

Calendar No. 106

118TH CONGRESS
1ST SESSION

S. 2103

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Intelligence Authorization Act for Fiscal Year 2024”.

- 1 (b) TABLE OF CONTENTS.—The table of contents for
 2 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. 303. Policy and performance framework for mobility of intelligence community workforce.
 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

- Sec. 1001. Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2023.
- Sec. 1002. Protecting Ballot Measures from Foreign Influence Act of 2023.

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.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) CONGRESSIONAL INTELLIGENCE COMMIT-
4 TEES.—The term “congressional intelligence com-
5 mittees” has the meaning given such term in section
6 3 of the National Security Act of 1947 (50 U.S.C.
7 3003).

8 (2) INTELLIGENCE COMMUNITY.—The term
9 “intelligence community” has the meaning given
10 such term in such section.

11 **TITLE I—INTELLIGENCE**
12 **ACTIVITIES**

13 **SEC. 101. AUTHORIZATION OF APPROPRIATIONS.**

14 Funds are hereby authorized to be appropriated for
15 fiscal year 2024 for the conduct of the intelligence and
16 intelligence-related activities of the Federal Government.

17 **SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.**

18 (a) SPECIFICATIONS OF AMOUNTS.—The amounts
19 authorized to be appropriated under section 101 for the
20 conduct of the intelligence activities of the Federal Gov-
21 ernment are those specified in the classified Schedule of
22 Authorizations prepared to accompany this Act.

23 (b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AU-
24 THORIZATIONS.—

25 (1) AVAILABILITY.—The classified Schedule of
26 Authorizations referred to in subsection (a) shall be

1 made available to the Committee on Appropriations
2 of the Senate, the Committee on Appropriations of
3 the House of Representatives, and to the President.

4 (2) DISTRIBUTION BY THE PRESIDENT.—Sub-
5 ject to paragraph (3), the President shall provide for
6 suitable distribution of the classified Schedule of Au-
7 thorizations referred to in subsection (a), or of ap-
8 propriate portions of such Schedule, within the exec-
9 utive branch of the Federal Government.

10 (3) LIMITS ON DISCLOSURE.—The President
11 shall not publicly disclose the classified Schedule of
12 Authorizations or any portion of such Schedule ex-
13 cept—

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

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

19 (C) as otherwise required by law.

20 **SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT AC-**
21 **COUNT.**

22 (a) AUTHORIZATION OF APPROPRIATIONS.—There is
23 authorized to be appropriated for the Intelligence Commu-
24 nity Management Account of the Director of National In-
25 telligence for fiscal year 2024 the sum of \$658,950,000.

1 (b) CLASSIFIED AUTHORIZATION OF APPROPRIA-
 2 TIONS.—In addition to amounts authorized to be appro-
 3 priated for the Intelligence Community Management Ac-
 4 count by subsection (a), there are authorized to be appro-
 5 priated for the Intelligence Community Management Ac-
 6 count for fiscal year 2024 such additional amounts as are
 7 specified in the classified Schedule of Authorizations re-
 8 ferred to in section 102(a).

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

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

16 **TITLE II—CENTRAL INTEL-**
 17 **LIGENCE AGENCY RETIRE-**
 18 **MENT AND DISABILITY SYS-**
 19 **TEM**

20 **SEC. 201. AUTHORIZATION OF APPROPRIATIONS.**

21 There is authorized to be appropriated for the Cen-
 22 tral Intelligence Agency Retirement and Disability Fund
 23 \$514,000,000 for fiscal year 2024.

1 **TITLE III—INTELLIGENCE**
 2 **COMMUNITY MATTERS**
 3 **Subtitle A—General Intelligence**
 4 **Community Matters**

5 **SEC. 301. POST-GRADUATE EMPLOYMENT OF DEPARTMENT**
 6 **OF DEFENSE CYBER AND DIGITAL SERVICE**
 7 **ACADEMY SCHOLARSHIP RECIPIENTS IN IN-**
 8 **TELLIGENCE COMMUNITY.**

9 Section 1535(d) of the James M. Inhofe National De-
 10 fense Authorization Act for Fiscal Year 2023 (Public Law
 11 117–263) is amended by inserting “or of an element of
 12 the intelligence community (as that term is defined in sec-
 13 tion 3 of the National Security Act of 1947 (50 U.S.C.
 14 3003))” after “missions of the Department”.

15 **SEC. 302. PLAN TO RECRUIT, TRAIN, AND RETAIN PER-**
 16 **SONNEL WITH EXPERIENCE IN FINANCIAL IN-**
 17 **TELLIGENCE AND EMERGING TECH-**
 18 **NOLOGIES.**

19 (a) **IN GENERAL.**—Not later than 180 days after the
 20 date of the enactment of this Act, the Director of National
 21 Intelligence, in coordination with the heads of human cap-
 22 ital of the Central Intelligence Agency, the National Secu-
 23 rity Agency, and the Federal Bureau of Investigation,
 24 shall submit to the congressional intelligence committees
 25 a plan for the intelligence community to recruit, train, and

1 retain personnel who have skills and experience in finan-
2 cial intelligence and emerging technologies in order to im-
3 prove analytic tradecraft.

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

6 (1) An assessment, including measurable bench-
7 marks of progress, of current initiatives of the intel-
8 ligence community to recruit, train, and retain per-
9 sonnel who have skills and experience in financial in-
10 telligence and emerging technologies.

11 (2) An assessment of whether personnel in the
12 intelligence community who have such skills are cur-
13 rently well integrated into the analytical cadre of the
14 relevant elements of the intelligence community that
15 produce analyses with respect to financial intel-
16 ligence and emerging technologies.

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

22 (4) A determination of whether the National In-
23 telligence University has the resources and expertise
24 necessary to train existing personnel in financial in-
25 telligence and emerging technologies.

1 (5) A strategy, including measurable bench-
2 marks of progress, to, by January 1, 2025, increase
3 by 10 percent the analytical cadre of personnel with
4 expertise and previous employment in financial intel-
5 ligence and emerging technologies.

6 **SEC. 303. POLICY AND PERFORMANCE FRAMEWORK FOR**
7 **MOBILITY OF INTELLIGENCE COMMUNITY**
8 **WORKFORCE.**

9 (a) IN GENERAL.—Not later than 180 days after the
10 date of the enactment of this Act, the Director of National
11 Intelligence shall develop and implement a policy and per-
12 formance framework to ensure the timely and effective
13 mobility of employees and contractors of the Federal Gov-
14 ernment who are transferring employment between ele-
15 ments of the intelligence community.

16 (b) ELEMENTS.—The policy and performance frame-
17 work required by subsection (a) shall include processes
18 with respect to the following:

19 (1) Human resources.

20 (2) Medical reviews.

21 (3) Determinations of suitability or eligibility
22 for access to classified information in accordance
23 with Executive Order 13467 (50 U.S.C. 3161 note;
24 relating to reforming processes related to suitability
25 for Government employment, fitness for contractor

1 employees, and eligibility for access to classified na-
2 tional security information).

