents.

(5) The total number of United States citizens and lawful permanent residents detained or imprisoned in Venezuela as of the date on which the report is submitted.

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

SEC. 422. SENSE OF CONGRESS ON PRIORITY OF FENTANYL IN NATIONAL INTELLIGENCE PRIORITIES FRAMEWORK.

It is the sense of Congress that the trafficking of illicit fentanyl, including precursor chemicals and manufacturing equipment associated with illicit fentanyl production and organizations that traffic or finance the trafficking of illicit fentanyl, originating from the People’s Republic of China and Mexico should be among the highest priorities in the National Intelligence Priorities Framework of the Office of the Director of National Intelligence.
TITLE V—MATTERS PERTAINING TO UNITED STATES ECONOMIC AND EMERGING TECHNOLOGY COMPETITION WITH UNITED STATES ADVERSARIES

Subtitle A—General Matters

SEC. 501. OFFICE OF GLOBAL COMPETITION ANALYSIS.

(a) DEFINITIONS.—In this section:

(1) EXECUTIVE AGENCY.—The term “Executive agency” has the meaning given such term in section 105 of title 5, United States Code.

(2) OFFICE.—The term “Office” means the Office of Global Competition Analysis established under subsection (b).

(b) ESTABLISHMENT.—

(1) IN GENERAL.—The President shall establish an office for analysis of global competition.

(2) PURPOSES.—The purposes of the Office are as follows:

(A) To carry out a program of analysis relevant to United States leadership in science, technology, and innovation sectors critical to national security and economic prosperity relative to other countries, particularly those coun-
tries that are strategic competitors of the United States.

(B) To support policy development and decision making across the Federal Government to ensure United States leadership in science, technology, and innovation sectors critical to national security and economic prosperity relative to other countries, particularly those countries that are strategic competitors of the United States.

(3) DESIGNATION.—The office established under paragraph (1) shall be known as the “Office of Global Competition Analysis”.

(c) ACTIVITIES.—In accordance with the priorities determined under subsection (d), the Office shall—

(1) subject to subsection (f), acquire, access, use, and handle data or other information relating to the purposes of the Office under subsection (b);

(2) conduct long- and short-term analyses regarding—

(A) United States policies that enable technological competitiveness relative to those of other countries, particularly with respect to countries that are strategic competitors of the United States;
(B) United States science and technology ecosystem elements, including regional and national research development and capacity, technology innovation, and science and engineering education and research workforce, relative to those of other countries, particularly with respect to countries that are strategic competitors of the United States;

(C) United States technology development, commercialization, and advanced manufacturing ecosystem elements, including supply chain resiliency, scale-up manufacturing testbeds, access to venture capital and financing, technical and entrepreneurial workforce, and production, relative to those of other countries, particularly with respect to countries that are strategic competitors of the United States;

(D) United States competitiveness in technology and innovation sectors critical to national security and economic prosperity relative to other countries, including the availability and scalability of United States technology in such sectors abroad, particularly with respect to countries that are strategic competitors of the United States;
(E) trends and trajectories, including rate of change in technologies, related to technology and innovation sectors critical to national security and economic prosperity;

(F) threats to United States national security interests as a result of any foreign country’s dependence on technologies of strategic competitors of the United States; and

(G) threats to United States interests based on dependencies on foreign technologies critical to national security and economic prosperity;

(3) solicit input on technology and economic trends, data, and metrics from relevant private sector stakeholders, including entities involved in financing technology development and commercialization, and engage with academia to inform the analyses under paragraph (2); and

(4) to the greatest extent practicable and as may be appropriate, ensure that versions of the analyses under paragraph (2) are unclassified and available to relevant Federal agencies and offices.

(d) DETERMINATION OF PRIORITIES.—On a periodic basis, the Director of the Office of Science and Technology Policy, the Assistant to the President for Economic Policy,
and the Assistant to the President for National Security Affairs shall, in coordination with such heads of Executive agencies as the Director of the Office of Science and Technology Policy and such Assistants jointly consider appropriate, jointly determine the priorities of the Office with respect to subsection (b)(2)(A), considering, as may be appropriate, the strategies and reports under subtitle B of title VI of the Research and Development, Competition, and Innovation Act (Public Law 117–167).

(c) Administration.—Subject to the availability of appropriations, to carry out the purposes set forth under subsection (b)(2), the Office shall enter into an agreement with a federally funded research and development center, a university-affiliated research center, or a consortium of federally funded research and development centers and university-affiliated research centers.

(f) Acquisition, Access, Use, and Handling of Data or Information.—In carrying out the activities under subsection (c), the Office—

(1) shall acquire, access, use, and handle data or information in a manner consistent with applicable provisions of law and policy, including laws and policies providing for the protection of privacy and civil liberties, and subject to any restrictions required by the source of the information;
(2) shall have access, upon written request, to all information, data, or reports of any Executive agency that the Office determines necessary to carry out the activities under subsection (c), provided that such access is—

(A) conducted in a manner consistent with applicable provisions of law and policy of the originating agency, including laws and policies providing for the protection of privacy and civil liberties; and

(B) consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters; and

(3) may obtain commercially available information that may not be publicly available.

(g) DETAILEE SUPPORT.—Consistent with applicable law, including sections 1341, 1517, and 1535 of title 31, United States Code, and section 112 of title 3, United States Code, the head of a department or agency within the executive branch of the Federal Government may detail personnel to the Office in order to assist the Office in carrying out any activity under subsection (c), consistent with the priorities determined under subsection (d).
(h) **ANNUAL REPORT.**—Not less frequently than once each year, the Office shall submit to Congress a report on the activities of the Office under this section, including a description of the priorities under subsection (d) and any support, disaggregated by Executive agency, provided to the Office consistent with subsection (g) in order to advance those priorities.

(i) **PLANS.**—Before establishing the Office under subsection (b)(1), the President shall submit to the appropriate committees of Congress a report detailing plans for—

1. the administrative structure of the Office, including—
   - (A) a detailed spending plan that includes administrative costs; and
   - (B) a disaggregation of costs associated with carrying out subsection (e);
2. ensuring consistent and sufficient funding for the Office; and
3. coordination between the Office and relevant Executive agencies and offices.

(j) **AUTHORIZATION OF APPROPRIATIONS.**—There is authorized to be appropriated to carry out this section $20,000,000 for fiscal year 2024.
(k) **FUNDING.**—This section shall be carried out using amounts appropriated on or after the date of the enactment of this Act.

**SEC. 502. ASSIGNMENT OF DETAILEES FROM INTELLIGENCE COMMUNITY TO DEPARTMENT OF COMMERCE.**

(a) **AUTHORITY.**—In order to better facilitate the sharing of actionable intelligence on foreign adversary intent, capabilities, threats, and operations that pose a threat to the interests or security of the United States, particularly as they relate to the procurement, development, and use of dual-use and emerging technologies, the Director of National Intelligence may assign or facilitate the assignment of members from across the intelligence community to serve as detailees to the Bureau of Industry and Security of the Department of Commerce.

(b) **ASSIGNMENT.**—Detailees assigned pursuant to subsection (a) shall be drawn from such elements of the intelligence community as the Director considers appropriate, in consultation with the Secretary of Commerce.

(c) **EXPERTISE.**—The Director shall ensure that detailees assigned pursuant to subsection (a) have subject matter expertise on countries of concern, including China, Iran, North Korea, and Russia, as well as functional areas such as illicit procurement, counterproliferation, emerging
and foundational technology, economic and financial intelligence, information and communications technology systems, supply chain vulnerability, and counterintelligence.

(d) DUTY CREDIT.—The detail of an employee of the intelligence community to the Department of Commerce under subsection (a) shall be without interruption or loss of civil service status or privilege.

SEC. 503. THREATS POSED BY INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES TRANSACTIONS AND OTHER ACTIVITIES.

(a) DEFINITIONS.—In this section:

(1) COVERED TRANSACTION.—The term “covered transaction” means a transaction reviewed under authority established under Executive Order 13873, Executive Order 13984, Executive Order 14034, or any successor order.

(2) EMERGING AND FOUNDATIONAL TECHNOLOGIES.—The term “emerging and foundational technologies” means emerging and foundational technologies described in section 1758(a)(1) of the Export Control Reform Act of 2018 (50 U.S.C. 4817(a)(1)).

(3) EXECUTIVE ORDER 13873.—The term “Executive Order 13873” means Executive Order 13873 (84 Fed. Reg. 22689; relating to securing informa-
tion and communications technology and services
supply chain).

(4) EXECUTIVE ORDER 13984.—The term “Ex-
ecutive Order 13984” means Executive Order 13984
(86 Fed. Reg. 6837; relating to taking additional
steps to address the national emergency with respect
to significant malicious cyber-enabled activities).

(5) EXECUTIVE ORDER 14034.—The term “Ex-
eecutive Order 14034” means Executive Order 14034
(84 Fed. Reg. 31423; relating to protecting Ameri-
cans’ sensitive data from foreign adversaries).

(6) SIGNIFICANT TRANSACTION.—The term
“significant transaction” means a covered trans-
caction that—

(A) involves emerging or foundational tech-
nologies;

(B) poses an undue or unacceptable risk to
national security; and

(C) involves—

(i) an individual who acts as an agent,
representative, or employee, or any indi-
vidual who acts in any other capacity at
the order, request, or under the direction
or control, of a foreign adversary or of an
individual whose activities are directly or
indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;

(ii) any individual, wherever located, who is a citizen or resident of a nation-state controlled by a foreign adversary;

(iii) any corporation, partnership, association, or other organization organized under the laws of a nation-state controlled by a foreign adversary; or

(iv) any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary.

(b) THREAT ASSESSMENT BY DIRECTOR OF NATIONAL INTELLIGENCE.—

(1) IN GENERAL.—The Director of National Intelligence shall expeditiously carry out a threat assessment of each significant transaction.

(2) IDENTIFICATION OF GAPS.—Each assessment required by paragraph (1) shall include the identification of any recognized gaps in the collection of intelligence relevant to the assessment.

(3) VIEWS OF INTELLIGENCE COMMUNITY.—

The Director of National Intelligence shall seek and
incorporate into each assessment required by paragraph (1) the views of all affected or appropriate elements of the intelligence community with respect to the significant transaction or class of significant transactions.

(4) Provision of Assessment.—The Director of National Intelligence shall provide an assessment required by paragraph (1) to such agency heads and committees of Congress as the Director considers appropriate, as necessary, to implement Executive Order 13873, Executive Order 13984, Executive Order 14034, or any successor order.

(c) Interaction With Intelligence Community.—

(1) In General.—The Director of National Intelligence shall ensure that the intelligence community remains engaged in the collection, analysis, and dissemination to such agency heads as the Director considers appropriate of any additional relevant information that may become available during the course of any investigation or review process conducted under authority established under Executive Order 13873, Executive Order 13984, Executive Order 14034, or any successor order.
(2) ELEMENTS.—The collection, analysis, and dissemination of information described in paragraph (1) shall include routine assessments of the following:

(A) The intent, capability, and operations of foreign adversaries as related to a significant transaction or class of significant transactions.

(B) Supply chains and procurement networks associated with the procurement of emerging and foundational technologies by foreign adversaries.

(C) Emerging and foundational technologies pursued by foreign adversaries, including information on prioritization, spending, and technology transfer measures.

(D) The intent, capability, and operations of the use by malicious cyber actors of infrastructure as a service (IaaS) against the United States.

(E) The impact on the intelligence community of a significant transaction or class of significant transactions.

(d) INFORMATION IN CIVIL ACTIONS.—

(1) PROTECTED INFORMATION IN CIVIL ACTIONS.—If a civil action challenging an action or
finding under Executive Order 13873, Executive Order 13984, Executive Order 14034, or any successor order is brought, and the court determines that protected information in the administrative record relating to the action or finding, including classified or other information subject to privilege or protections under any provision of law, is necessary to resolve the action, that information shall be submitted ex parte and in camera to the court and the court shall maintain that information under seal. This paragraph does not confer or imply any right to judicial review.

(2) Nonapplicability of Use of Information Provisions.—The use of information provisions of sections 106, 305, 405, and 706 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806, 1825, 1845, and 1881e) shall not apply in a civil action described in paragraph (1).

(c) Rule of Construction Concerning Right to Access.—No provision of this section may be construed to create a right to obtain access to information in the possession of the Federal Government that was considered by the Secretary of Commerce under authority established under Executive Order 13873, Executive Order 13984, Executive Order 14034, or any successor order, including
any classified information or sensitive but unclassified information.

(f) Administrative Record.—The following information may be included in the administrative record relating to an action or finding described in subsection (d)(1) and shall be submitted only to the court ex parte and in camera:

(1) Sensitive security information, as defined in section 1520.5 of title 49, Code of Federal Regulations.

(2) Privileged law enforcement information.

(3) Information obtained or derived from any activity authorized under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), except that, with respect to such information, subsections (c), (e), (f), (g), and (h) of section 106 (50 U.S.C. 1806), subsections (d), (f), (g), (h), and (i) of section 305 (50 U.S.C. 1825), subsections (e), (e), (f), (g), and (h) of section 405 (50 U.S.C. 1845), and section 706 (50 U.S.C. 1881e) of that Act shall not apply.

(4) Information subject to privilege or protection under any other provision of law, including the Currency and Foreign Transactions Reporting Act of 1970 (31 U.S.C. 5311 et seq.).
(g) Treatment Consistent With Section.—Any information that is part of the administrative record filed ex parte and in camera under subsection (d)(1), or cited by the court in any decision in a civil action described in such subsection, shall be treated by the court consistent with the provisions of this section. In no event shall such information be released to the petitioner or as part of the public record.

(h) Inapplicability of Freedom of Information Act.—Any information submitted to the Federal Government by a party to a covered transaction in accordance with this section, as well as any information the Federal Government may create relating to review of the covered transaction, is exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the “Freedom of Information Act”).

SEC. 504. REVISION OF REGULATIONS DEFINING SENSITIVE NATIONAL SECURITY PROPERTY FOR COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES REVIEWS.

Not later than 180 days after the date of the enactment of this Act, the Secretary of the Treasury shall revise section 802.211 of title 31, Code of Federal Regulations, to expand the definition of “covered real estate”, such as by treating facilities and property of elements of the intel-
Intelligence community and National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)) comparably to military installations.