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

6 (a) IN GENERAL.—Section 135(d) of the Higher
7 Education Act of 1965 (20 U.S.C. 1015d(d)), as amended
8 by section 6206(a)(4) of the Foreign Service Families Act
9 of 2021 (Public Law 117–81), is further amended—

10 (1) in paragraph (1), by striking “or” after the
11 semicolon;

12 (2) in paragraph (2), by striking the period at
13 the end and inserting “; or”; and

14 (3) by adding at the end the following new
15 paragraph:

16 “(3) a member of the intelligence community
17 (as defined in section 3 of the National Security Act
18 of 1947 (50 U.S.C. 3003)) (other than a member of
19 the Armed Forces of the United States) who is on
20 active duty for a period of more than 30 days.”.

21 (b) EFFECTIVE DATE.—The amendments made by
22 subsection (a) shall take effect at each public institution
23 of higher education in a State that receives assistance
24 under the Higher Education Act of 1965 (20 U.S.C. 1001

1 et seq.) for the first period of enrollment at such institu-
2 tion that begins after July 1, 2026.

3 **SEC. 305. STANDARDS, CRITERIA, AND GUIDANCE FOR**
4 **COUNTERINTELLIGENCE VULNERABILITY AS-**
5 **SESSMENTS AND SURVEYS.**

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

9 “(A) COUNTERINTELLIGENCE VULNER-
10 ABILITY ASSESSMENTS AND SURVEYS.—To de-
11 velop standards, criteria, and guidance for
12 counterintelligence risk assessments and sur-
13 veys of the vulnerability of the United States to
14 intelligence threats, including with respect to
15 critical infrastructure and critical technologies,
16 in order to identify the areas, programs, and
17 activities that require protection from such
18 threats.”.

19 **SEC. 306. IMPROVING ADMINISTRATION OF CERTAIN POST-**
20 **EMPLOYMENT RESTRICTIONS FOR INTEL-**
21 **LIGENCE COMMUNITY.**

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

24 (1) in subsection (c)(1)—

1 (A) by striking “A former” and inserting
2 the following:

3 “(A) IN GENERAL.—A former”; and

4 (B) by adding at the end the following:

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

7 “(i) IN GENERAL.—In the case of a
8 former employee who occupies a covered
9 post-service position in violation of sub-
10 section (a), whether the former employee
11 voluntarily notified the Director of Na-
12 tional Intelligence of the intent of the
13 former employee to occupy such covered
14 post-service position before occupying such
15 post-service position may be used in deter-
16 mining whether the violation was knowing
17 and willful for purposes of subparagraph
18 (A).

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

24 (2) in subsection (d)—

1 (A) in paragraph (1), by inserting “the re-
2 strictions under subsection (a) and” before “the
3 report requirements”;

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

6 (C) in paragraph (3)(B), by striking “be-
7 fore the person ceases to occupy a covered intel-
8 ligence position” and inserting “when the per-
9 son occupies a covered intelligence position”.

10 **SEC. 307. MISSION OF THE NATIONAL COUNTERINTEL-**
11 **LIGENCE AND SECURITY CENTER.**

12 (a) IN GENERAL.—Section 904 of the Counterintel-
13 ligence Enhancement Act of 2002 (50 U.S.C. 3383) is
14 amended—

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

17 (2) by inserting after subsection (c) the fol-
18 lowing:

19 “(d) MISSION.—The mission of the National Coun-
20 terintelligence and Security Center shall include orga-
21 nizing and leading strategic planning for counterintel-
22 ligence activities of the United States Government by inte-
23 grating instruments of national power as needed to
24 counter foreign intelligence.”.

25 (b) CONFORMING AMENDMENTS.—

1 (1) COUNTERINTELLIGENCE ENHANCEMENT
2 ACT OF 2002.—Section 904 of the Counterintel-
3 ligence Enhancement Act of 2002 (50 U.S.C. 3383)
4 is amended—

5 (A) in subsection (e), as redesignated by
6 subsection (a)(1), by striking “Subject to sub-
7 section (e)” both places it appears and inserting
8 “Subject to subsection (f)”; and

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

10 (i) in paragraph (1), by striking “sub-
11 section (d)(1)” and inserting “subsection
12 (e)(1)”; and

13 (ii) in paragraph (2), by striking
14 “subsection (d)(2)” and inserting “sub-
15 section (e)(2)”.

16 (2) COUNTERINTELLIGENCE AND SECURITY EN-
17 HANCEMENTS ACT OF 1994.—Section
18 811(d)(1)(B)(ii) of the Counterintelligence and Se-
19 curity Enhancements Act of 1994 (50 U.S.C.
20 3381(d)(1)(B)(ii)) is amended by striking “section
21 904(d)(2) of that Act (50 U.S.C. 3383(d)(2))” and
22 inserting “section 904(e)(2) of that Act (50 U.S.C.
23 3383(e)(2))”.

1 **SEC. 308. PROHIBITION RELATING TO TRANSPORT OF INDI-**
2 **VIDUALS DETAINED AT UNITED STATES**
3 **NAVAL STATION, GUANTANAMO BAY, CUBA.**

4 (a) DEFINITION OF INDIVIDUAL DETAINED AT
5 GUANTANAMO.—In this section, the term “individual de-
6 tained at Guantanamo” has the meaning given that term
7 in section 1034(f)(2) of the National Defense Authoriza-
8 tion Act for Fiscal Year 2016 (Public Law 114–92; 129
9 Stat. 971; 10 U.S.C. 801 note).

10 (b) PROHIBITION ON CHARTERING PRIVATE OR COM-
11 Mercial AIRCRAFT TO TRANSPORT INDIVIDUALS DE-
12 TAINED AT UNITED STATES NAVAL STATION, GUANTA-
13 NAMO BAY, CUBA.—No head of an element of the intel-
14 ligence community may charter any private or commercial
15 aircraft to transport an individual who is or was an indi-
16 vidual detained at Guantanamo.

17 **SEC. 309. DEPARTMENT OF ENERGY REVIEW OF CERTAIN**
18 **FOREIGN VISITORS AND ASSIGNEES TO NA-**
19 **TIONAL LABORATORIES.**

20 (a) DEFINITIONS.—In this section:

21 (1) APPROPRIATE COMMITTEES OF CON-
22 GRESS.—The term “appropriate committees of Con-
23 gress” means—

24 (A) the Select Committee on Intelligence of
25 the Senate;

1 (B) the Committee on Energy and Natural
2 Resources of the Senate;

3 (C) the Permanent Select Committee on
4 Intelligence of the House of Representatives;
5 and

6 (D) the Committee on Energy and Com-
7 merce of the House of Representatives.

8 (2) DIRECTOR.—The term “Director” means
9 the Director of the Office of Intelligence and Coun-
10 terintelligence of the Department of Energy (or a
11 designee).

12 (3) FOREIGN NATIONAL.—The term “foreign
13 national” has the meaning given the term “alien” in
14 section 101(a) of the Immigration and Nationality
15 Act (8 U.S.C. 1101(a)).

16 (4) NATIONAL LABORATORY.—The term “Na-
17 tional Laboratory” has the meaning given the term
18 in section 2 of the Energy Policy Act of 2005 (42
19 U.S.C. 15801).

20 (5) SENSITIVE COUNTRY.—The term “sensitive
21 country” means a country to which particular con-
22 sideration is given for policy reasons during the De-
23 partment of Energy internal review and approval
24 process for visits by, and assignments of, foreign na-
25 tionals to National Laboratories.

1 (6) SENSITIVE COUNTRY NATIONAL.—The term
2 “sensitive country national” means a foreign na-
3 tional who was born in, is a citizen of, or is em-
4 ployed by a government, employer, institution, or or-
5 ganization of, a sensitive country.

6 (7) SENSITIVE COUNTRY VISITOR OR AS-
7 SIGNEE.—

8 (A) IN GENERAL.—The term “sensitive
9 country visitor or assignee” means a visitor or
10 assignee who is a sensitive country national.

11 (B) ASSOCIATED DEFINITIONS.—For pur-
12 poses of this paragraph:

13 (i) ASSIGNEE.—The term “assignee”
14 means an individual who is seeking ap-
15 proval from, or has been approved by, a
16 National Laboratory to access the prem-
17 ises, information, or technology of the Na-
18 tional Laboratory for a period of more
19 than 30 consecutive calendar days.

20 (ii) VISITOR.—The term “visitor”
21 mans an individual who is seeking approval
22 from, or has been approved by, a National
23 Laboratory to access the premises, infor-
24 mation, or technology of the National Lab-

1 oratory for any period other than a period
2 described in clause (i).

3 (b) RECOMMENDATIONS WITH RESPECT TO SEN-
4 SITIVE COUNTRY VISITORS OR ASSIGNEES.—

5 (1) NOTIFICATION AND RECOMMENDATION RE-
6 QUIREMENT.—On determination that a proposed
7 sensitive country visitor or assignee poses a counter-
8 intelligence risk to a National Laboratory, the Direc-
9 tor shall—

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

12 (B) provide a recommendation to the Na-
13 tional Laboratory on whether to grant or deny
14 the proposed sensitive country visitor or as-
15 signee access to the premises, information, or
16 technology of the National Laboratory.

17 (2) PROHIBITION.—A National Laboratory may
18 not allow a sensitive country visitor or assignee that
19 the Director has identified as a counterintelligence
20 risk under paragraph (1) to have any access to the
21 premises, information, or technology of the National
22 Laboratory until the Director has submitted the no-
23 tification and recommendation to the National Lab-
24 oratory as described in paragraph (1).

1 (3) APPLICATION TO OTHER NATIONAL LAB-
2 ORATORIES.—If the Director makes a recommenda-
3 tion under paragraph (1) that a sensitive country
4 visitor or assignee should not be granted access to
5 the premises, information, or technology of a Na-
6 tional Laboratory—

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

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

12 (c) NOTIFICATION TO DIRECTOR.—

13 (1) IN GENERAL.—After receiving a rec-
14 ommendation to deny access under subsection
15 (b)(1)(B), a National Laboratory shall submit to the
16 Director a notification of the decision of the Na-
17 tional Laboratory to grant or deny access to the
18 premises, information, or technology of the National
19 Laboratory to the sensitive country visitor or as-
20 signee that is the subject of the recommendation.

21 (2) TIMING.—If a National Laboratory decides
22 to grant access to a sensitive country visitor or as-
23 signee despite a recommendation to deny access, the
24 notification under paragraph (1) shall be submitted
25 to the Director before the sensitive country visitor or

1 assignee is granted access to the premises, informa-
2 tion, or technology of the National Laboratory.

3 (d) REPORTS TO CONGRESS.—

4 (1) IN GENERAL.—The Director shall submit to
5 the appropriate committees of Congress an unclassi-
6 fied quarterly report listing each instance in which
7 a National Laboratory indicates in a notification
8 submitted under subsection (c)(1) that the National
9 Laboratory has decided to grant a sensitive country
10 visitor or assignee access to the premises, informa-
11 tion, or technology of the National Laboratory.

12 (2) REQUIREMENT.—Each quarterly report
13 under paragraph (1) shall include the recommenda-
14 tion of the Director under subsection (b)(1)(B) with
15 respect to the applicable sensitive country visitor or
16 assignee.

17 **SEC. 310. CONGRESSIONAL OVERSIGHT OF INTELLIGENCE**
18 **COMMUNITY RISK ASSESSMENTS.**

19 (a) RISK ASSESSMENT DOCUMENTS AND MATE-
20 RIALS.—Except as provided in subsection (b), whenever
21 an element of the intelligence community conducts a risk
22 assessment arising from the mishandling or improper dis-
23 closure of classified information, the Director of National
24 Intelligence shall, not later than 30 days after the date
25 of the commencement of such risk assessment—

1 (1) submit to the congressional intelligence
2 committees copies of such documents and materials
3 as are—

4 (A) within the jurisdiction of such commit-
5 tees; and

6 (B) subject to the risk assessment; and

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

9 (b) EXCEPTION.—If the Director determines, with re-
10 spect to a risk assessment described in subsection (a), that
11 the documents and other materials otherwise subject to
12 paragraph (1) of such subsection (a) are of such a volume
13 that submittal pursuant to such paragraph would be im-
14 practicable, the Director shall—

15 (1) in lieu of submitting copies of such docu-
16 ments and materials, submit a log of such docu-
17 ments and materials; and

18 (2) pursuant to a request by the Select Com-
19 mittee on Intelligence of the Senate or the Perma-
20 nent Select Committee on Intelligence of the House
21 of Representatives for a copy of a document or ma-
22 terial included in such log, submit to such committee
23 such copy.

1 **SEC. 311. INSPECTOR GENERAL REVIEW OF DISSEMINA-**
2 **TION BY FEDERAL BUREAU OF INVESTIGA-**
3 **TION RICHMOND, VIRGINIA, FIELD OFFICE**
4 **OF CERTAIN DOCUMENT.**

5 (a) REVIEW REQUIRED.—Not later than 120 days
6 after the date of the enactment of this Act, the Inspector
7 General of the Department of Justice shall conduct a re-
8 view of the actions and events, including any underlying
9 policy direction, that served as a basis for the January
10 23, 2023, dissemination by the field office of the Federal
11 Bureau of Investigation located in Richmond, Virginia, of
12 a document titled “Interest of Racially or Ethnically Moti-
13 vated Violent Extremists in Radical-Traditionalist Catho-
14 lic Ideology Almost Certainly Presents New Mitigation
15 Opportunities.”.

16 (b) SUBMITTAL TO CONGRESS.—The Inspector Gen-
17 eral of the Department of Justice shall submit to the con-
18 gressional intelligence committees the findings of the In-
19 spector General with respect to the review required by sub-
20 section (a).

21 **SEC. 312. OFFICE OF INTELLIGENCE AND ANALYSIS.**

22 Section 201 of the Homeland Security Act of 2002
23 (6 U.S.C. 121) is amended by adding at the end the fol-
24 lowing:

25 “(h) PROHIBITION.—

1 “(1) DEFINITION.—In this subsection, the term
2 ‘United States person’ means a United States cit-
3 izen, an alien known by the Office of Intelligence
4 and Analysis to be a permanent resident alien, an
5 unincorporated association substantially composed of
6 United States citizens or permanent resident aliens,
7 or a corporation incorporated in the United States,
8 except for a corporation directed and controlled by
9 1 or more foreign governments.