SEC. 505. SUPPORT OF INTELLIGENCE COMMUNITY FOR EXPORT CONTROLS AND OTHER MISSIONS OF THE DEPARTMENT OF COMMERCE.

(a) Definitions.—In this section:

(1) Emerging and foundational technologies.—The term “emerging and foundational technologies” includes technologies identified under section 1758(a)(1) of the Export Control Reform Act of 2018 (50 U.S.C. 4817(a)(1)).

(2) Foreign adversary.—The term “foreign adversary” means any foreign government, foreign regime, or foreign nongovernment person determined by the Director of National Intelligence to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of United States persons.

(b) Collection, Analysis, and Dissemination Required.—

(1) In general.—The Director of National Intelligence—
(A) is authorized to collect, retain, analyze, and disseminate information or intelligence necessary to support the missions of the Department of Commerce, including with respect to the administration of export controls pursuant to the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.); and

(B) shall, through regular consultation with the Secretary of Commerce, ensure that the intelligence community is engaged in such collection, retention, analysis, and dissemination.

(2) INFORMATION TO BE COLLECTED, ANALYZED, AND DISSEMINATED.—The information to be collected, analyzed, and disseminated under subsection (a) shall include information relating to the following:

(A) The intent, capability, and operations of foreign adversaries with respect to items under consideration to be controlled pursuant to the authority provided by part I of the Export Control Reform Act of 2018 (50 U.S.C. 4811 et seq.).
(B) Attempts by foreign adversaries to circumvent controls on items imposed pursuant to that part.

(C) Supply chains and procurement networks associated with procurement and development of emerging and foundational technologies by foreign adversaries.

(D) Emerging and foundational technologies pursued by foreign adversaries, including relevant information on prioritization, spending, and technology transfer measures with respect to such technologies.

(E) The scope and application of the export control systems of foreign countries, including decisions with respect to individual export transactions.

(F) Corporate and contractual relationships, ownership, and other equity interests, including monetary capital contributions, corporate investments, and joint ventures, resulting in end uses of items that threaten the national security and foreign policy interests of the United States, as described in the policy set forth in section 1752 of the Export Control Reform Act of 2018 (50 U.S.C. 4811).
(G) The effect of export controls imposed pursuant to part I of that Act (50 U.S.C. 4811 et seq.), including—

(i) the effect of actions taken and planned to be taken by the Secretary of Commerce under the authority provided by that part; and

(ii) the effectiveness of such actions in achieving the national security and foreign policy objectives of such actions.

(c) Provision of Analysis to Department of Commerce.—Upon the request of the Secretary of Commerce, the Director of National Intelligence shall expeditiously—

(1) carry out analysis of any matter relating to the national security of the United States that is relevant to a mission of the Department of Commerce; and

(2) consistent with the protection of sources and methods, make such analysis available to the Secretary and such individuals as the Secretary may designate to receive such analysis.

(d) Identification of Single Office to Support Missions of Department of Commerce.—The Director of National Intelligence shall identify a single of-
fice within the intelligence community to be responsible
for supporting the missions of the Department of Com-
merce.

(e) TREATMENT OF CLASSIFIED AND SENSITIVE IN-
FORMATION.—

(1) IN GENERAL.—A civil action challenging an
action or finding of the Secretary of Commerce
made on the basis of any classified or sensitive infor-
mination made available to officials of the Department
of Commerce pursuant to this section may be
brought only in the United States Court of Appeals
for the District of Columbia Circuit.

(2) CONSIDERATION AND TREATMENT IN CIVIL
ACTIONS.—If a civil action described in paragraph
(1) is brought, and the court determines that pro-
tected information in the administrative record, in-
cluding classified or other information subject to
privilege or protections under any provision of law,
is necessary to resolve the civil action, that informa-
tion shall be submitted ex parte and in camera to
the court and the court shall maintain that informa-
tion under seal. This paragraph does not confer or
imply any right to judicial review.

(3) ADMINISTRATIVE RECORD.—
(A) IN GENERAL.—The following information may be included in the administrative record relating to an action or finding described in paragraph (1) and shall be submitted only to the court ex parte and in camera:

(i) Sensitive security information, as defined by section 1520.5 of title 49, Code of Federal Regulations.

(ii) Privileged law enforcement information.

(iii) Information obtained or derived from any activity authorized under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(iv) Information subject to privilege or protection under any other provision of law.

(B) TREATMENT CONSISTENT WITH SECTION.—Any information that is part of the administrative record filed ex parte and in camera under subparagraph (A), or cited by the court in any decision in a civil action described in paragraph (1), shall be treated by the court consistent with the provisions of this subsection.
In no event shall such information be released to the petitioner or as part of the public record.

(4) **Nonapplicability of Use of Information Provisions.**—The use of information provisions of sections 106, 305, 405, and 706 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806, 1825, 1845, and 1881e) shall not apply in a civil action challenging an action or finding of the Secretary of Commerce made on the basis of information made available to officials of the Department of Commerce pursuant to this section.

(5) **Rule of Construction Concerning Right to Access.**—No provision of this section shall be construed to create a right to obtain access to information in the possession of the Federal Government that was considered in an action or finding of the Secretary of Commerce, including any classified information or sensitive but unclassified information.

(6) **Exemption from Freedom of Information Act.**—Any information made available to officials of the Department of Commerce pursuant to this section is exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the “Freedom of Information Act”).
SEC. 506. REVIEW REGARDING INFORMATION COLLECTION AND ANALYSIS WITH RESPECT TO ECONOMIC COMPETITION.

(a) Review.—

(1) In general.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall complete a review of the requirements and access to commercial information used by elements of the intelligence community for analysis of capital flows, investment security, beneficial ownership of entities, and other transactions and functions related to identifying threats, gaps, and opportunities with respect to economic competition with foreign countries, including the People's Republic of China.

(2) Elements.—The review required by paragraph (1) shall include the following:

(A) The length and expiration of licenses for access to commercial information.

(B) The number of such licenses permitted for each element of the intelligence community.

(C) The number of such licenses permitted for Federal departments and agencies that are not elements of the intelligence community, including the Department of Commerce.

(b) Report; Briefing.—
(1) IN GENERAL.—Not later than 60 days after
the date on which the review required by subsection
(a)(1) is completed, the Director of National Intel-
ligence shall submit a report and provide a briefing
to Congress on the findings of the review.

(2) ELEMENTS.—The report and briefing re-
quired by paragraph (1) shall include the following:

(A) The findings of the review required by
subsection (a)(1).

(B) Recommendations of the Director on
whether and how the standardization of access
to commercial information, the expansion of li-
censes for such access, the lengthening of li-
cense terms beyond 1 year, and the issuance of
Government-wide (as opposed to agency-by-
agency) licenses would advance the open-source
collection and analytical requirements of the in-
telligence community with respect to economic
competition with foreign countries, including
the People’s Republic of China.

(C) An assessment of cost savings or in-
creases that may result from the standardiza-
tion described in subparagraph (B).

(3) FORM.—The report and briefing required
by paragraph (1) may be classified.
Subtitle B—Next-generation Energy, Biotechnology, and Artificial Intelligence

SEC. 511. EXPANDED ANNUAL ASSESSMENT OF ECONOMIC AND TECHNOLOGICAL CAPABILITIES OF THE PEOPLE’S REPUBLIC OF CHINA.

Section 6503(c)(3) of the Intelligence Authorization Act for Fiscal Year 2023 (Public Law 117–263) is amended by adding at the end the following:

“(I) A detailed assessment, prepared in consultation with all elements of the working group—

“(i) of the investments made by the People’s Republic of China in—

“(I) artificial intelligence;

“(II) next-generation energy technologies, especially small modular reactors and advanced batteries; and

“(III) biotechnology; and

“(ii) that identifies—

“(I) competitive practices of the People’s Republic of China relating to the technologies described in clause (i);
“(II) opportunities to counter the practices described in subclause (I);

“(III) countries the People’s Republic of China is targeting for exports of civil nuclear technology;

“(IV) countries best positioned to utilize civil nuclear technologies from the United States in order to facilitate the commercial export of those technologies;

“(V) United States vulnerabilities in the supply chain of these technologies; and

“(VI) opportunities to counter the export by the People’s Republic of China of civil nuclear technologies globally.

“(J) An identification and assessment of any unmet resource or authority needs of the working group that affect the ability of the working group to carry out this section.”.

**SEC. 512. PROCUREMENT OF PUBLIC UTILITY CONTRACTS.**

Subparagraph (B) of section 501(b)(1) of title 40, United States Code, is amended to read as follows:

“(B) Public utility contracts.—
“(i) IN GENERAL.—A contract for public utility services may be made—

“(I) except as provided in subclause (II), for a period of not more than 10 years; or

“(II) for an executive agency that is, or has a component that is, an element of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), for a period of not more than 30 years, if the executive agency determines the extended period is in the best interests of national security.

“(ii) PAYMENT.—The cost of a public utility services contract for any year may be paid from annual appropriations for that year.”.

SEC. 513. ASSESSMENT OF USING CIVIL NUCLEAR ENERGY FOR INTELLIGENCE COMMUNITY CAPABILITIES.

(a) ASSESSMENT REQUIRED.—The Director of National Intelligence shall, in consultation with the heads of such other elements of the intelligence community as the
Director considers appropriate, conduct an assessment of
capabilities identified by the Intelligence Community Con-
tinuity Program established pursuant to section E(3) of
Intelligence Community Directive 118, or any successor
directive, or such other facilities or capabilities as may be
determined by the Director to be critical to United States
national security, that have unique energy needs—

1. to ascertain the feasibility and advisability
   of using civil nuclear reactors to meet such needs;
   and

2. to identify such additional resources, tech-
   nologies, infrastructure, or authorities needed, or
   other potential obstacles, to commence use of a nu-
   clear reactor to meet such needs.

(b) REPORT.—Not later than 180 days after the date
of the enactment of this Act, the Director shall submit
to the congressional intelligence committees a report,
which may be in classified form, on the findings of the
Director with respect to the assessment conducted pursu-
ant to subsection (a).
(a) In general.—Section 6702 of the Intelligence Authorization Act for Fiscal Year 2023 (50 U.S.C. 3334m) is amended—

(1) in subsection (a), in the matter preceding paragraph (1), by striking “subsection (b)” and inserting “subsection (c)”;

(2) by redesignating subsection (b) as subsection (c); and

(3) by inserting after subsection (a) the following:

“(b) Policies.—

“(1) In general.—In carrying out subsection (a)(1), not later than 1 year after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2024, the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community, shall establish the policies described in paragraph (2).

“(2) Policies described.—The policies described in this paragraph are policies for the acquisition, adoption, development, use, coordination, and maintenance of artificial intelligence capabilities that—
“(A) establish a lexicon relating to the use of machine learning and artificial intelligence developed or acquired by elements of the intelligence community;

“(B) establish guidelines for evaluating the performance of models developed or acquired by elements of the intelligence community, such as—

“(i) specifying conditions for the continuous monitoring of artificial intelligence capabilities for performance, including the conditions for retraining or retiring models based on performance;

“(ii) documenting performance objectives, including specifying how performance objectives shall be developed and contractually enforced for capabilities procured from third parties;

“(iii) specifying the manner in which models should be audited, as necessary, including the types of documentation that should be provided to any auditor; and

“(iv) specifying conditions under which models used by elements of the intelligence community should be subject to
testing and evaluation for vulnerabilities to
techniques meant to undermine the avail-
ability, integrity, or privacy of an artificial
intelligence capability;

“(C) establish guidelines for tracking de-
dendencies in adjacent systems, capabilities, or
processes impacted by the retraining or
sunsetting of any model described in subpara-
graph (B);

“(D) establish documentation requirements
for capabilities procured from third parties,
aligning such requirements, as necessary, with
existing documentation requirements applicable
to capabilities developed by elements of the in-
telligence community and, to the greatest extent
possible, with industry standards;

“(E) establish standards for the docu-
mentation of imputed, augmented, or synthetic
data used to train any model developed, proc-
cured, or used by an element of the intelligence
community; and

“(F) provide guidance on the acquisition
and usage of models that have previously been
trained by a third party for subsequent modi-
fication and usage by such an element.
“(3) POLICY REVIEW AND REVISION.—The Director of National Intelligence shall periodically review and revise each policy established under paragraph (1).”.

(b) CONFORMING AMENDMENT.—Section 6712(b)(1) of such Act (50 U.S.C. 3024 note) is amended by striking “section 6702(b)” and inserting “section 6702(c)”.

SEC. 515. STRATEGY FOR SUBMITTAL OF NOTICE BY PRIVATE PERSONS TO FEDERAL AGENCIES REGARDING CERTAIN RISKS AND THREATS RELATING TO ARTIFICIAL INTELLIGENCE.

(a) FINDINGS.—Congress finds the following:

(1) Artificial intelligence systems demonstrate increased capabilities in the generation of synthetic media and computer programming code, and in areas such as object recognition, natural language processing, biological design, 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 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 misuse or malfunction of these systems, such as to generate synthetic media for disinformation campaigns, develop or refine malware for computer network exploitation activity, design or develop dual-use biological entities such as toxic small molecules, proteins, or pathogenic organisms, enhance surveillance capabilities in ways that undermine the privacy of citizens of the United States, and increase the risk of exploitation or malfunction of information technology systems incorporating artificial intelligence systems in mission-critical fields such as health care, critical infrastructure, and transportation.

(b) STRATEGY REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the President shall establish a strategy by which 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—

(1) information security risks emanating from artificial intelligence systems, such as the use of an
artificial intelligence system to develop or refine ma-
licious software;

(2) information security risks such as indica-
tions of compromise or other threat information in-
dicating a compromise to the confidentiality, integ-
rity, or availability of an artificial intelligence sys-
tem, or to the supply chain of an artificial intel-
ligence system, including training or test data,
frameworks, computing environments, or other com-
ponents necessary for the training, management, or
maintenance of an artificial intelligence system;

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

(4) suspected foreign malign influence (as de-
dined 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;
and

(5) any other unlawful activity facilitated by, or
directed at, an artificial intelligence system.

(c) ELEMENTS.—The strategy established pursuant
to subsection (b) shall include the following:
(1) An outline of a plan for Federal agencies to engage in industry outreach and public education on the risks posed by, and directed at, artificial intelligence systems.