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

12 “(A) IN GENERAL.—Notwithstanding any
13 other provision of law, the Office of Intelligence
14 and Analysis may not engage in the collection
15 of information or intelligence targeting any
16 United States person except as provided in sub-
17 paragraph (B).

18 “(B) EXCEPTION.—Subparagraph (A)
19 shall not apply to any employee, officer, or con-
20 tractor of the Office of Intelligence and Anal-
21 ysis who is responsible for collecting informa-
22 tion from individuals working for a State, local,
23 or Tribal territory government or a private em-
24 ployer.”.

1 “(A) the Committee on the Judiciary of
2 the Senate; and

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

5 “(4) CONGRESSIONAL TRANSPORTATION AND
6 INFRASTRUCTURE COMMITTEES.—The term ‘con-
7 gressional transportation and infrastructure commit-
8 tees’ means—

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

11 “(B) the Committee on Transportation
12 and Infrastructure of the House of Representa-
13 tives.

14 “(5) COVERED FACILITY OR ASSET.—The term
15 ‘covered facility or asset’ means the headquarters
16 compound of the Agency and the property controlled
17 and occupied by the Federal Highway Administra-
18 tion located immediately adjacent to such compound
19 (subject to a risk-based assessment as defined for
20 purposes of this section), or any other installation
21 and protected property of the Agency where the fa-
22 cility or asset—

23 “(A) is identified as high risk and a poten-
24 tial target for unlawful unmanned aircraft ac-
25 tivity by the Director, in coordination with the

1 Secretary of Transportation, with respect to po-
2 tentially affected airspace, through a risk-based
3 assessment for purposes of this section;

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

5 “(C) directly relates to one or more func-
6 tions authorized to be performed by the Agency,
7 pursuant to the National Security Act of 1947
8 (50 U.S.C. 3001 et seq.) or this Act.

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

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

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

20 “(9) RISK-BASED ASSESSMENT.—The term
21 ‘risk-based assessment’ includes an evaluation of
22 threat information specific to a covered facility or
23 asset and, with respect to potential effects on the
24 safety and efficiency of the national airspace system
25 and the needs of national security at each covered

1 facility or asset identified by the Director, an evalua-
2 tion of each of the following factors:

3 “(A) Potential effects on safety, efficiency,
4 and use of the national airspace system, includ-
5 ing potential effects on manned aircraft and un-
6 manned aircraft systems, aviation safety, air-
7 port operations, infrastructure, and air naviga-
8 tion services relating to the use of any system
9 or technology for carrying out the actions de-
10 scribed in subsection (c)(1).

11 “(B) Options for mitigating any identified
12 effects on the national airspace system relating
13 to the use of any system or technology, includ-
14 ing minimizing when possible the use of any
15 system or technology that disrupts the trans-
16 mission of radio or electronic signals, for car-
17 rying out the actions described in subsection
18 (c)(1).

19 “(C) Potential consequences of any actions
20 taken under subsection (c)(1) to the national
21 airspace system and infrastructure, if not miti-
22 gated.

23 “(D) The ability to provide reasonable ad-
24 vance notice to aircraft operators consistent

1 with the safety of the national airspace system
2 and the needs of national security.

3 “(E) The setting and character of any cov-
4 ered facility or asset, including whether it is lo-
5 cated in a populated area or near other struc-
6 tures, and any potential for interference with
7 wireless communications or for injury or dam-
8 age to persons or property.

9 “(F) Potential consequences to national se-
10 curity if threats posed by unmanned aircraft
11 systems or unmanned aircraft are not mitigated
12 or defeated.

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

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

19 “(12) UNMANNED AIRCRAFT AND UNMANNED
20 AIRCRAFT SYSTEM.—The terms ‘unmanned aircraft’
21 and ‘unmanned aircraft system’ have the meanings
22 given such terms in section 44801 of title 49, United
23 States Code.

1 “(13) WIRE COMMUNICATION.—The term ‘wire
2 communication’ has the meaning given such term in
3 section 2510 of title 18, United States Code.

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

11 “(1) such actions described in subsection (c)(1)
12 that are necessary to detect, identify, monitor, track,
13 or mitigate a credible threat (as defined by the Di-
14 rector, in consultation with the Secretary of Trans-
15 portation) that an unmanned aircraft system or un-
16 manned aircraft poses to the safety or security of a
17 covered facility or asset; and

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

19 “(c) ACTIONS.—

20 “(1) ACTIONS DESCRIBED.—The actions de-
21 scribed in this paragraph are the following:

22 “(A) During the operation of the un-
23 manned aircraft system, detect, identify, mon-
24 itor, and track the unmanned aircraft system or
25 unmanned aircraft, without prior consent, in-

1 including by means of intercept or other access of
2 a wire communication, an oral communication,
3 or an electronic communication used to control
4 the unmanned aircraft system or unmanned air-
5 craft.

6 “(B) Warn the operator of the unmanned
7 aircraft system or unmanned aircraft, including
8 by doing so passively or actively, and by direct
9 or indirect physical, electronic, radio, and elec-
10 tromagnetic means.

11 “(C) Disrupt control of the unmanned air-
12 craft system or unmanned aircraft, without
13 prior consent, including by disabling the un-
14 manned aircraft system or unmanned aircraft
15 by intercepting, interfering with, or causing in-
16 terference with wire, oral, electronic, or radio
17 communications used to control the unmanned
18 aircraft system or unmanned aircraft.

19 “(D) Seize or exercise control of the un-
20 manned aircraft system or unmanned aircraft.

21 “(E) Seize or otherwise confiscate the un-
22 manned aircraft system or unmanned aircraft.

23 “(F) Use reasonable force, if necessary, to
24 seize or otherwise disable, damage, or destroy

1 the unmanned aircraft system or unmanned air-
2 craft.

3 “(2) RESEARCH, TESTING, TRAINING, AND
4 EVALUATION.—The Director shall conduct research,
5 testing, and training on, and evaluation of, any
6 equipment, including any electronic equipment, to
7 determine the capability and utility of the equipment
8 prior to the use of the equipment for any action de-
9 scribed in paragraph (1). Personnel and contractors
10 who do not have duties that include the safety, secu-
11 rity, or protection of people, facilities, or assets may
12 engage in research, testing, training, and evaluation
13 activities pursuant to this section.

14 “(3) COORDINATION.—

15 “(A) SECRETARY OF TRANSPORTATION.—
16 The Director shall develop the actions described
17 in paragraph (1) in coordination with the Sec-
18 retary of Transportation.

19 “(B) ADMINISTRATOR OF FEDERAL AVIA-
20 TION ADMINISTRATION.—The Director shall co-
21 ordinate with the Administrator of the Federal
22 Aviation Administration on any action described
23 in paragraphs (1) and (3) so the Administrator
24 may ensure that unmanned aircraft system de-
25 tection and mitigation systems do not adversely

1 affect or interfere with safe airport operations,
2 navigation, air traffic services, or the safe and
3 efficient operation of the national airspace sys-
4 tem.

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

9 “(e) REGULATIONS AND GUIDANCE.—

10 “(1) ISSUANCE.—The Director and the Sec-
11 retary of Transportation may each prescribe regula-
12 tions, and shall each issue guidance, to carry out
13 this section.

14 “(2) COORDINATION.—

15 “(A) REQUIREMENT.—The Director shall
16 coordinate the development of guidance under
17 paragraph (1) with the Secretary of Transpor-
18 tation.

19 “(B) AVIATION SAFETY.—The Director
20 shall coordinate with the Secretary of Transpor-
21 tation and the Administrator of the Federal
22 Aviation Administration before issuing any
23 guidance, or otherwise implementing this sec-
24 tion, so the Administrator may ensure that un-
25 manned aircraft system detection and mitiga-

1 tion systems do not adversely affect or interfere
2 with safe airport operations, navigation, air
3 traffic services, or the safe and efficient oper-
4 ation of the national airspace system.

5 “(f) PRIVACY PROTECTION.—The regulations pre-
6 scribed or guidance issued under subsection (e) shall en-
7 sure that—

8 “(1) the interception or acquisition of, access
9 to, or maintenance or use of, communications to or
10 from an unmanned aircraft system or unmanned air-
11 craft under this section is conducted in a manner
12 consistent with the First and Fourth Amendments
13 to the Constitution of the United States and applica-
14 ble provisions of Federal law;

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

19 “(3) records of such communications are main-
20 tained only for as long as necessary, and in no event
21 for more than 180 days, unless the Director deter-
22 mines that maintenance of such records for a longer
23 period is required under Federal law or necessary
24 for the investigation or prosecution of a violation of

1 law, to fulfill a duty, responsibility, or function of
2 the Agency, or for the purpose of any litigation;

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

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

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

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

17 “(D) would support the enforcement activi-
18 ties of a regulatory agency of the Federal Gov-
19 ernment in connection with a criminal or civil
20 investigation of, or any regulatory, statutory, or
21 other enforcement action relating to, an action
22 described in subsection (c) that is necessary to
23 fulfill a duty, responsibility, or function of the
24 Agency;

1 “(E) is necessary to protect against dan-
2 gerous or unauthorized activity by unmanned
3 aircraft systems or unmanned aircraft;

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

6 “(G) is otherwise required by law.

7 “(g) BUDGET.—

8 “(1) IN GENERAL.—The Director shall submit
9 to the congressional intelligence committees, as a
10 part of the budget requests of the Agency for each
11 fiscal year after fiscal year 2024, a consolidated
12 funding display that identifies the funding source for
13 the actions described in subsection (c)(1) within the
14 Agency.

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

18 “(h) SEMIANNUAL BRIEFINGS AND NOTIFICA-
19 TIONS.—

20 “(1) BRIEFINGS.—Not later than 180 days
21 after the date of the enactment of this section, and
22 semiannually thereafter, the Director shall provide
23 the congressional intelligence committees, the con-
24 gressional judiciary committees, and the congres-
25 sional transportation and infrastructure committees

1 a briefing on the activities carried out pursuant to
2 this section during the period covered by the brief-
3 ing.

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

7 “(3) CONTENTS.—Each briefing under para-
8 graph (1) shall include the following:

9 “(A) Policies, programs, and procedures to
10 mitigate or eliminate effects of such activities
11 on the national airspace system and other crit-
12 ical national transportation infrastructure.

13 “(B) A description of instances in which
14 actions described in subsection (c)(1) have been
15 taken, including all such instances that may
16 have resulted in harm, damage, or loss to a per-
17 son or to private property.

18 “(C) A description of the guidance, poli-
19 cies, or procedures established to address pri-
20 vacy, civil rights, and civil liberties issues impli-
21 cated by the actions allowed under this section,
22 as well as any changes or subsequent efforts
23 that would significantly affect privacy, civil
24 rights, or civil liberties.

1 “(D) A description of options considered
2 and steps taken to mitigate any identified ef-
3 fects on the national airspace system relating to
4 the use of any system or technology, including
5 the minimization of the use of any technology
6 that disrupts the transmission of radio or elec-
7 tronic signals, for carrying out the actions de-
8 scribed in subsection (c)(1).

9 “(E) A description of instances in which
10 communications intercepted or acquired during
11 the course of operations of an unmanned air-
12 craft system or unmanned aircraft were main-
13 tained for more than 180 days or disclosed out-
14 side the Agency.

15 “(F) How the Director and the Secretary
16 of Transportation have informed the public as
17 to the possible use of authorities under this sec-
18 tion.

19 “(G) How the Director and the Secretary
20 of Transportation have engaged with Federal,
21 State, local, territorial, or tribal law enforce-
22 ment agencies to implement and use such au-
23 thorities.

24 “(H) An assessment of whether any gaps
25 or insufficiencies remain in laws, regulations,

1 and policies that impede the ability of the Agen-
2 cy to counter the threat posed by the malicious
3 use of unmanned aircraft systems or unmanned
4 aircraft, and any recommendations to remedy
5 such gaps or insufficiencies.

6 “(4) FORM.—Each briefing under paragraph
7 (1) shall be in unclassified form, but may be accom-
8 panied by an additional classified report.

9 “(5) NOTIFICATIONS.—

10 “(A) COVERED FACILITIES AND ASSETS.—
11 Not later than 30 days before exercising any
12 authority under this section at a covered facility
13 or asset for the first time doing so at such cov-
14 ered facility or asset, the Director shall submit
15 to the congressional intelligence committees—

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

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

21 “(B) DEPLOYMENT OF NEW TECH-
22 NOLOGIES.—

23 “(i) IN GENERAL.—Not later than 30
24 days after deploying any new technology to
25 carry out the actions described in sub-

1 section (c)(1), the Director shall submit to
2 the congressional intelligence committees a
3 notification of the use of such technology.

4 “(ii) CONTENTS.—Each notice sub-
5 mitted pursuant to clause (i) shall include
6 a description of options considered to miti-
7 gate any identified effects on the national
8 airspace system relating to the use of any
9 system or technology, including the mini-
10 mization of the use of any technology that
11 disrupts the transmission of radio or elec-
12 tronic signals, for carrying out the actions
13 described in subsection (c)(1).

14 “(i) RULE OF CONSTRUCTION.—Nothing in this sec-
15 tion may be construed—

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

19 “(2) to vest in the Secretary of Transportation
20 or the Administrator of the Federal Aviation Admin-
21 istration any authority of the Director.

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

1 “(k) TERMINATION.—

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

8 “(2) EXTENSION.—The President may extend
9 by 1 year the termination date specified in para-
10 graph (1) if, before termination, the President cer-
11 tifies to Congress that such extension is in the na-
12 tional security interests of the United States.”.