(2) Use of research and development, stakeholder outreach, and risk management frameworks established pursuant to provisions of law in effect on the day before the date of the enactment of this Act or Federal agency guidelines.

**TITLE VI—WHISTLEBLOWER MATTERS**

**SEC. 601. SUBMITTAL TO CONGRESS OF COMPLAINTS AND INFORMATION BY WHISTLEBLOWERS IN THE INTELLIGENCE COMMUNITY.**

(a) Amendments to Chapter 4 of Title 5.—

(1) Appointment of security officers.—

Section 416 of title 5, United States Code, is amended by adding at the end the following:

“(i) Appointment of Security Officers.—Each Inspector General under this section, including the designees of the Inspector General of the Department of Defense pursuant to subsection (b)(3), shall appoint within their offices security officers to provide, on a permanent basis, confidential, security-related guidance and direction to an employee of their respective establishment, an em-
ployee assigned or detailed to such establishment, or an employee of a contractor of such establishment who intends to report to Congress a complaint or information, so that such employee can obtain direction on how to report to Congress in accordance with appropriate security practices.”.

(2) PROCEDURES.—Subsection (e) of such section is amended—

(A) in paragraph (1), by inserting “or any other committee of jurisdiction of the Senate or the House of Representatives” after “either or both of the intelligence committees”;

(B) by amending paragraph (2) to read as follows:

“(2) LIMITATION.—

“(A) IN GENERAL.—Except as provided in subparagraph (B), the employee may contact an intelligence committee or another committee of jurisdiction directly as described in paragraph (1) of this subsection or in subsection (b)(4) only if the employee—

“(i) before making such a contact, furnishes to the head of the establishment, through the Inspector General (or designee), a statement of the employee’s com-
plaint or information and notice of the employee’s intent to contact an intelligence committee or another committee of jurisdiction of the Senate or the House of Representatives directly; and

“(ii)(I) obtains and follows, from the head of the establishment, through the Inspector General (or designee), procedural direction on how to contact an intelligence committee or another committee of jurisdiction of the Senate or the House of Representatives in accordance with appropriate security practices; or

“(II) obtains and follows such procedural direction from the applicable security officer appointed under subsection (i).

“(B) LACK OF PROCEDURAL DIRECTION.—If an employee seeks procedural direction under subparagraph (A)(ii) and does not receive such procedural direction within 30 days, or receives insufficient direction to report to Congress a complaint or information, the employee may contact an intelligence committee or any other committee of jurisdiction of the Senate or the House of Representatives directly without ob-
taining or following the procedural direction otherwise required under such subparagraph.”; and

(C) by redesigning paragraph (3) as paragraph (4); and

(D) by inserting after paragraph (2) the following:

“(3) COMMITTEE MEMBERS AND STAFF.—An employee of an element of the intelligence community who intends to report to Congress a complaint or information may report such complaint or information to the Chairman and Vice Chairman or Ranking Member, as the case may be, of an intelligence committee or another committee of jurisdiction of the Senate or the House of Representatives, a nonpartisan member of the committee staff designated for purposes of receiving complaints or information under this section, or a member of the majority staff and a member of the minority staff of the committee.”.

(3) CLARIFICATION OF RIGHT TO REPORT DIRECTLY TO CONGRESS.—Subsection (b) of such section is amended by adding at the end the following:

“(4) CLARIFICATION OF RIGHT TO REPORT DIRECTLY TO CONGRESS.—Subject to paragraphs (2)
and (3) of subsection (e), an employee of an element of the intelligence community who intends to report to Congress a complaint or information may report such complaint or information directly to Congress, regardless of whether the complaint or information is with respect to an urgent concern—

“(A) in lieu of reporting such complaint or information under paragraph (1); or

“(B) in addition to reporting such complaint or information under paragraph (1).”.

(b) Amendments to National Security Act of 1947.—

(1) Appointment of security officers.—Section 103H(j) of the National Security Act of 1947 (50 U.S.C. 3033(j)) is amended by adding at the end the following:

“(5) The Inspector General shall appoint within the Office of the Inspector General security officers as required by section 416(i) of title 5, United States Code.”.

(2) Procedures.—Subparagraph (D) of section 103H(k)(5) of such Act (50 U.S.C. 3033(k)(5)) is amended—

(A) in clause (i), by inserting “or any other committee of jurisdiction of the Senate or
the House of Representatives” after “either or
both of the congressional intelligence commit-
tees”;  
(B) by amending clause (ii) to read as fol-
ows:  
“(ii)(I) Except as provided in subclause (II), an
employee may contact a congressional intelligence
committee or another committee of jurisdiction di-
rectly as described in clause (i) only if the em-
ployee—

“(aa) before making such a contact, fur-
nishes to the Director, through the Inspector
General, a statement of the employee’s com-
plaint or information and notice of the employ-
ee’s intent to contact a congressional intel-
ligence committee or another committee of ju-
risdiction of the Senate or the House of Rep-
resentatives directly; and

“(bb)(AA) obtains and follows, from the
Director, through the Inspector General, proce-
dural direction on how to contact a congress-
sional intelligence committee or another com-
mittee of jurisdiction of the Senate or the
House of Representatives in accordance with
appropriate security practices; or
“(BB) obtains and follows such procedural direction from the applicable security officer appointed under section 416(i) of title 5, United States Code.

“(II) If an employee seeks procedural direction under subclause (I)(bb) and does not receive such procedural direction within 30 days, or receives insufficient direction to report to Congress a complaint or information, the employee may contact a congressional intelligence committee or any other committee of jurisdiction of the Senate or the House of Representatives directly without obtaining or following the procedural direction otherwise required under such subclause.”;

(C) by redesignating clause (iii) as clause (iv); and

(D) by inserting after clause (ii) the following:

“(iii) An employee of an element of the intelligence community who intends to report to Congress a complaint or information may report such complaint or information to the Chairman and Vice Chairman or Ranking Member, as the case may be, of a congressional intelligence committee or another
committee of jurisdiction of the Senate or the House of Representatives, a nonpartisan member of the committee staff designated for purposes of receiving complaints or information under this section, or a member of the majority staff and a member of the minority staff of the committee.”.

(3) Clarification of right to report directly to Congress.—Subparagraph (A) of such section is amended—

(A) by inserting “(i)” before “An employee of”; and

(B) by adding at the end the following:

“(ii) Subject to clauses (ii) and (iii) of subparagraph (D), an employee of an element of the intelligence community who intends to report to Congress a complaint or information may report such complaint or information directly to Congress, regardless of whether the complaint or information is with respect to an urgent concern—

“(I) in lieu of reporting such complaint or information under clause (i); or

“(II) in addition to reporting such complaint or information under clause (i).”.

(c) Amendments to the Central Intelligence Agency Act of 1949.—
(1) APPOINTMENT OF SECURITY OFFICERS.—
Section 17(d)(5) of the Central Intelligence Agency
Act of 1949 (50 U.S.C. 3517(d)(5)) is amended by
adding at the end the following:
“(I) The Inspector General shall appoint within the
Office of the Inspector General security officers as re-
quired by section 416(i) of title 5, United States Code.”.

(2) PROCEDURES.—Subparagraph (D) of such
section is amended—

(A) in clause (i), by inserting “or any
other committee of jurisdiction of the Senate or
the House of Representatives” after “either or
both of the intelligence committees”;

(B) by amending clause (ii) to read as fol-
lows:

“(ii)(I) Except as provided in subclause (II), an em-
ployee may contact an intelligence committee or another
committee of jurisdiction directly as described in clause
(i) only if the employee—

“(aa) before making such a contact, furnishes
to the Director, through the Inspector General, a
statement of the employee’s complaint or informa-
tion and notice of the employee’s intent to contact
an intelligence committee or another committee of
jurisdiction of the Senate or the House of Representatives directly; and

“(bb)(AA) obtains and follows, from the Director, through the Inspector General, procedural direction on how to contact an intelligence committee or another committee of jurisdiction of the Senate or the House of Representatives in accordance with appropriate security practices; or

“(BB) obtains and follows such procedural direction from the applicable security officer appointed under section 416(i) of title 5, United States Code.

“(II) If an employee seeks procedural direction under subclause (I)(bb) and does not receive such procedural direction within 30 days, or receives insufficient direction to report to Congress a complaint or information, the employee may contact an intelligence committee or another committee of jurisdiction of the Senate or the House of Representatives directly without obtaining or following the procedural direction otherwise required under such subclause.”;

(C) by redesignating clause (iii) as clause (iv); and

(D) by inserting after clause (ii) the following:
“(iii) An employee of the Agency who intends to report to Congress a complaint or information may report such complaint or information to the Chairman and Vice Chairman or Ranking Member, as the case may be, of an intelligence committee or another committee of jurisdiction of the Senate or the House of Representatives, a non-partisan member of the committee staff designated for purposes of receiving complaints or information under this section, or a member of the majority staff and a member of the minority staff of the committee.”.

(3) **Clarification of right to report directly to Congress.**—Subparagraph (A) of such section is amended—

(A) by inserting “(i)” before “An employee of”; and

(B) by adding at the end the following:

“(ii) Subject to clauses (ii) and (iii) of subparagraph (D), an employee of the Agency who intends to report to Congress a complaint or information may report such complaint or information directly to Congress, regardless of whether the complaint or information is with respect to an urgent concern—

“(I) in lieu of reporting such complaint or information under clause (i); or
“(II) in addition to reporting such complaint or
information under clause (i).”.

(d) **Rule of Construction.**—Nothing in this sec-
tion or an amendment made by this section shall be con-
strued to revoke or diminish any right of an individual
provided by section 2303 of title 5, United States Code.

**SEC. 602. PROHIBITION AGAINST DISCLOSURE OF WHIS-
TLEBLOWER IDENTITY AS REPRISAL
AGAINST WHISTLEBLOWER DISCLOSURE BY
EMPLOYEES AND CONTRACTORS IN INTEL-
LIGENCE COMMUNITY.**

(a) **In General.**—Section 1104 of the National Se-
curity Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subsection (a)(3) of such section—

(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) a knowing and willful disclosure re-
vealing the identity or other personally identifi-
able information of an employee or contractor
employee so as to identify the employee or con-
tractor employee as an employee or contractor
employee who has made a lawful disclosure de-
scribed in subsection (b) or (c); or”;

(2) by redesignating subsections (f) and (g) as
subsections (g) and (h), respectively; and

(3) by inserting after subsection (e) the fol-
lowing:

“(f) PERSONNEL ACTIONS INVOLVING DISCLOSURE
OF WHISTLEBLOWER IDENTITY.—A personnel action de-
scribed in subsection (a)(3)(J) shall not be considered to
be in violation of subsection (b) or (c) under the following
circumstances:

“(1) The personnel action was taken with the
express consent of the employee or contractor em-
ployee.

“(2) An Inspector General with oversight re-
sponsibility for a covered intelligence community ele-
ment determines that—

“(A) the personnel action was unavoidable
under section 103H(g)(3)(A) of this Act (50
U.S.C. 3033(g)(3)(A)), section 17(e)(3)(A) of
the Central Intelligence Agency Act of 1949 (50
U.S.C. 3517(e)(3)(A)), section 407(b) of title 5,
United States Code, or section 420(b)(2)(B) of
such title;
“(B) the personnel action was made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken; or

“(C) the personnel action was required by statute or an order from a court of competent jurisdiction.”.

(b) APPLICABILITY TO DETAILLEES.—Subsection (a) of section 1104 of such Act (50 U.S.C. 3234) is amended by adding at the end the following:

“(5) EMPLOYEE.—The term ‘employee’, with respect to an agency or a covered intelligence community element, includes an individual who has been detailed to such agency or covered intelligence community element.”.

(e) PRIVATE RIGHT OF ACTION FOR UNLAWFUL DISCLOSURE OF WHISTLEBLOWER IDENTITY.—Subsection (g) of such section, as redesignated by subsection (a)(2) of this section, is amended to read as follows:

“(g) 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.

“(3) Private right of action for disclosures of whistleblower identity in violation of prohibition against reprisals.—Subject to paragraph (4), in a case in which an employee of an agency takes a personnel action described in subsection (a)(3)(J) against an employee of a covered intelligence community element as a reprisal in violation of subsection (b) or in a case in which an employee or contractor employee takes a personnel action described in subsection (a)(3)(J) against another contractor employee as a reprisal in violation of subsection (c), the employee or contractor employee against whom the personnel action was taken may, consistent with section 1221 of title 5, United States Code, bring a private action for all appropriate remedies, including injunctive relief and compensatory and punitive damages, in an amount not to exceed $250,000, against the agency of the employee or contracting agency of the contractor em-
ployee who took the personnel action, in a Federal
district court of competent jurisdiction.

“(4) Requirements.—

“(A) Review by Inspector General

and by external review panel.—Before
the employee or contractor employee may bring
a private action under paragraph (3), the em-
ployee or contractor employee shall exhaust ad-
ministrative remedies by—

“(i) first, obtaining a disposition of
their claim by requesting review by the ap-
propriate inspector general; and

“(ii) second, if the review under clause
(i) does not substantiate reprisal, by sub-
mitting to the Inspector General of the In-
telligence Community a request for a re-
view of the claim by an external review
panel under section 1106.

“(B) Period to Bring Action.—The em-
ployee or contractor employee may bring a pri-
ivate right of action under paragraph (3) during
the 180-day period beginning on the date on
which the employee or contractor employee is
notified of the final disposition of their claim
under section 1106.”.
SEC. 603. 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. 604. 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.
SEC. 605. MODIFICATION AND REPEAL OF REPORTING REQUIREMENTS.


(b) Repeal of Requirement for Inspectors General Reviews of Enhanced Personnel Security Programs.—

(1) In general.—Section 11001 of title 5, United States Code, is amended—

(A) by striking subsection (d); and

(B) by redesignating subsection (e) as subsection (d).

(2) Technical corrections.—Subsection (d) of section 11001 of such title, as redesignated by paragraph (1)(B), is amended—

(A) in paragraph (3), by adding “and” after the semicolon at the end; and
(B) in paragraph (4), by striking “; and”

and inserting a period.