13 **SEC. 322. CHANGE TO PENALTIES AND INCREASED AVAIL-**
14 **ABILITY OF MENTAL HEALTH TREATMENT**
15 **FOR UNLAWFUL CONDUCT ON CENTRAL IN-**
16 **TELLIGENCE AGENCY INSTALLATIONS.**

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

1 **SEC. 323. MODIFICATIONS TO PROCUREMENT AUTHORI-**
2 **TIES OF THE CENTRAL INTELLIGENCE AGEN-**
3 **CY.**

4 Section 3 of the Central Intelligence Agency Act of
5 1949 (50 U.S.C. 3503) is amended—

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

12 (2) in subsection (d), by striking “in para-
13 graphs” and all that follows through “1947” and in-
14 serting “in sections 3201 through 3204 of title 10,
15 United States Code, shall not be delegable. Each de-
16 termination or decision required by sections 3201
17 through 3204, 3321 through 3323, and 3841 of title
18 10, United States Code”.

19 **SEC. 324. ESTABLISHMENT OF CENTRAL INTELLIGENCE**
20 **AGENCY STANDARD WORKPLACE SEXUAL**
21 **MISCONDUCT COMPLAINT INVESTIGATION**
22 **PROCEDURE.**

23 (a) **WORKPLACE SEXUAL MISCONDUCT DEFINED.—**

24 The term “workplace sexual misconduct”—

1 (1) means unwelcome sexual advances, requests
2 for sexual favors, and other verbal or physical con-
3 duct of a sexual nature when—

4 (A) submission to such conduct is made ei-
5 ther explicitly or implicitly a term or condition
6 of an individual's employment;

7 (B) submission to or rejection of such con-
8 duct by an individual is used as the basis for
9 employment decisions affecting such individual;
10 or

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

15 (2) includes sexual harassment and sexual as-
16 sault.

17 (b) STANDARD COMPLAINT INVESTIGATION PROCE-
18 DURE.—Not later than 90 days after the date of the en-
19 actment of this Act, the Director of the Central Intel-
20 ligence Agency shall—

21 (1) establish a standard workplace sexual mis-
22 conduct complaint investigation procedure;

23 (2) implement the standard workplace sexual
24 misconduct complaint investigation procedure

1 through clear workforce communication and edu-
2 cation on the procedure; and

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

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

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

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

18 (A) documentation of the complaint;

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

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

23 (D) preliminary investigation of the com-
24 plaint;

1 (3) set forth standard criteria for determining
2 whether a complaint of workplace sexual misconduct
3 will be referred to law enforcement and the time-
4 frame within which such a referral shall occur; and

5 (4) for any complaint not referred to law en-
6 forcement, set forth standard criteria for deter-
7 mining—

8 (A) whether a complaint has been substan-
9 tiated; and

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

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

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

20 (A) complaints referred to law enforce-
21 ment; and

22 (B) complaints substantiated.

23 (2) For each complaint described in paragraph
24 (1) that is substantiated, a description of the dis-
25 ciplinary action taken by the Director.

1 **SEC. 325. PAY CAP FOR DIVERSITY, EQUITY, AND INCLU-**
2 **SION STAFF AND CONTRACT EMPLOYEES OF**
3 **THE CENTRAL INTELLIGENCE AGENCY.**

4 (a) **IN GENERAL.**—Notwithstanding any other provi-
5 sion of law—

6 (1) the annual rate of basic pay for a staff em-
7 ployee of the Central Intelligence Agency with the
8 duties described in subsection (b) shall not exceed
9 the annual rate of basic pay for an officer of the Di-
10 rectorate of Operations in the Clandestine Service
11 Trainee program of the Agency; and

12 (2) the Director of the Central Intelligence
13 Agency shall ensure that no contract employee per-
14 forming duties described in subsection (b) under an
15 Agency contract receives an annual amount for per-
16 forming such duties that exceeds the annual rate of
17 basic pay described in paragraph (1).

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

20 (1) Developing, refining, and implementing di-
21 versity, equity, and inclusion policy.

22 (2) Leading working groups and councils to de-
23 velop diversity, equity, and inclusion goals and objec-
24 tives to measure performance and outcomes.

1 (3) Creating and implementing diversity, equity,
2 and inclusion education, training courses, and work-
3 shops for staff and contract employees.

4 (c) APPLICABILITY TO CURRENT EMPLOYEES.—

5 (1) STAFF EMPLOYEES.—Any staff employee of
6 the Central Intelligence Agency in a position with
7 duties described in subsection (b) receiving an an-
8 nual rate of basic pay as of the date of the enact-
9 ment of this Act that exceeds the rate allowed under
10 subsection (a) shall be reassigned to another position
11 not later than 180 days after such date.

12 (2) CONTRACT EMPLOYEES.—Any contract em-
13 ployee of the Central Intelligence Agency performing
14 duties described in subsection (b) receiving an an-
15 nual amount under an Agency contract for per-
16 forming such duties as of the date of the enactment
17 of this Act that exceeds the rate allowed under sub-
18 section (b) shall be reassigned to another position
19 not later than 180 days after such date.

1 **TITLE IV—MATTERS CON-**
2 **CERNING FOREIGN COUN-**
3 **TRIES**

4 **Subtitle A—People’s Republic of**
5 **China**

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

9 (a) DEFINITIONS.—In this section:

10 (1) APPROPRIATE COMMITTEES OF CON-
11 GRESS.—The term “appropriate committees of Con-
12 gress” means—

13 (A) the congressional intelligence commit-
14 tees;

15 (B) the Committee on Foreign Relations
16 and the Subcommittee on Defense of the Com-
17 mittee on Appropriations of the Senate; and

18 (C) the Committee on Foreign Affairs and
19 the Subcommittee on Defense of the Committee
20 on Appropriations of the House of Representa-
21 tives.

22 (2) ATROCITY.—The term “atrocitv”—

23 (A) means a crime against humanity, geno-
24 cide, or a war crime; and

1 (B) when used with respect to the People's
2 Republic of China, means an atrocity that is
3 committed by an individual who is—

4 (i) a member of People's Liberation
5 Army, or the security or other defense
6 services, including the Ministry of State
7 Security, the Ministry of Public Security,
8 and the United Front Work Department,
9 of the People's Republic of China;

10 (ii) an employee of any other element
11 of the Government of the People's Republic
12 of China, including the regional govern-
13 ments of Xinjiang, Tibet, and Hong Kong;

14 (iii) a member of the Chinese Com-
15 munist Party; or

16 (iv) an agent or contractor of an indi-
17 vidual specified in subparagraph (A), (B),
18 or (C).

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

22 (4) FOREIGN PERSON.—The term “foreign per-
23 son” means—

24 (A) any person or entity that is not a
25 United States person; or

1 (B) any entity not organized under the
2 laws of the United States or of any jurisdiction
3 within the United States.

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

8 (b) INTELLIGENCE COMMUNITY COORDINATOR FOR
9 ACCOUNTABILITY OF ATROCITIES OF THE PEOPLE’S RE-
10 PUBLIC OF CHINA.—

11 (1) DESIGNATION.—Not later than 90 days
12 after the date of the enactment of this Act, the Di-
13 rector of National Intelligence shall designate a sen-
14 ior official of the Office of the Director of National
15 Intelligence to serve as the intelligence community
16 coordinator for accountability of atrocities of the
17 People’s Republic of China (in this section referred
18 to as the “Coordinator”).