TITLE VII—CLASSIFICATION
REFORM
Subtitle A—Classification Reform
Act of 2023

CHAPTER 1—SHORT TITLE; DEFINITIONS

SEC. 701. SHORT TITLE.

This subtitle may be cited as the “Classification Re-
form Act of 2023”.

SEC. 702. DEFINITIONS.

Title VIII of the National Security Act of 1947 (50
U.S.C. 3161 et seq.) is amended—

(1) in the title heading by striking “ACCESS
TO CLASSIFIED INFORMATION PROCE-
DURES” and inserting “PROTECTION OF
NATIONAL SECURITY INFORMATION”;

(2) in the matter before section 801, by insert-
ing the following:

“Subtitle A—Definitions

“SEC. 800. DEFINITIONS.

“In this title:

“(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 Gov-
ernment that comes into the possession of classified
information.

“(2) AUTHORIZED INVESTIGATIVE AGENCY.—
The term ‘authorized investigative agency’ means an
agency authorized by law or regulation to conduct a
counterintelligence investigation or investigations of
persons who are proposed for access to classified in-
formation to ascertain whether such persons satisfy
the criteria for obtaining and retaining access to
such information.

“(3) Classify, classified, classification.—
The terms ‘classify’, ‘classified’, and ‘classification’
refer to the process by which information is deter-
mined to require protection from unauthorized dis-
closure pursuant to this title in order to protect the
national security of the United States.

“(4) Classified information.—The term
‘classified information’ means information that has
been classified.

“(5) Computer.—The term ‘computer’ means
any electronic, magnetic, optical, electrochemical, or
other high-speed data processing device performing
logical, arithmetic, or storage functions, and includes
any data storage facility or communications facility
directly related to or operating in conjunction with
such device and any data or other information
stored or contained in such device.

“(6) Consumer reporting agency.—The
term ‘consumer reporting agency’ has the meaning
given such term in section 603 of the Consumer

“(7) Declassify, declassified, declassification.—The terms ‘declassify’, ‘declassified’,
and ‘declassification’ refer to the process by which
information that has been classified is determined to
no longer require protection from unauthorized dis-
closure pursuant to this title.

“(8) Document.—The term ‘document’ means
any recorded information, regardless of the nature of
the medium or the method or circumstances of re-
cording.

“(9) Employee.—The term ‘employee’ includes
any person who receives a salary or compensation of
any kind from the United States Government, is a
contractor of the United States Government or an
employee thereof, is an unpaid consultant of the
United States Government, or otherwise acts for or
on behalf of the United States Government, except
as otherwise determined by the President.

“(10) **EXECUTIVE AGENT FOR CLASSIFICATION**
AND DECLASSIFICATION.—The term ‘Executive
Agent for Classification and Declassification’ means
the Executive Agent for Classification and Declas-
sification established by section 811(a).

“(11) **FINANCIAL AGENCY AND HOLDING COM-
PANY.**—The terms ‘financial agency’ and ‘financial
institution’ have the meanings given to such terms
in section 5312(a) of title 31, United States Code,
and the term ‘holding company’ has the meaning
given to such term in section 1101(6) of the Right

“(12) **FOREIGN POWER AND AGENT OF A FOR-
EIGN POWER.**—The terms ‘foreign power’ and ‘agent
of a foreign power’ have the meanings given such
terms in section 101 of the Foreign Intelligence Sur-

“(13) **INFORMATION.**—The term ‘information’
means any knowledge that can be communicated, or
documentary material, regardless of its physical
form or characteristics, that is owned by, is pro-
duced by or for, or is under the control of the
United States Government.

“(15) ORIGINAL CLASSIFICATION AUTHORITY.—The term ‘original classification authority’ means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

“(16) RECORDS.—The term ‘records’ means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency’s control under the terms of the contract, license, certificate, or grant.

“(17) STATE.—The term ‘State’ means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, the Republic of the Marshall Islands, the Federated States of Micronesia, and the Republic of
Palau, and any other possession of the United States.

“Subtitle B—Access to Classified Information Procedures”; and

(3) by striking section 805.

CHAPTER 2—GOVERNANCE AND ACCOUNTABILITY FOR REFORM OF THE SECURITY CLASSIFICATION SYSTEM

SEC. 711. EXECUTIVE AGENT FOR CLASSIFICATION AND DECLASSIFICATION.

Title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.), as amended by section 702, is further amended by adding at the end the following:

“Subtitle C—Security Classification Governance

“SEC. 811. EXECUTIVE AGENT FOR CLASSIFICATION AND DECLASSIFICATION.

“(a) Establishment.—There is in the executive branch of the Federal Government an Executive Agent for Classification and Declassification who shall be responsible for promoting programs, processes, and systems relating to classification and declassification, including developing technical solutions for automating declassification review and directing resources for such purposes in the Federal Government.
“(b) DESIGNATION.—The Director of National Intelligence shall serve as the Executive Agent for Classification and Declassification.

“(c) DUTIES.—The duties of the Executive Agent for Classification and Declassification are as follows:

“(1) To promote classification and declassification programs, processes, and systems with the goal of ensuring that declassification activities keep pace with classification activities and that classified information is declassified at such time as it no longer meets the standard for classification.

“(2) To promote classification and declassification programs, processes, and systems that ensure secure management of and tracking of classified records.

“(3) To promote the establishment of a federated classification and declassification system to streamline, modernize, and oversee declassification across agencies.

“(4) To direct resources to develop, coordinate, and implement a federated classification and declassification system that includes technologies that automate declassification review and promote consistency in declassification determinations across the executive branch of the Federal Government.
“(5) To work with the Director of the Office of Management and Budget in developing a line item for classification and declassification in each budget of the President that is submitted for a fiscal year under section 1105(a) of title 31, United States Code.

“(6) To identify and support the development of—

“(A) best practices for classification and declassification among agencies; and

“(B) goal-oriented classification and declassification pilot programs.

“(7) To promote and implement technological and automated solutions relating to classification and declassification, with human input as necessary for key policy decisions.

“(8) To promote feasible, sustainable, and interoperable programs and processes to facilitate a federated classification and declassification system.

“(9) To direct the implementation across agencies of the most effective programs and approaches relating to classification and declassification.

“(10) To establish, oversee, and enforce acquisition and contracting policies relating to classification and declassification programs.
“(11) In coordination with the Information Security Oversight Office—

“(A) to issue policies and directives to the heads of agencies relating to directing resources and making technological investments in classification and declassification that include support for a federated system;

“(B) to ensure implementation of the policies and directives issued under subparagraph (A);

“(C) to collect information on classification and declassification practices and policies across agencies, including training, accounting, challenges to effective declassification, and costs associated with classification and declassification;

“(D) to develop policies for ensuring the accuracy of information obtained from Federal agencies; and

“(E) to develop accurate and relevant metrics for judging the success of classification and declassification policies and directives.

“(12) To work with appropriate agencies to oversee the implementation of policies, procedures, and processes governing the submission of materials for pre-publication review by persons obligated to
submit materials for such review by the terms of a nondisclosure agreement signed in accordance with Executive Order 12968 (50 U.S.C. 3161 note; relating to access to classified information), or successor order, and to ensure such policies, procedures, and processes—

“(A) include clear and consistent guidance on materials that must be submitted and the mechanisms for making such submissions;

“(B) produce timely and consistent determinations across agencies; and

“(C) incorporate mechanisms for the timely appeal of such determinations.

“(d) Consultation With Executive Committee on Classification and Declassification Programs and Technology.—In making decisions under this section, the Executive Agent for Classification and Declassification shall consult with the Executive Committee on Classification and Declassification Programs and Technology established under section 102(a).

“(e) Coordination With the National Declassification Center.—In implementing a federated classification and declassification system, the Executive Agent for Classification and Declassification shall act in coordination with the National Declassification Center estab-
lished by section 3.7(a) of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or successor order.

“(f) STANDARDS AND DIRECTIVES OF THE INFORMATION SECURITY OVERSIGHT OFFICE.—The programs, policies, and systems promoted by the Executive Agent for Classification and Declassification shall be consistent with the standards and directives established by the Information Security Oversight Office.

“(g) ANNUAL REPORT.—

“(1) IN GENERAL.—Not later than the end of the first full fiscal year beginning after the date of the enactment of the Classification Reform Act of 2023 and not less frequently than once each fiscal year thereafter, the Executive Agent for Classification and Declassification shall submit to Congress and make available to the public a report on the implementation of classification and declassification programs and processes in the most recently completed fiscal year.

“(2) COORDINATION.—Each report submitted and made available under paragraph (1) shall be coordinated with the annual report of the Information Security Oversight Office issued pursuant to section 814(d).
“(3) CONTENTS.—Each report submitted and made available under subsection (a) shall include, for the period covered by the report, the following:

“(A) The costs incurred by the Federal Government for classification and declassification.

“(B) A description of information systems of the Federal Government and technology programs, processes, and systems of agencies related to classification and declassification.

“(C) A description of the policies and directives issued by the Executive Agent for Classification and Declassification and other activities of the Executive Agent for Classification and Declassification.

“(D) A description of the challenges posed to agencies in implementing the policies and directives of the Executive Agent for Classification and Declassification as well as relevant implementing policies of the agencies.

“(E) A description of pilot programs and new investments in programs, processes, and systems relating to classification and declassification and metrics of effectiveness for such programs, processes, and systems.
“(F) A description of progress and challenges in achieving the goal described in (c)(1).

“(h) FUNDING.—

“(1) AUTHORIZATION OF APPROPRIATIONS.—

There are authorized to be appropriated to carry out this section amounts as follows:

“(A) $5,000,000 for fiscal year 2024.

“(B) For fiscal year 2025 and each fiscal year thereafter, such sums as may be necessary to carry out this section.

“(2) BUDGET ESTIMATES.—In each budget that the President submits to Congress for a fiscal year under section 1105(a) of title 31, United States Code, the President shall include an estimate of the amounts required to carry out this section in that fiscal year.”.

SEC. 712. EXECUTIVE COMMITTEE ON CLASSIFICATION AND DECLASSIFICATION PROGRAMS AND TECHNOLOGY.

Subtitle C of title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.), as added by section 711, is further amended by adding at the end the following:
“SEC. 812. EXECUTIVE COMMITTEE ON CLASSIFICATION
AND DECLASSIFICATION PROGRAMS AND
TECHNOLOGY.

“(a) ESTABLISHMENT.—There is established a com-
mittee to provide direction, advice, and guidance to the
Executive Agent for Classification and Declassification on
matters relating to classification and declassification pro-
grams and technology.

“(b) DESIGNATION.—The committee established by
subsection (a) shall be known as the ‘Executive Committee
on Classification and Declassification Programs and Tech-
nology’ (in this section referred to as the ‘Committee’).

“(c) MEMBERSHIP.—

“(1) COMPOSITION.—The Committee shall be
composed of the following:

“(A) The Director of National Intelligence.

“(B) The Under Secretary of Defense for
Intelligence.

“(C) The Secretary of Energy.

“(D) The Secretary of State.

“(E) The Director of the National Declass-
sification Center.

“(F) The Director of the Information Sec-

ity Oversight Board.

“(G) The Director of the Office of Man-
agement and Budget.
“(H) Such other members as the Executive Agent for Classification and Declassification considers appropriate.

“(2) CHAIRPERSON.—The President shall appoint the chairperson of the Committee.”.

SEC. 713. ADVISORY BODIES FOR EXECUTIVE AGENT FOR CLASSIFICATION AND DECLASSIFICATION.

Subtitle C of title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.), as added by section 711 and amended by section 712, is further amended by adding at the end the following:

“SEC. 813. ADVISORY BODIES FOR EXECUTIVE AGENT FOR CLASSIFICATION AND DECLASSIFICATION.

“The following are hereby advisory bodies for the Executive Agent for Classification and Declassification:

“(1) The Public Interest Declassification Board established by section 703(a) of the Public Interest Declassification Act of 2000 (Public Law 106–567).

“(2) The Office of the Historian of the Department of State.

“(3) The Historical Office of the Secretary of Defense.

“(4) The Office of the Chief Historian of the Central Intelligence Agency.”.
SEC. 714. INFORMATION SECURITY OVERSIGHT OFFICE.

Subtitle C of title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.), as added by section 711 and amended by sections 712 and 713, is further amended by adding at the end the following:

“SEC. 814. INFORMATION SECURITY OVERSIGHT OFFICE.

“(a) Establishment.—

“(1) In general.—There is hereby established in the executive branch of the Federal Government an office to ensure the Government protects and provides proper access to information to advance the national and public interest by standardizing and assessing the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

“(2) Designation.—The office established by paragraph (1) shall be known as the ‘Information Security Oversight Office’ (in this section referred to as the ‘Office’).

“(b) Director.—There is in the Office a director who shall be the head of the Office and who shall be appointed by the President.

“(c) Duties.—The duties of the director of the Office, which the director shall carry out in coordination with the Executive Agent for Classification and Declassification, are as follows:
“(1) To develop directives to implement a uniform system across the United States Government for classifying, safeguarding, declassifying, and downgrading of national security information.

“(2) To oversee implementation of such directives by agencies through establishment of strategic goals and objectives and periodic assessment of agency performance vis-à-vis such goals and objectives.

“(d) ANNUAL REPORT.—Each fiscal year, the director of the Office shall submit to Congress a report on the execution of the duties of the director under subsection (c).

“(e) FUNDING.—

“(1) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section amounts as follows:

“(A) $5,000,000 for fiscal year 2024.

“(B) For fiscal year 2025 and each fiscal year thereafter, such sums as may be necessary to carry out this section.

“(2) BUDGET ESTIMATES.—In each budget that the President submits to Congress for a fiscal year under section 1105(a) of title 31, United States Code, the President shall include an estimate of the
amounts required to carry out this section in that fiscal year.’’.

CHAPTER 3—REDUCING OVERCLASSIFICATION

SEC. 721. CLASSIFICATION AND DECLASSIFICATION OF INFORMATION.

(a) In General.—Title VIII of the National Security Act of 1947, as amended by chapter 2 of this subtitle, is further amended by adding at the end the following:

“Subtitle D—Classification and Declassification

“SEC. 821. CLASSIFICATION AND DECLASSIFICATION OF INFORMATION.