19 (2) DUTIES.—The Coordinator shall lead the
20 efforts of and coordinate and collaborate with the in-
21 telligence community with respect to the following:

22 (A) Identifying and addressing any gaps in
23 intelligence collection relating to atrocities of
24 the People’s Republic of China, including by
25 recommending the modification of the priorities

1 of the intelligence community with respect to
2 intelligence collection and by utilizing informal
3 processes and collaborative mechanisms with
4 key elements of the intelligence community to
5 increase collection on atrocities of the People's
6 Republic of China.

7 (B) Prioritizing and expanding the intel-
8 ligence analysis with respect to ongoing atroc-
9 ities of the People's Republic of China and dis-
10 seminating within the United States Govern-
11 ment intelligence relating to the identification
12 and activities of foreign persons suspected of
13 being involved with or providing support to
14 atrocities of the People's Republic of China, in-
15 cluding genocide and forced labor practices in
16 Xinjiang, in order to support the efforts of
17 other Federal agencies, including the Depart-
18 ment of State, the Department of the Treasury,
19 the Office of Foreign Assets Control, the De-
20 partment of Commerce, the Bureau of Industry
21 and Security, U.S. Customs and Border Protec-
22 tion, and the National Security Council, to hold
23 the People's Republic of China accountable for
24 such atrocities.

1 (C) Increasing efforts to declassify and
2 share with the people of the United States and
3 the international community information re-
4 garding atrocities of the People’s Republic of
5 China in order to expose such atrocities and
6 counter the disinformation and misinformation
7 campaign by the People’s Republic of China to
8 deny such atrocities.

9 (D) Documenting and storing intelligence
10 and other unclassified information that may be
11 relevant to preserve as evidence of atrocities of
12 the People’s Republic of China for future ac-
13 countability, and ensuring that other relevant
14 Federal agencies, including the Atrocities Early
15 Warning Task Force, receive appropriate sup-
16 port from the intelligence community with re-
17 spect to the collection, analysis, preservation,
18 and, as appropriate, dissemination, of intel-
19 ligence related to atrocities of the People’s Re-
20 public of China, which may include the informa-
21 tion from the annual report required by section
22 6504 of the Intelligence Authorization Act for
23 Fiscal Year 2023 (Public Law 117–263).

24 (E) Sharing information with the Forced
25 Labor Enforcement Task Force, established

1 under section 741 of the United States-Mexico-
2 Canada Agreement Implementation Act (19
3 U.S.C. 4681), the Department of Commerce,
4 and the Department of the Treasury for the
5 purposes of entity listings and sanctions.

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

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

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

19 (4) ANNUAL REPORT TO CONGRESS.—

20 (A) REPORTS REQUIRED.—Not later than
21 May 1, 2024, and annually thereafter until May
22 1, 2034, the Director shall submit to the appro-
23 priate committees of Congress a report detail-
24 ing, for the year covered by the report—

1 (i) the analytical findings, changes in
2 collection, and other activities of the intel-
3 ligence community with respect to ongoing
4 atrocities of the People's Republic of
5 China;

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

9 (I) providing support to Federal
10 agencies to hold the People's Republic
11 of China accountable for such atroc-
12 ities; and

13 (II) sharing information with the
14 people of the United States to counter
15 the disinformation and misinformation
16 campaign by the People's Republic of
17 China to deny such atrocities; and

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

20 (B) FORM.—Each report submitted under
21 subparagraph (A) may be submitted in classi-
22 fied form, consistent with the protection of in-
23 telligence sources and methods.

1 (c) SUNSET.—This section shall cease to have effect
2 on the date that is 10 years after the date of the enact-
3 ment of this Act.

4 **SEC. 402. INTERAGENCY WORKING GROUP AND REPORT ON**
5 **THE MALIGN EFFORTS OF THE PEOPLE'S RE-**
6 **PUBLIC OF CHINA IN AFRICA.**

7 (a) ESTABLISHMENT.—

8 (1) IN GENERAL.—The Director of National In-
9 telligence, in consultation with such heads of ele-
10 ments of the intelligence community as the Director
11 considers appropriate, shall establish an interagency
12 working group within the intelligence community to
13 analyze the tactics and capabilities of the People's
14 Republic of China in Africa.

15 (2) ESTABLISHMENT FLEXIBILITY.—The work-
16 ing group established under paragraph (1) may be—

17 (A) independently established; or

18 (B) to avoid redundancy, incorporated into
19 existing working groups or cross-intelligence ef-
20 forts within the intelligence community.

21 (b) REPORT.—

22 (1) IN GENERAL.—Not later than 120 days
23 after the date of the enactment of this Act, and
24 twice annually thereafter, the working group estab-
25 lished under subsection (a) shall submit to the con-

1 gressional intelligence committees a report on the
2 specific tactics and capabilities of the People's Re-
3 public of China in Africa.

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

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

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

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

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

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

24 (D) A description of actions taken by the
25 intelligence community to counter such efforts.

1 heads of elements of the intelligence community as the As-
2 sistant Secretary considers relevant, shall submit to the
3 congressional intelligence committees the following:

4 (1) A comprehensive assessment that identifies
5 critical areas in the security, diplomatic, economic,
6 financial, technological, scientific, commercial, aca-
7 demic, and cultural spheres in which the United
8 States does not enjoy a reciprocal relationship with
9 the People's Republic of China.

10 (2) A comprehensive assessment that describes
11 how the lack of reciprocity between the People's Re-
12 public of China and the United States in the areas
13 identified in the assessment required by paragraph
14 (1) provides advantages to the People's Republic of
15 China.

16 (b) FORM OF ASSESSMENTS.—

17 (1) CRITICAL AREAS.—The assessment required
18 by subsection (a)(1) shall be submitted in unclassi-
19 fied form.

20 (2) ADVANTAGES.—The assessment required by
21 subsection (a)(2) shall be submitted in classified
22 form.

1 **SEC. 405. ANNUAL BRIEFING ON INTELLIGENCE COMMU-**
2 **NITY EFFORTS TO IDENTIFY AND MITIGATE**
3 **CHINESE COMMUNIST PARTY POLITICAL IN-**
4 **FLUENCE OPERATIONS AND INFORMATION**
5 **WARFARE AGAINST THE UNITED STATES.**

6 (a) DEFINITIONS.—In this section:

7 (1) CHINESE ENTITIES ENGAGED IN POLITICAL
8 INFLUENCE OPERATIONS AND INFORMATION WAR-
9 FARE.—The term “Chinese entities engaged in polit-
10 ical influence operations and information warfare”
11 means all of the elements of the Government of the
12 People’s Republic of China and the Chinese Com-
13 munist Party involved in information warfare oper-
14 ations, such as—

15 (A) the Ministry of State Security;

16 (B) the intelligence services of the People’s
17 Republic of China;

18 (C) the United Front Work Department
19 and other united front organs;

20 (D) state-controlled media systems, such
21 as the China Global Television Network
22 (CGTN); and

23 (E) any entity involved in information war-
24 fare operations by demonstrably and inten-
25 tionally disseminating false information and
26 propaganda of the Government of the People’s

1 Republic of China or the Chinese Communist
2 Party.

3 (2) POLITICAL INFLUENCE OPERATION.—The
4 term “political influence operation” means a coordi-
5 nated and often concealed application of
6 disinformation, press manipulation, economic coer-
7 cion, targeted investments, corruption, or academic
8 censorship, which are often intended—

9 (A) to coerce and corrupt United States in-
10 terests, values, institutions, or individuals; and

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

16 (b) BRIEFING REQUIRED.—Not later than 120 days
17 after the date of the enactment of this Act and annually
18 thereafter until the date that is 5 years after the date of
19 the enactment of this Act, the Director of the Foreign Ma-
20 lign Influence Center shall, in collaboration with the heads
21 of the elements of the intelligence community, provide the
22 congressional intelligence committees a classified briefing
23 on the ways in which the relevant elements of the intel-
24 ligence community are working internally and coordi-
25 nating across the intelligence community to identify and

1 mitigate the actions of Chinese entities engaged in political
2 influence operations and information warfare against the
3 United States, including against United States persons.