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

“(b) Establishment of Standards 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) permit the classification of information only in cases in which the information meets the standard set forth in subsection (c) and require the declassification of information that does not meet such standard;

“(ii) provide for no more than two levels of classification;

“(iii) provide for the declassification of information classified under this title in accordance with subsection (d);

“(iv) provide for the automatic declassification of classified records with permanent historical value in accordance with subsection (e); and
“(v) provide for the timely review of materials submitted for pre-publication review in accordance with subsection (g).

“(2) NOTICE AND COMMENT.—

“(A) NOTICE.—The President shall publish in the Federal Register notice regarding the categories and procedures proposed to be established under paragraph (1).

“(B) COMMENT.—The President shall provide an opportunity for interested persons to submit comments on the categories and procedures covered by subparagraph (A).

“(C) DEADLINE.—The President shall complete the establishment of categories and procedures under this subsection not later than 60 days after publishing notice in the Federal Register under subparagraph (A). Upon completion of the establishment of such categories and procedures, the President shall publish in the Federal Register notice regarding such categories and procedures.

“(3) MODIFICATION.—In the event the President determines to modify any categories or procedures established under paragraph (1), subpara-
graphs (A) and (B) of paragraph (2) shall apply to
the modification of such categories or procedures.

“(4) AGENCY STANDARDS AND PROCEDURES.—

“(A) IN GENERAL.—The head of each
agency shall establish a single set of consoli-
dated 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 title.

“(B) DEADLINE.—Each agency head shall
establish the standards and procedures under
subparagraph (A) not later than 60 days after
the date on which the President publishes no-
tice under paragraph (2)(C) of the categories
and standards established by the President
under this subsection.

“(C) SUBMITTAL TO CONGRESS.—Each
agency head shall submit to Congress the
standards and procedures established by such
agency head under this paragraph.

“(e) STANDARD FOR CLASSIFICATION AND DECLASS-
IFICATION.—
“(1) **In general.**—Subject to paragraphs (2) and (3), information may be classified under this title, and classified information under review for de-classification under this title may remain classified, only if the harm to national security that might reasonably be expected from disclosure of such information outweighs the public interest in disclosure of such information.

“(2) **Default rules.**—

“(A) **Default with respect to classification.**—In the event of significant doubt as to whether the harm to national security that might reasonably be expected from the disclosure of information would outweigh the public interest in the disclosure of such information, such information shall not be classified.

“(B) **Default with respect to de-classification.**—In the event of significant doubt as to whether the harm to national security that might reasonably be expected from the disclosure of information previously classified under this title would outweigh the public interest in the disclosure of such information, such information shall be declassified.
“(3) CRITERIA.—For purposes of this subsection, in determining the harm to national security that might reasonably be expected from disclosure of information, and the public interest in the disclosure of information, the official making the determination shall consider the following:

“(A) With regard to the harm to national security that might reasonably be expected from disclosure of information, whether or not disclosure of the information would—

“(i) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

“(ii) reveal information that would assist in the development or use of weapons of mass destruction;

“(iii) reveal information that would impair United States cryptologic systems or activities;
“(iv) reveal information that would impair the application of state-of-the-art technology within a United States weapons system;

“(v) reveal actual United States military war plans that remain in effect;

“(vi) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

“(vii) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

“(viii) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

“(ix) violate a statute, treaty, or international agreement.
“(B) With regard to the public interest in disclosure of information—

“(i) whether or not disclosure of the information would better enable United States citizens to hold Government officials accountable for their actions and policies;

“(ii) whether or not disclosure of the information would assist the United States criminal justice system in holding persons responsible for criminal acts or acts contrary to the Constitution;

“(iii) whether or not disclosure of the information would assist Congress, or any committee or subcommittee thereof, in carrying out its oversight responsibilities with regard to the executive branch or in adequately informing itself of executive branch policies and activities in order to carry out its legislative responsibilities;

“(iv) whether the disclosure of the information would assist Congress or the public in understanding the interpretation of the Federal Government of a provision of law, including Federal regulations, Pres-
identical directives, statutes, case law, and
the Constitution of the United States; or

“(v) whether or not disclosure of the
information would bring about any other
significant benefit, including an increase in
public awareness or understanding of Gov-
ernment activities or an enhancement of
Government efficiency.

“(4) WRITTEN JUSTIFICATION FOR CLASSIFICA-
TION.—

“(A) ORIGINAL CLASSIFICATION.—Each
agency official who makes a decision to classify
information not previously classified shall, at
the time of the classification decision—

“(i) identify himself or herself; and

“(ii) provide in writing a detailed jus-
tification of that decision.

“(B) DERIVATIVE CLASSIFICATION.—In
any case in which an agency official or con-
tractor employee classifies a document on the
basis of information previously classified that is
included or referenced in the document, the of-
official or employee, as the case may be, shall—

“(i) identify himself or herself in that
document; and

VerDate Sep 11 2014 23:46 Jun 22, 2023 Jkt 039200 PO 00000 Frm 00148 Fmt 6652 Sfmt 6201 E:\BILLS\S2103.RS S2103pbinns on DSKJLVW7X2PROD with $$_JOB
“(ii) use a concise notation, or similar means, to document the basis for that decision.

“(5) Classification prohibitions and limitations.—

“(A) In general.—In no case shall information 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 national security.

“(B) Basic scientific research.—Basic scientific research information not clearly related to national security shall not be classified.

“(C) Reclassification.—Information may not be reclassified after being declassified and release to the public under proper authority unless personally approved by the President based on a determination that such reclassification—
tion is required to prevent significant and de-
monstrable damage to national security;
“(d) **DECLASSIFICATION OF INFORMATION CLASSI-
FIED UNDER ACT.**—
“(1) **IN GENERAL.**—No information may re-
main classified indefinitely.
“(2) **MAXIMUM PERIOD OF CLASSIFICATION.**—
Except as provided in paragraphs (3), (4), and (5),
information may not remain classified under this
title after the date that is 25 years after the date
of the original classification of the information.
“(3) **EARLIER DECLASSIFICATION.**—When
classifying information under this title, an agency
official may provide for the declassification of the in-
formation as of a date or event that is earlier than
the date otherwise provided for under paragraph (2).
“(4) **LATER DECLASSIFICATION.**—When
classifying information under this title, an agency
official may provide for the declassification of the in-
formation on the date that is 50 years after the date
of the classification if the head of the agency—
“(A) determines that there is no likely set
of circumstances under which declassification
would occur within the time otherwise provided
for under paragraph (2);
“(B)(i) obtains the concurrence of the director of the Information Security Oversight Office in the determination; or

“(ii) seeks but is unable to obtain concurrence under clause (i), obtains the concurrence of the President; and

“(C) submits to the President a certification of the determination.

“(5) POSTPONEMENT OF DECLASSIFICATION.—

“(A) IN GENERAL.—The declassification of any information or category of information that would otherwise be declassified under paragraph (2) or (4) may be postponed, but only with the personal approval of the President based on a determination that such postponement is required to prevent significant and demonstrable damage to the national security of the United States.

“(B) GENERAL DURATION OF POSTPONEMENT.—Information the declassification of which is postponed under this paragraph may remain classified not longer than 10 years after the date of the postponement, unless such classification is renewed by the President.
“(C) **Congressional notification.**—

Within 30 days of any postponement or renewal of a postponement under this paragraph, the President shall provide written notification to Congress of such postponement or renewal that describes the significant and demonstrable damage to the national security of the United States that justifies such postponement or renewal.

“(6) **Basis for determinations.**—An agency official making a determination under this subsection with respect to the duration of classification of information, or the declassification of information, shall make the determination required under subsection (c) with respect to classification or declassification in accordance with an assessment of the criteria specified in paragraph (3) of such subsection (c) that is current as of the determination.

“(e) **Automatic declassification of classified records.**—

“(1) **In general.**—Except as provided in paragraph (2), all classified records that are more than 50 years old and have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified on Decem-
ber 31 of the year that is 50 years after the date
on which the records were created, whether or not
the records have been reviewed.

“(2) POSTPONEMENT.—

“(A) AGENCY POSTPONEMENT.—The head
of an agency may postpone automatic declass-
sification under paragraph (1) of specific
records or information, or renew a period of
postponed automatic declassification, if the
agency head determines that disclosure of the
records or information would clearly and de-
monstrably be expected—

“(i) to reveal the identity of a con-
fidential human source or a human intel-
ligence source; or

“(ii) to reveal information that would
assist in the development, production, or
use of weapons of mass destruction.

“(B) PRESIDENTIAL POSTPONEMENT.—
The President may postpone automatic declass-
sification under paragraph (1) of specific
records or information if the President deter-
mines that such postponement is required to
prevent significant and demonstrable damage to
the national security of the United States.
“(C) General duration of postponement.—A period of postponement of automatic declassification under this paragraph shall not exceed 10 years after the date of the postponement, unless renewed by the agency head who postponed the automatic declassification or the President.

“(D) Congressional notification.—Within 30 days of any postponement or renewal of a postponement under this paragraph, the President or the head of the agency responsible for the postponement shall provide written notification to Congress of such postponement or renewal that describes the justification for such postponement or renewal.

“(f) Declassification of current classified information.—

“(1) Procedures.—The President shall establish procedures for declassifying information that was classified before the date of the enactment of the Classification Reform Act of 2023. Such procedures shall, to the maximum extent practicable, be consistent with the provisions of this section.

“(2) Automatic declassification.—The procedures established under paragraph (1) shall in-
clude procedures for the automatic declassification of information referred to in paragraph (1) that has remained classified for more than 25 years as of such date.

“(3) NOTICE AND COMMENT.—

“(A) NOTICE.—The President shall publish notice in the Federal Register of the procedures proposed to be established under this subsection.

“(B) COMMENT.—The President shall provide an opportunity for interested persons to submit comments on the procedures covered by subparagraph (A).

“(C) DEADLINE.—The President shall complete the establishment of procedures under this subsection not later than 60 days after publishing notice in the Federal Register under subparagraph (A). Upon completion of the establishment of such procedures, the President shall publish in the Federal Register notice regarding such procedures.

“(g) PRE-PUBLICATION REVIEW.—

“(1) IN GENERAL.—The head of each agency that requires personnel to sign a nondisclosure agreement in accordance with Executive Order
12968 (50 U.S.C. 3161 note; relating to access to classified information), or successor order, providing for the submittal of materials for pre-publication review, shall establish a process for the timely review of such materials consistent with the requirements of this title.

“(2) REQUIREMENTS.—Each process established under paragraph (1) shall include the following:

“(A) Clear guidance on materials required to be submitted and the means of submission.

“(B) Mechanisms for ensuring consistent decision making across multiple agencies.

“(C) Mechanisms for appeal of decisions made in the course of the review process.

“(3) CENTRALIZED APPEAL.—The President shall establish a mechanism for centralized appeal of agency decisions made pursuant to this subsection.”.

(b) CONFORMING AMENDMENT TO FOIA.—Section 552(b)(1) of title 5, United States Code, is amended to read as follows:

“(1)(A) specifically authorized to be classified under the title VIII of the National Security Act of 1947, or specifically authorized under criteria estab-
lished by an Executive order to be kept secret in the
interest of national security; and

“(B) are in fact properly classified pursuant to
that title or Executive order;”.

(c) EFFECTIVE DATE.—

(1) IN GENERAL.—Section 821 of the National
Security Act of 1947, as added by subsection (a),
and the amendment made by subsection (b), shall
take effect on the date that is 180 days after the
date of the enactment of this Act.

(2) RELATION TO PRESIDENTIAL DIREC-
TIVES.—Presidential directives regarding classifying,
safeguarding, and declassifying national security in-
formation, including Executive Order 13526 (50
U.S.C. 3161 note; relating to classified national se-
curity information), or successor order, in effect on
the day before the date of the enactment of this Act,
as well as procedures issued pursuant to such Presi-
dential directives, shall remain in effect until super-
seded by procedures issues pursuant to section 821
of the National Security Act of 1947, as added by
subsection (a).
SEC. 722. DECLASSIFICATION WORKING CAPITAL FUNDS.

Subtitle D of title VIII of the National Security Act of 1947, as added by section 721, is amended by adding at the end the following:

"SEC. 822. DECLASSIFICATION WORKING CAPITAL FUNDS.

"(a) Definition of Covered Agency.—In this section, the term ‘covered agency’ means an agency that has original classification authority.

"(b) Programs Required.—Not later than 90 days after the date of the enactment of the Classification Reform Act of 2023, each head of a covered agency shall establish a program for the automatic declassification of classified records that have permanent historical value.

"(c) Estimates.—Each head of a covered agency shall ensure that the program established by the head pursuant to subsection (b) includes a mechanism for estimating the number of classified records generated by each subcomponent of the covered agency each fiscal year.

"(d) Declassification Working Capital Funds.—

“(1) Establishment.—For each covered agency, there is established in the Treasury of the United States a fund to be known as the ‘Declassification Working Capital Fund’ of the respective covered agency.
“(2) CONTENTS OF FUNDS.—Each fund established under paragraph (1) shall consist of the following:

“(A) Amounts transferred to the fund under subsection (e).

“(B) Amounts appropriated to the fund.

“(3) AVAILABILITY AND USE OF FUNDS.—Subject to the concurrence of the Executive Agent for Classification and Declassification, amounts in a fund of a covered agency established by paragraph (1) shall be available, without fiscal year limitation, to promote and implement technological and automated solutions that are interoperable across covered agencies to support the programs of covered agencies established pursuant to subsection (b).

“(e) TRANSFERS TO THE FUNDS.—Each head of a covered agency shall issue regulations for the covered agency, subject to review and approval by the Executive Agent for Classification and Declassification, that require each subcomponent of the covered agency to transfer, on a periodic basis, to the fund established for the covered agency under subsection (c)(1), an amount for a period that bears the same ratio to the total amount transferred to the fund by all subcomponents of the covered agency for that period as the ratio of—
“(1) the estimate for the subcomponent pursuant to the mechanism required by subsection (c) for that period; bears to
“(2) the aggregate of all of the estimates for all subcomponents of the Executive agency under such mechanism for the same period.”.

SEC. 723. TRANSPARENCY OFFICERS.

Section 1062(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee–1(a)) is amended—

(1) in paragraph (3), by striking “; and” and inserting a semicolon;
(2) in paragraph (4)(C), by striking the period at the end and inserting “; and”;
(3) by adding at the end the following:

“(5) assist the head of such department, agency, or element and other officials of such department, agency, or element in identifying records of significant public interest and prioritizing appropriate review of such records in order to facilitate the public disclosure of such records in redacted or unredacted form.”;

(4) in paragraph (4), by redesignating subparagraphs (A) through (C) as clauses (i) through (iii),
respectively, and indenting such clauses 2 ems to the right;

(5) by redesignating paragraphs (1) through (5) as subparagraphs (A) through (E), respectively, and indenting such subparagraphs 2 ems to the right;

(6) in the matter before subparagraph (A), as redesignated by paragraph (5), by striking “The Attorney General” and inserting the following:

“(1) IN GENERAL.—The Attorney General”;

and

(7) by adding at the end the following:

“(2) Determining public interest in disclosure.—In assisting the head of a department, agency, or element and other officials of such department, agency, or element in identifying records of significant public interest under subparagraph (E) of paragraph (1), a senior officer designated under such paragraph shall consider—

“(A) whether or not disclosure of the information would better enable United States citizens to hold Federal Government officials accountable for their actions and policies;

“(B) whether or not disclosure of the information would assist the United States crimi-
nal justice system in holding persons responsi-
ble for criminal acts or acts contrary to the
Constitution;

“(C) whether or not disclosure of the infor-
mation would assist Congress, or any committee
or subcommittee thereof, in carrying out its
oversight responsibilities with regard to the ex-
ceutive branch or in adequately informing itself
of executive branch policies and activities in
order to carry out its legislative responsibilities;

“(D) whether the disclosure of the infor-
mation would assist Congress or the public in
understanding the interpretation of the Federal
Government of a provision of law, including
Federal regulations, Presidential directives,
statutes, case law, and the Constitution of the
United States; or

“(E) whether or not disclosure of the in-
formation would bring about any other signifi-
cant benefit, including an increase in public
awareness or understanding of Government ac-
tivities or an enhancement of Federal Govern-
ment efficiency.”.
CHAPTER 4—PREVENTING MISHANDLING
OF CLASSIFIED INFORMATION

SEC. 731. SECURITY REVIEW OF CERTAIN RECORDS OF THE
PRESIDENT AND VICE PRESIDENT.

Title VIII of the National Security Act of 1947, as
amended by chapters 2 and 3 of this subtitle, is further
amended by adding at the end the following:

“Subtitle E—Protection of
Classified Information

“SEC. 831. SECURITY REVIEW OF CERTAIN RECORDS OF
THE PRESIDENT AND VICE PRESIDENT.

“(a) DEFINITIONS.—In this section:

“(1) ARCHIVIST, DOCUMENTARY MATERIAL,
PRESIDENTIAL RECORDS, PERSONAL RECORDS.—
The terms ‘Archivist’, ‘documentary material’, ‘Pres-
idential records’, and ‘personal records’ have the
meanings given such terms in section 2201 of title
44, United States Code.

“(2) COMMINGLED OR UNCATEGORIZED
RECORDS.—

“(A) IN GENERAL.—Except as provided in
subparagraph (B), the term ‘commingled or
uncategorized records’ means all documentary
materials not categorized as Presidential
records or personal records upon their creation
or receipt and filed separately pursuant to section 2203(d) of title 44, United States Code.

“(B) EXCEPTION.—The term ‘commingled or uncategorized records’ does not include documentary materials that are—

“(i) official records of an agency (as defined in section 552(f) of title 5, United States Code);

“(ii) stocks of publications and stationery; or

“(iii) extra copies of documents produced only for convenience of reference, when such copies are clearly so identified.

“(3) OFFICIAL RECORDS OF AN AGENCY.—The term ‘official records of an agency’ means official records of an agency within the meaning of such terms in section 552 of title 5, United States.

“(b) PRESUMPTION AS PRESIDENTIAL RECORDS.—Commingled or uncategorized records shall be presumed to be Presidential records, unless the President or Vice President—

“(1) categorizes the commingled or uncategorized records as personal records in accordance with subsection (c); or
“(2) determines the commingled or uncategorized records are—

“(A) official records of an agency;

“(B) stocks of publications and stationery;

or

“(C) extra copies of documents produced only for convenience of reference, when such copies are clearly so identified.

“(e) CATEGORIZING COMMINGLED OR UNCATEGORIZED RECORDS AS PERSONAL RECORDS.—At any time during the President or Vice President’s term of office, the President or Vice President may categorize commingled or uncategorized records as personal records if—

“(1) the Archivist performs a security review of the commingled or uncategorized records that is reasonably designed to identify records that contain standard markings indicating that records contain classified information;

“(2) the President obtains written confirmation from the Archivist that the review conducted pursuant to paragraph (1) did not identify any records that contain standard markings indicating that records contain classified information or, if such
markings were improperly applied, that such markings have been corrected; and

“(3) the President obtains written confirmation from the Archivist that the Archivist is not aware of any other requirement that would preclude categorizing the commingled or uncategorized records as personal records.

“(d) Review of Commingled or Uncategorized Records of Former Presidents and Vice Presidents.—

“(1) Requests for review.—During the 180-day period following the end of the term of office of a former President or Vice President—

“(A) the former President or Vice President may request that the Archivist review the categorization of any commingled or uncategorized records created or received during the term of the former President or Vice President; and

“(B) the Archivist shall perform a security review of the commingled or uncategorized records pursuant to the request.

“(2) Actions upon completion of review.—If, pursuant to a review under paragraph (1), the Archivist determines that any commingled
or uncategorized records reviewed are improperly categorized, the Archivist shall—

“(A) submit to the President a recommendation to correct the categorization of the records; and

“(B) notify the former President or Vice President of that recommendation.”.

SEC. 732. MANDATORY COUNTERINTELLIGENCE RISK ASSESSMENTS.

(a) IN GENERAL.—Subtitle E of title VIII of the National Security Act of 1947, as added by section 731, is amended by adding at the end the following:

“SEC. 832. MANDATORY COUNTERINTELLIGENCE RISK ASSESSMENTS.

“(a) Mishandling or Unauthorized Disclosure of Classified Information Defined.—In this section, the term ‘mishandling or unauthorized disclosure of classified information’ means any unauthorized storage, retention, communication, confirmation, acknowledgment, or physical transfer of classified information.

“(b) Assessments.—The Director of the National Counterintelligence and Security Center shall prepare a written assessment of the risk to national security from any mishandling or unauthorized disclosure of classified information involving the conduct of the President, Vice
President, or an official listed in Level I of the Executive
Schedule under section 5312 of title 5, United States
Code, within 90 days of the detection of such mishandling
or unauthorized disclosure.

“(c) DESCRIPTION OF RISKS.—A written assessment
prepared pursuant to subsection (b) shall describe the risk
to national security if the classified information were to
be exposed in public or to a foreign adversary.

“(d) SUBMITTAL OF ASSESSMENTS.—Each written
assessment prepared pursuant to subsection (b) shall be
submitted to Congress, in classified form, upon comple-
tion.”.

(b) PROSPECTIVE APPLICATION.—Section 832 of
such Act, as added by subsection (a), shall apply to inci-
dents of mishandling or unauthorized disclosure of classi-
fied information (as defined in such section) detected on
or after the date of the enactment of this Act.

SEC. 733. MINIMUM STANDARDS FOR EXECUTIVE AGENCY
INSIDER THREAT PROGRAMS.

(a) DEFINITIONS.—In this section, the terms “agen-
cy” and “classified information” have the meanings given
such terms in section 800 of the National Security Act
of 1947, as added by section 702 of this subtitle.

(b) ESTABLISHMENT OF INSIDER THREAT PRO-
GRAMS.—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 in order 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 that 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.

CHAPTER 5—OTHER MATTERS

SEC. 741. PROHIBITIONS.

(a) Withholding Information From Congress.—Nothing in this subtitle or an amendment made by this subtitle shall be construed to authorize the withholding of information from Congress.

(b) Judicial Review.—Except in the case of the amendment to section 552 of title 5, United States Code, made by section 721(b), no person may seek or obtain judicial review of any provision of this subtitle or any action taken under a provision of this subtitle.

SEC. 742. CONFORMING AMENDMENT.

Section 804 of the National Security Act of 1947 (50 U.S.C. 3163) is amended by striking “this title” and inserting “sections 801 and 802”.

SEC. 743. CLERICAL AMENDMENT.

The table of contents for the National Security Act of 1947 is amended by striking the items relating to title VIII and inserting the following:

“TITLE VIII—PROTECTION OF NATIONAL SECURITY INFORMATION

“Subtitle A—Definitions

“Sec. 800. Definitions.

“Subtitle B—Access to Classified Information Procedures

“Sec. 801. Procedures.”
Subtitle B—Sensible Classification

Act of 2023

SEC. 751. SHORT TITLE.

This subtitle may be cited as the “Sensible Classification Act of 2023”.

SEC. 752. DEFINITIONS.

In this subtitle:

(1) AGENCY.—The term “agency” has the meaning given the term “Executive agency” in section 105 of title 5, United States Code.

(2) CLASSIFICATION.—The term “classification” means the act or process by which information is determined to be classified information.

(3) CLASSIFIED INFORMATION.—The term “classified information” means information that has
been determined pursuant to Executive Order 12958
(50 U.S.C. 3161 note; relating to classified national
security information), or successor order, to require
protection against unauthorized disclosure and is
marked to indicate its classified status when in doc-
umentary form.

(4) DECLASSIFICATION.—The term “declass-
sification” means the authorized change in the sta-
tus of information from classified information to un-
classified information.

(5) DOCUMENT.—The term “document” means
any recorded information, regardless of the nature of
the medium or the method or circumstances of re-
cording.

(6) DOWNGRADE.—The term “downgrade”
means a determination by a declassification author-
ity that information classified and safeguarded at a
specified level shall be classified and safeguarded at
a lower level.

(7) INFORMATION.—The term “information”
means any knowledge that can be communicated or
documentary material, regardless of its physical
form or characteristics, that is owned by, is pro-
duced by or for, or is under the control of the
United States Government.
8. ORIGINATE, ORIGINATING, AND ORIGINATED.—The term “originate”, “originating”, and “originated”, with respect to classified information and an authority, means the authority that classified the information in the first instance.

9. RECORDS.—The term “records” means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency’s control under the terms of the contract, license, certificate, or grant.

10. SECURITY CLEARANCE.—The term “security clearance” means an authorization to access classified information.

11. UNAUTHORIZED DISCLOSURE.—The term “unauthorized disclosure” means a communication or physical transfer of classified information to an unauthorized recipient.

12. UNCLASSIFIED INFORMATION.—The term “unclassified information” means information that is not classified information.
SEC. 753. FINDINGS AND SENSE OF THE SENATE.

(a) FINDINGS.—The Senate makes the following findings:

(1) According to a report released by the Office of the Director of Intelligence in 2020 titled "Fiscal Year 2019 Annual Report on Security Clearance Determinations", more than 4,000,000 individuals have been granted eligibility for a security clearance.

(2) At least 1,300,000 of such individuals have been granted access to information classified at the Top Secret level.

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

(1) the classification system of the Federal Government is in urgent need of reform;

(2) the number of people with access to classified information is exceedingly high and must be justified or reduced;

(3) reforms are necessary to reestablish trust between the Federal Government and the people of the United States; and

(4) classification should be limited to the minimum necessary to protect national security while balancing the public’s interest in disclosure.
SEC. 754. CLASSIFICATION AUTHORITY.

(a) IN GENERAL.—The authority to classify information originally may be exercised only by—

(1) the President and, in the performance of executive duties, the Vice President;

(2) the head of an agency or an official of any agency authorized by the President pursuant to a designation of such authority in the Federal Register; and

(3) an official of the Federal Government to whom authority to classify information originally has been delegated pursuant to subsection (c).

(b) SCOPE OF AUTHORITY.—An individual authorized by this section to classify information originally at a specified level may also classify the information originally at a lower level.

(c) DELEGATION OF ORIGINAL CLASSIFICATION AUTHORITY.—An official of the Federal Government may be delegated original classification authority subject to the following:

(1) Delegation of original classification authority shall be limited to the minimum required to administer this section. Agency heads shall be responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.
(2) Authority to originally classify information at the level designated as “Top Secret” may be delegated only by the President, in the performance of executive duties, the Vice President, or an agency head or official designated pursuant to subsection (a)(2).

(3) Authority to originally classify information at the level designated as “Secret” or “Confidential” may be delegated only by the President, in the performance of executive duties, the Vice President, or an agency head or official designated pursuant to subsection (a)(2), or the senior agency official described in section 5.4(d) of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or successor order, provided that official has been delegated “Top Secret” original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided by paragraphs (1), (2), and (3). Each delegation shall identify the official by name or position title.

(d) TRAINING REQUIRED.—

(1) IN GENERAL.—An individual may not be delegated original classification authority under this...
section unless the individual has first received training described in paragraph (2).

(2) TRAINING DESCRIBED.—Training described in this paragraph is training on original classification that includes instruction on the proper safeguarding of classified information and of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.

(c) EXCEPTIONAL CASES.—

(1) IN GENERAL.—When an employee, contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that employee, contractor, licensee, certificate holder, or grantee to require classification, the information shall be protected in a manner consistent with Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or successor order.

(2) TRANSMITTAL.—An employee, contractor, licensee, certificate holder, or grantee described in paragraph (1), who originates information described in such paragraph, shall promptly transmit such information to—
(A) the agency that has appropriate subject matter interest and classification authority with respect to this information; or

(B) if it is not clear which agency has appropriate subject matter interest and classification authority with respect to the information, the Director of the Information Security Oversight Office.

(3) AGENCY DECISIONS.—An agency that receives information pursuant to paragraph (2)(A) or (4) shall decide within 30 days whether to classify this information.

(4) INFORMATION SECURITY OVERSIGHT OFFICE ACTION.—If the Director of the Information Security Oversight Office receives information under paragraph (2)(B), the Director shall determine the agency having appropriate subject matter interest and classification authority and forward the information, with appropriate recommendations, to that agency for a classification determination.

SEC. 755. PROMOTING EFFICIENT DECLASSIFICATION REVIEW.

(a) IN GENERAL.—Whenever an agency is processing a request pursuant to section 552 of title 5, United States Code (commonly known as the “Freedom of Information
Act”) or the mandatory declassification review provisions of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or successor order, and identifies responsive classified records that are more than 25 years of age as of December 31 of the year in which the request is received, the head of the agency shall review the record and process the record for declassification and release by the National Declassification Center of the National Archives and Records Administration.

(b) APPLICATION.—Subsection (a) shall apply—

(1) regardless of whether or not the record described in such subsection is in the legal custody of the National Archives and Records Administration; and

(2) without regard for any other provisions of law or existing agreements or practices between agencies.

SEC. 756. TRAINING TO PROMOTE SENSIBLE CLASSIFICATION.

(a) DEFINITIONS.—In this section:

(1) OVER-CLASSIFICATION.—The term “over-classification” means classification at a level that exceeds the minimum level of classification that is suf-
ficient to protect the national security of the United States.

(2) **Sensible Classification.**—The term “sensible classification” means classification at a level that is the minimum level of classification that is sufficient to protect the national security of the United States.

(b) **Training Required.**—Each head of an agency with classification authority shall conduct training for employees of the agency with classification authority to discourage over-classification and to promote sensible classification.

**SEC. 757. IMPROVEMENTS TO PUBLIC INTEREST DECLASSIFICATION BOARD.**

Section 703 of the Public Interest Declassification Act of 2000 (50 U.S.C. 3355a) is amended—

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

“(5) A member of the Board whose term has expired may continue to serve until a successor is appointed and sworn in.”; and

(2) in subsection (f)—

(A) by inserting “(1)” before “Any employee”; and

(B) by adding at the end the following:
“(2)(A) In addition to any employees detailed to the Board under paragraph (1), the Board may hire not more than 12 staff members.

“(B) There are authorized to be appropriated to carry out subparagraph (A) such sums as are necessary for fiscal year 2024 and each fiscal year thereafter.”

SEC. 758. IMPLEMENTATION OF TECHNOLOGY FOR CLASSIFICATION AND DECLASSIFICATION.

(a) In General.—Not later than 1 year after the date of the enactment of this Act, the Administrator of the Office of Electronic Government (in this section referred to as the “Administrator”) shall, in consultation with the Secretary of Defense, the Director of the Central Intelligence Agency, the Director of National Intelligence, the Public Interest Declassification Board, the Director of the Information Security Oversight Office, and the head of the National Declassification Center of the National Archives and Records Administration—

(1) research a technology-based solution—

(A) utilizing machine learning and artificial intelligence to support efficient and effective systems for classification and declassification; and
(B) to be implemented on an interoperable and federated basis across the Federal Government; and

(2) submit to the President a recommendation regarding a technology-based solution described in paragraph (1) that should be adopted by the Federal Government.

(b) STAFF.—The Administrator may hire sufficient staff to carry out subsection (a).

(c) REPORT.—Not later than 540 days after the date of the enactment of this Act, the President shall submit to Congress a classified report on the technology-based solution recommended by the Administrator under subsection (a)(2) and the President’s decision regarding its adoption.

SEC. 759. STUDIES AND RECOMMENDATIONS ON NECESSITY OF SECURITY CLEARANCES.

(a) AGENCY STUDIES ON NECESSITY OF SECURITY CLEARANCES.—

(1) STUDIES REQUIRED.—The head of each agency that grants security clearances to personnel of such agency shall conduct a study on the necessity of such clearances.

(2) REPORTS REQUIRED.—
(A) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, each head of an agency that conducts a study under paragraph (1) shall submit to Congress a report on the findings of the agency head with respect to such study, which the agency head may classify as appropriate.

(B) REQUIRED ELEMENTS.—Each report submitted by the head of an agency under subparagraph (A) shall include, for such agency, the following:

(i) The number of personnel eligible for access to information up to the “Top Secret” level.

(ii) The number of personnel eligible for access to information up to the “Secret” level.

(iii) Information on any reduction in the number of personnel eligible for access to classified information based on the study conducted under paragraph (1).

(iv) A description of how the agency head will ensure that the number of security clearances granted by such agency will be kept to the minimum required for the
conduct of agency functions, commensurate
with the size, needs, and mission of the
agency.

(3) INDUSTRY.—This subsection shall apply to
the Secretary of Defense in the Secretary’s capacity
as the Executive Agent for the National Industrial
Security Program, and the Secretary shall treat con-
tractors, licensees, and grantees as personnel of the
Department of Defense for purposes of the studies
and reports required by this subsection.

(b) DIRECTOR OF NATIONAL INTELLIGENCE REVIEW
OF SENSITIVE COMPARTMENTED INFORMATION.—The
Director of National Intelligence shall—

(1) review the number of personnel eligible for
access to sensitive compartmented information; and

(2) submit to Congress a report on how the Di-
rector will ensure that the number of such personnel
is limited to the minimum required.

(c) AGENCY REVIEW OF SPECIAL ACCESS PRO-
GRAMS.—Each head of an agency who is authorized to es-
tablish a special access program by Executive Order
13526 (50 U.S.C. 3161 note; relating to classified na-
tional security information), or successor order, shall—
(1) review the number of personnel of the agency eligible for access to such special access programs; and

(2) submit to Congress a report on how the agency head will ensure that the number of such personnel is limited to the minimum required.

(d) Secretary of Energy Review of Q and L Clearances.—The Secretary of Energy shall—

(1) review the number of personnel of the Department of Energy granted Q and L access; and

(2) submit to Congress a report on how the Secretary will ensure that the number of such personnel is limited to the minimum required

(e) Independent Reviews.—Not later than 180 days after the date on which a study is completed under subsection (a) or a review is completed under subsections (b) through (d), the Director of the Information Security Oversight Office of the National Archives and Records Administration, the Director of National Intelligence, and the Public Interest Declassification Board shall each review the study or review, as the case may be.
TITLE VIII—SECURITY CLEARANCE AND TRUSTED WORKFORCE

SEC. 801. REVIEW OF SHARED INFORMATION TECHNOLOGY SERVICES FOR PERSONNEL VETTING.

Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a review of the extent to which the intelligence community can use information technology services shared among the intelligence community for purposes of personnel vetting, including with respect to human resources, suitability, and security.

SEC. 802. TIMELINESS STANDARD FOR RENDERING DETERMINATIONS OF TRUST FOR PERSONNEL VETTING.

(a) Timeliness Standard.—

(1) In general.—The President shall, acting through the Security Executive Agent and the Suitability and Credentialing Executive Agent, establish and publish in the Federal Register new timeliness performance standards for processing personnel vetting trust determinations in accordance with the Federal personnel vetting performance management standards.
(2) **QUINQUENNIAL REVIEWS.**—Not less frequently than once every 5 years, the President shall, acting through the Security Executive Agent and the Suitability and Credentialing Executive Agent—

(A) review the standards established pursuant to paragraph (1); and

(B) pursuant to such review—

(i) update such standards as the President considers appropriate; and

(ii) publish in the Federal Register such updates as may be made pursuant to clause (i).

(3) **CONFORMING AMENDMENT.**—Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341) is amended by striking subsection (g).

(b) **QUARTERLY REPORTS ON IMPLEMENTATION.**—

(1) **IN GENERAL.**—Not less frequently than quarterly, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly make available to the public a quarterly report on the compliance of Executive agencies (as defined in section 105 of title 5, United States Code) with the standards established pursuant to subsection (a).
(2) Disaggregation.—Each report made available pursuant to paragraph (1) shall disaggregate data by appropriate category of personnel risk and between Government and contractor personnel.

(c) Complementary Standards for Intelligence Community.—The Director of National Intelligence may, in consultation with the Security, Suitability, and Credentialing Performance Accountability Council established pursuant to Executive Order 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for Government employment, fitness for contractor employees, and eligibility for access to classified national security information) establish for the intelligence community standards complementary to those established pursuant to subsection (a).

SEC. 803. ANNUAL REPORT ON PERSONNEL VETTING TRUST DETERMINATIONS.

(a) Definition of Personnel Vetting Trust Determination.—In this section, the term “personnel vetting trust determination” means any determination made by an executive branch agency as to whether an individual can be trusted to perform job functions or to be granted access necessary for a position.
(b) Annual Report.—Not later than March 30, 2024, and annually thereafter for 5 years, the Director of National Intelligence, acting as the Security Executive Agent, and the Director of the Office of Personnel Management, acting as the Suitability and Credentialing Executive Agent, in coordination with the Security, Suitability, and Credentialing Performance Accountability Council, shall jointly make available to the public a report on specific types of personnel vetting trust determinations made during the fiscal year preceding the fiscal year in which the report is made available, disaggregated by the following:

1. Determinations of eligibility for national security-sensitive positions, separately noting—
   a. the number of individuals granted access to national security information; and
   b. the number of individuals determined to be eligible for but not granted access to national security information.

2. Determinations of suitability or fitness for a public trust position.

3. Status as a Government employee, a contractor employee, or other category.

(c) Elimination of Report Requirement.—Section 3001 of the Intelligence Reform and Terrorism Pre-
vention Act of 2004 (50 U.S.C. 3341) is amended by striking subsection (h).

SEC. 804. SURVEY TO ASSESS STRENGTHS AND WEAKNESSES OF TRUSTED WORKFORCE 2.0.

Not later than 1 year after the date of the enactment of this Act, and once every 2 years thereafter until 2029, the Comptroller General of the United States shall administer a survey to such sample of Federal agencies, Federal contractors, and other persons that require security clearances to access classified information as the Comptroller General considers appropriate to assess—

(1) the strengths and weaknesses of the implementation of the Trusted Workforce 2.0 initiative; and

(2) the effectiveness of vetting Federal personnel while managing risk during the onboarding of such personnel.

SEC. 805. PROHIBITION ON DENIAL OF ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION SOLELY BECAUSE OF PAST USE OF CANNABIS.

(a) DEFINITIONS.—In this section:

(1) CANNABIS.—The term “cannabis” has the meaning given the term “marihuana” in section 102 of the Controlled Substances Act (21 U.S.C. 802).
(2) Eligibility for access to classified information.—The term “eligibility for access to classified information” has the meaning given the term in the procedures established pursuant to section 801(a) of the National Security Act of 1947 (50 U.S.C. 3161(a)).

(b) Prohibition.—Notwithstanding any other provision of law, the head of an element of the intelligence community may not make a determination to deny eligibility for access to classified information to an individual based solely on the use of cannabis by the individual prior to the submission of the application for a security clearance by the individual.

TITLE IX—ANOMALOUS HEALTH INCIDENTS

SEC. 901. IMPROVED FUNDING FLEXIBILITY FOR PAYMENTS MADE BY THE CENTRAL INTELLIGENCE AGENCY FOR QUALIFYING INJURIES TO THE BRAIN.

Section 19A(d) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b(d)) is amended by striking paragraph (3) and inserting the following new paragraph:

“(3) Funding.—
“(A) IN GENERAL.—Payment under paragraph (2) in a fiscal year may be made using any funds—

“(i) appropriated in advance specifically for payments under such paragraph; or

“(ii) reprogrammed in accordance with section 504 of the National Security Act of 1947 (50 U.S.C. 3094).

“(B) BUDGET.—For each fiscal year, the Director shall include with the budget justification materials submitted to Congress in support of the budget of the President for that fiscal year pursuant to section 1105(a) of title 31, United States Code, an estimate of the funds required in that fiscal year to make payments under paragraph (2).”.

SEC. 902. CLARIFICATION OF REQUIREMENTS TO SEEK CERTAIN BENEFITS RELATING TO INJURIES TO THE BRAIN.

(a) IN GENERAL.—Section 19A(d) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b(d)) is amended by adding at the end of paragraph (5) the following new sentence: “A covered dependent, covered employee, or covered individual shall not be required to seek
any other benefit furnished by the United States Government to be eligible for the payment authorized under paragraph (2).”.

(b) REGULATIONS. —Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall—

(1) revise the regulations of the Expanded Care Program of the Central Intelligence Agency to conform with the amendment made by subsection (a); and

(2) submit to the congressional intelligence committees copies of such regulations, as revised pursuant to paragraph (1).

SEC. 903. INTELLIGENCE COMMUNITY IMPLEMENTATION OF HAVANA ACT OF 2021 AUTHORITIES.

(a) REGULATIONS. —Except as provided in subsection (c), not later than 180 days after the date of the enactment of this Act, each head of an element of the intelligence community that has not already done so shall—

(1) issue regulations and procedures to implement the authorities provided by section 19A(d) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b(d)) and section 901(i) of title IX of division J of the Further Consolidated Appropriations Act, 2020 (22 U.S.C. 2680b(i)) to provide pay-
ments under such sections, to the degree that such
authorities are applicable to the head of the element;
and
(2) submit to the congressional intelligence
committees copies of such regulations.
(b) REPORTING.—Not later than 210 days after the
date of the enactment of this Act, each head of an element
of the intelligence community shall submit to the congres-
sional intelligence committees a report on—
(1) the estimated number of individuals associ-
ated with their element that may be eligible for pay-
ment under the authorities described in subsection
(a)(1);
(2) an estimate of the obligation that the head
of the intelligence community element expects to
incur in fiscal year 2025 as a result of establishing
the regulations pursuant to subsection (a)(1); and
(3) any perceived barriers or concerns in imple-
menting such authorities.
(c) ALTERNATIVE REPORTING.—Not later than 180
days after the date of the enactment of this Act, each head
of an element of the intelligence community (other than
the Director of the Central Intelligence Agency) who be-
lieves that the authorities described in subsection (a)(1)
are not currently relevant for individuals associated with
their element, or who are not otherwise in position to issue
the regulations and procedures required by subsection
(a)(1) shall provide written and detailed justification to
the congressional intelligence committees to explain this
position.

SEC. 904. REPORT AND BRIEFING ON CENTRAL INTEL-
LIGENCE AGENCY HANDLING OF ANOMA-
LOUS HEALTH INCIDENTS.

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term “Agency” means the
Central Intelligence Agency.

(2) QUALIFYING INJURY.—The term “quali-
fying injury” has the meaning given such term in
section 19A(d)(1) of the Central Intelligence Agency
Act of 1949 (50 U.S.C. 3519b(d)(1)).

(b) IN GENERAL.—Not later than 60 days after the
date of the enactment of this Act, the Director of the Cen-
tral Intelligence Agency shall submit to the congressional
intelligence committees a report on the handling of anom-
lous health incidents by the Agency.

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

(1) HAVANA ACT IMPLEMENTATION.—

(A) An explanation of how the Agency de-
termines whether a reported anomalous health
incident resulted in a qualifying injury or a qualifying injury to the brain.

(B) The number of participants of the Expanded Care Program of the Central Intelligence Agency who—

(i) have a certified qualifying injury or a certified qualifying injury to the brain; and

(ii) as of September 30, 2023, applied to the Expanded Care Program due to a reported anomalous health incident.

(C) A comparison of the number of anomalous health incidents reported by applicants to the Expanded Care Program that occurred in the United States and that occurred in a foreign country.

(D) The specific reason each applicant was approved or denied for payment under the Expanded Care Program.

(E) The number of applicants who were initially denied payment but were later approved on appeal.

(F) The average length of time, from the time of application, for an applicant to receive a determination from the Expanded Care Pro-
gram, aggregated by qualifying injuries and qualifying injuries to the brain.

(2) PRIORITY CASES.—

(A) A detailed list of priority cases of anomalous health incidents, including, for each incident, locations, dates, times, and circumstances.

(B) For each priority case listed in accordance with subparagraph (A), a detailed explanation of each credible alternative explanation that the Agency assigned to the incident, including—

(i) how the incident was discovered;

(ii) how the incident was assigned within the Agency; and

(iii) whether an individual affected by the incident is provided an opportunity to appeal the credible alternative explanation.

(C) For each priority case of an anomalous health incident determined to be largely consistent with the definition of “anomalous health incident” established by the National Academy of Sciences and for which the Agency does not have a credible alternative explanation, a detailed description of such case.
(3) Anomalous health incident sensors.—

(A) A list of all types of sensors that the Agency has developed or deployed with respect to reports of anomalous health incidents, including, for each type of sensor, the deployment location, the date and the duration of the employment of such type of sensor, and, if applicable, the reason for removal.

(B) A list of entities to which the Agency has provided unrestricted access to data associated with anomalous health incidents.

(C) A list of requests for support the Agency has received from elements of the Federal Government regarding sensor development, testing, or deployment, and a description of the support provided in each case.

(D) A description of all emitter signatures obtained by sensors associated with anomalous health incidents in Agency holdings since 2016, including—

(i) the identification of any of such emitters that the Agency prioritizes as a threat; and
(ii) an explanation of such prioritization.

(d) ADDITIONAL SUBMISSIONS.—Concurrent with the submission of the report required by subsection (b), the Director of the Central Intelligence Agency shall submit to the congressional intelligence committees—

(1) a template of each form required to apply for the Expanded Care Program, including with respect to payments for a qualifying injury or a qualifying injury to the brain;

(2) copies of internal guidance used by the Agency to adjudicate claims for the Expanded Care Program, including with respect to payments for a qualifying injury to the brain;

(3) the case file of each applicant to the Expanded Care Program who applied due to a reported anomalous health incident, including supporting medical documentation, with name and other identifying information redacted;

(4) copies of all informational and instructional materials provided to employees of and other individuals affiliated with the Agency with respect to applying for the Expanded Care Program; and

(5) copies of Agency guidance provided to employees of and other individuals affiliated with the
Agency with respect to reporting and responding to a suspected anomalous health incident, and the roles and responsibilities of each element of the Agency tasked with responding to a report of an anomalous health incident.

(e) Briefing.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall brief the congressional intelligence committees on the report.

**TITLE X—ELECTION SECURITY**

**SEC. 1001. STRENGTHENING ELECTION CYBERSECURITY TO UPHOLD RESPECT FOR ELECTIONS THROUGH INDEPENDENT TESTING ACT OF 2023.**

(a) Short Title.—This section may be cited as the “Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2023” or the “SECURE IT Act of 2023”.

(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 accredited laboratories under this section.

“(2) ACCREDITATION.—The Director of the National Institute of Standards and Technology shall recommend to the Commission entities the Director proposes be accredited to carry out penetration testing under this subsection and certify compliance with the penetration testing-related guidelines required by this subsection. The Commission shall vote on the accreditation of any entity recommended. The requirements for such accreditation shall be a subset of the requirements for accreditation of laboratories under subsection (b) and shall only be based on consideration of an entity’s competence to conduct penetration testing under this subsection.”.

(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 follow-
lowing new part:

“PART 7—INDEPENDENT SECURITY TESTING AND
COORDINATED CYBERSECURITY VULNER-
ABILITY DISCLOSURE PILOT PROGRAM FOR
ELECTION SYSTEMS

“SEC. 297. INDEPENDENT SECURITY TESTING AND COORDI-
NATED CYBERSECURITY VULNERABILITY
DISCLOSURE PILOT PROGRAM FOR ELEC-
TION SYSTEMS.

“(a) IN GENERAL.—

“(1) ESTABLISHMENT.—The Commission, in
consultation with the Secretary, shall establish an
Independent Security Testing and Coordinated Vul-
nerability Disclosure Pilot Program for Election Sys-
tems (VDP–E) (in this section referred to as the
‘program’) in order to test for and disclose cyberse-
curity vulnerabilities in election systems.

“(2) DURATION.—The program shall be con-
ducted for a period of 5 years.

“(3) REQUIREMENTS.—In carrying out the pro-
gram, the Commission, in consultation with the Sec-
retary, 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, after receiving 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; and

“(E) 180 days after the disclosure of a vulnerability under subparagraph (C)(ii)(I), no-
tify the Director of the Cybersecurity and Infra-structure Security Agency of the vulner-
ability for inclusion in the database of Common Vulnerabilities and Exposures.

“(4) VOLUNTARY PARTICIPATION; SAFE HAR-
BOR.—

“(A) VOLUNTARY PARTICIPATION.—Par-
ticipation 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 considered to 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.

“(ii) Exempt from the anti-circumven-
tion rule of section 1201 of title 17, United States Code (commonly known as the ‘Dig-
ital 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) EXEMPT FROM DISCLOSURE.—Cybersecurity vulnerabilities discovered under the program shall be exempt from section 552 of title 5, United States Code (commonly referred to as the ‘Freedom of Information Act’).

“(6) 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 elec-
tion system on behalf of a State or local elec-
tion 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 Cybersecu-
rity Information Sharing Act of 2015 (6 U.S.C.
1501).”.

(2) Clerical amendment.—The table of con-
tents of such Act is amended by adding at the end
of the items relating to subtitle D of title II the fol-
lowing:

“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. 1002. PROTECTING BALLOT MEASURES FROM FOREIGN INFLUENCE ACT OF 2023.

(a) SHORT TITLE.—This section may be cited as the “Protecting Ballot Measures from Foreign Influence Act of 2023”.

(b) IN GENERAL.—Section 319(a)(1)(A) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30121(a)(1)(A)) is amended by inserting “, or a State or local ballot initiative or ballot referendum” after “election”.

(c) EFFECTIVE DATE.—The amendment made by subsection (b) shall apply with respect to contributions and donations made on or after the date of enactment of this Act.

TITLE XI—OTHER MATTERS

SEC. 1101. MODIFICATION OF REPORTING REQUIREMENT FOR ALL-DOMAIN ANOMALY RESOLUTION OFFICE.

Section 1683(k)(1) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(k)(1)), as amended by section 6802(a) of the Intelligence Authorization Act for Fiscal Year 2023 (Public Law 117–263), is amended—

(1) in the heading, by striking “DIRECTOR OF NATIONAL INTELLIGENCE AND SECRETARY OF DE-
FENSE” and inserting “ALL-DOMAIN ANOMALY RES-
OLUTION OFFICE”; and

(2) in subparagraph (A), by striking “Director
of National Intelligence and the Secretary of De-
fense shall jointly” and inserting “Director of the
Office shall”.

SEC. 1102. MODIFICATIONS TO NOTIFICATION ON THE PRO-
VISION OF DEFENSE SENSITIVE SUPPORT.

(a) Modification of When Notification Is Re-
quired.—Paragraph (3) of section 1055(b) of the Na-
tional Defense Authorization Act for Fiscal Year 2017
(Public Law 114–328; 10 U.S.C. 113 note) is amended—

(1) in the paragraph heading, by inserting
“AND EXTRAORDINARY SECURITY PROTECTIONS”
after “SUPPORT”;

(2) in the matter preceding subparagraph (A),
by inserting “or requires extraordinary security pro-
tections” after “time-sensitive”;  

(3) in subparagraph (A), by inserting “or after
the activity supported concludes” after “providing
the support”; and

(4) in subparagraph (B)— 

(A) by inserting “or after the activity sup-
ported concludes” after “providing such sup-
port”; and
(B) by inserting “or after the activity sup-
ported concludes” after “providing the sup-
port”.

(b) EXEMPTION.—Such section is amended by adding
at the end the following:

“(6) EXEMPTION.—The requirements of this
subsection shall not apply to the provision of defense
sensitive support for travel of the following:

“(A) The Director of National Intelligence.

“(B) The Principal Deputy Director of Na-
tional Intelligence.

“(C) The Director of the Central Intel-
ligence Agency.

“(D) The Deputy Director of the Central
Intelligence Agency.”.

SEC. 1103. MODIFICATION OF CONGRESSIONAL OVERSIGHT
OF SPECIAL ACCESS PROGRAMS.

Section 3236 of the National Nuclear Security Ad-
ministration Act (50 U.S.C. 2426) is amended—

(1) by striking “congressional defense commit-
tees” each place it appears and inserting “ap-
propriate congressional committees”; and

(2) by adding at the end the following sub-
section:
“(g) APPROPRIATE CONGRESSIONAL COMMITTEES

Defined.—In this section, the term ‘appropriate congressional committees’ means—

“(1) the congressional defense committees;

“(2) the Select Committee on Intelligence of the Senate; and

“(3) the Permanent Select Committee on Intelligence of the House of Representatives.”.

SEC. 1104. 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, and the Committee on Appropriations of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Armed Services, 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) DIRECTOR.—The term “Director” means the Director of the All-domain Anomaly Resolution Office.

(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)), as amended by section 6802(a) of the Intelligence Authorization Act for Fiscal Year 2023 (Public Law 117–263).

(b) SENSE OF CONGRESS.—It is the sense of Congress that, due to the increasing potential for technology surprise from foreign adversaries and to ensure sufficient integration across the United States industrial base and avoid technology and security stovepipes—

(1) the United States industrial base must retain its global lead in critical advanced technologies; and

(2) the Federal Government must expand awareness about any historical exotic technology
antecedents previously provided by the Federal Government for research and development purposes.

(c) LIMITATIONS.—

(1) IN GENERAL.—No amount authorized to be appropriated or appropriated by this Act or any other Act may be obligated or expended, directly or indirectly, in part or in whole, for, on, in relation to, or in support of activities involving unidentified anomalous phenomena protected under any form of special access or restricted access limitations that have not been formally, officially, explicitly, and specifically described, explained, and justified to the appropriate committees of Congress, congressional leadership, and the Director, including for any activities relating to the following:

(A) Recruiting, employing, training, equipping, and operations of, and providing security for, government or contractor personnel with a primary, secondary, or contingency mission of capturing, recovering, and securing unidentified anomalous phenomena craft or pieces and components of such craft.

(B) Analyzing such craft or pieces or components thereof, including for the purpose of determining properties, material composition,
method of manufacture, origin, characteristics, usage and application, performance, operational modalities, or reverse engineering of such craft or component technology.

(C) Managing and providing security for protecting activities and information relating to unidentified anomalous phenomena from disclosure or compromise.

(D) Actions relating to reverse engineering or replicating unidentified anomalous phenomena technology or performance based on analysis of materials or sensor and observational information associated with unidentified anomalous phenomena.

(E) The development of propulsion technology, or aerospace craft that uses propulsion technology, systems, or subsystems, that is based on or derived from or inspired by inspection, analysis, or reverse engineering of recovered unidentified anomalous phenomena craft or materials.

(F) Any aerospace craft that uses propulsion technology other than chemical propellants, solar power, or electric ion thrust.
(2) Future Appropriations.—Paragraph (1) shall apply with respect to an amount appropriated after the date of the enactment of this Act, unless such paragraph is specifically waived for such amount, or such amount is specifically exempted from such paragraph, by an Act enacted after the date of the enactment of this Act.

(d) Notification and Reporting.—Any person currently or formerly under contract with the Federal Government that has in their possession material or information provided by or derived from the Federal Government relating to unidentified anomalous phenomena that formerly or currently is protected by any form of special access or restricted access shall—

(1) not later than 60 days after the date of the enactment of this Act, notify the Director of such possession; and

(2) not later than 180 days after the date of the enactment of this Act, make available to the Director for assessment, analysis, and inspection—

(A) all such material and information; and

(B) a comprehensive list of all non-earth origin or exotic unidentified anomalous phenomena material.
(c) LIABILITY.—No criminal or civil action may lie
or be maintained in any Federal or State court against
any person for receiving material or information described
in subsection (d) if that person complies with the notifica-
tion and reporting provisions described in such subsection.

(f) LIMITATION REGARDING INDEPENDENT RE-
SEARCH AND DEVELOPMENT.—

(1) IN GENERAL.—Consistent with Department
of Defense Instruction Number 3204.01 (dated Au-
gust 20, 2014, incorporating change 2, dated July
9, 2020; relating to Department policy for oversight
of independent research and development), inde-
pendent research and development funding relating
to material or information described in subsection
(e) shall not be allowable as indirect expenses for
purposes of contracts covered by such instruction,
unless such material and information is made avail-
able to the Director in accordance with subsection
(d).

(2) EFFECTIVE DATE AND APPLICABILITY.—
Paragraph (1) shall take effect on the date that is
60 days after the date of the enactment of this Act
and shall apply with respect to funding from
amounts appropriated before, on, or after such date.
(g) NOTICE TO CONGRESS.—Not later than 30 days after the date on which the Director has received a notification under paragraph (1) of subsection (d) or information or material under paragraph (2) of such subsection, the Director shall provide written notification of such receipt to the appropriate committees of Congress and congressional leadership.
A BILL

S. 2103

118TH CONGRESS

Calendar No. 106

To authorize appropriations for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

JUNE 22, 2023

Read twice and placed on the calendar.