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

6 (1) The Government of the People’s Republic of
7 China and the Chinese Communist Party tactics,
8 tools, and entities that spread disinformation, misin-
9 formation, and malign information and conduct in-
10 fluence operations, information campaigns, or other
11 propaganda efforts.

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

21 (3) The actions of the Foreign Malign Influence
22 Center to conduct outreach to identify and counter
23 tactics, tools, and entities described in paragraph (1)
24 by sharing information with allies and partners of
25 the United States, State and local governments, the

1 business community, and civil society that exposes
2 the political influence operations and information op-
3 erations of the Government of the People’s Republic
4 of China or the Chinese Communist Party carried
5 out against individuals and entities in the United
6 States.

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

10 (a) DEFINITION OF COUNTRY OF CONCERN.—In this
11 section, the term “country of concern” has the meaning
12 given that term in section 1(m)(1) of the State Depart-
13 ment Basic Authorities Act of 1956 (22 U.S.C.
14 2651a(m)(1)).

15 (b) ASSESSMENT.—The Director of National Intel-
16 ligence, in coordination with such other heads of the ele-
17 ments of the intelligence community as the Director con-
18 siders appropriate and the Secretary of Defense, shall con-
19 duct an assessment of the threat posed to United States
20 ports by cranes manufactured by countries of concern and
21 commercial entities of those countries, including the
22 Shanghai Zhenhua Heavy Industries Co. (ZPMC).

23 (c) REPORT AND BRIEFING.—

24 (1) IN GENERAL.—Not later than 180 days
25 after the date of the enactment of this Act, the Di-

1 rector of National Intelligence shall submit a report
2 and provide a briefing to Congress on the findings
3 of the assessment required by subsection (b).

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

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

13 **Subtitle B—Russian Federation**

14 **SEC. 411. ASSESSMENT OF LESSONS LEARNED BY INTEL-** 15 **LIGENCE COMMUNITY WITH RESPECT TO** 16 **CONFLICT IN UKRAINE.**

17 (a) IN GENERAL.—Not later than 180 days after the
18 date of the enactment of this Act and semiannually there-
19 after for 3 years, the Director of National Intelligence
20 shall produce and submit to the congressional intelligence
21 committees an assessment of the lessons learned by the
22 intelligence community with respect to the ongoing war
23 in Ukraine, particularly in regards to the quality and time-
24 liness of the information and intelligence support provided
25 by the United States to Ukraine.

1 (b) FORM.—The assessment submitted pursuant to
2 subsection (a) shall be submitted in unclassified form, but
3 may include a classified annex.

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

6 (a) NATIONAL INTELLIGENCE ESTIMATE RE-
7 QUIRED.—Not later than 180 days after the date of the
8 enactment of this Act, the Director of National Intel-
9 ligence shall produce and submit to the congressional in-
10 telligence committees a national intelligence estimate on
11 the implications of the ongoing war in Ukraine with re-
12 spect to a long-term United States and North Atlantic
13 Treaty Organization confrontation with Russia, including
14 the continued threat to the United States, the North At-
15 lantic Treaty Organization, and other allies of the United
16 States from the conventional and strategic military forces,
17 the intelligence activities, and the malign influence cam-
18 paigns of Russia.

19 (b) ELEMENTS.—The national intelligence estimate
20 produced pursuant to subsection (a) shall include the fol-
21 lowing:

22 (1) An assessment of the efficacy of the sanc-
23 tions regime in effect on the day before the date of
24 the enactment of this Act that is imposed upon Rus-

1 sia as a result of its illegal and unjustified invasion
2 of Ukraine, including—

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

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

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

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

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

22 (5) An assessment of other significant countries
23 that have not joined the sanctions regime against
24 Russia, why they have not done so, and what might
25 induce them to change this policy.

1 (c) FORM.—The national intelligence estimate sub-
2 mitted pursuant to subsection (a) shall be submitted in
3 unclassified form, but may include a classified annex.

4 **Subtitle C—Other Foreign**
5 **Countries**

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

8 (a) IN GENERAL.—Not later than 120 days after the
9 date of the enactment of this Act, the Director of National
10 Intelligence shall submit to the congressional intelligence
11 committees a report on efforts by the Maduro regime in
12 Venezuela to detain United States citizens and lawful per-
13 manent residents.

14 (b) ELEMENTS.—The report required by subsection
15 (a) shall include, regarding the arrest, capture, detain-
16 ment, or imprisonment of United States citizens and law-
17 ful permanent residents, the following:

18 (1) The names, positions, and institutional af-
19 filiation of Venezuelan individuals, or those acting
20 on their behalf, who have engaged in such activities.

21 (2) A description of any role played by
22 transnational criminal organizations, and an identi-
23 fication of such organizations.

1 **TITLE V—MATTERS PERTAINING**
2 **TO UNITED STATES ECO-**
3 **NOMIC AND EMERGING TECH-**
4 **NOLOGY COMPETITION WITH**
5 **UNITED STATES ADVER-**
6 **SARIES**

7 **Subtitle A—General Matters**

8 **SEC. 501. OFFICE OF GLOBAL COMPETITION ANALYSIS.**

9 (a) DEFINITIONS.—In this section:

10 (1) EXECUTIVE AGENCY.—The term “Executive
11 agency” has the meaning given such term in section
12 105 of title 5, United States Code.

13 (2) OFFICE.—The term “Office” means the Of-
14 fice of Global Competition Analysis established
15 under subsection (b).

16 (b) ESTABLISHMENT.—

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

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

21 (A) To carry out a program of analysis rel-
22 evant to United States leadership in science,
23 technology, and innovation sectors critical to
24 national security and economic prosperity rel-
25 ative to other countries, particularly those coun-

1 tries that are strategic competitors of the
2 United States.

3 (B) To support policy development and de-
4 cision making across the Federal Government
5 to ensure United States leadership in science,
6 technology, and innovation sectors critical to
7 national security and economic prosperity re-
8 lative to other countries, particularly those coun-
9 tries that are strategic competitors of the
10 United States.

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

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

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

19 (2) conduct long- and short-term analyses re-
20 garding—

21 (A) United States policies that enable tech-
22 nological competitiveness relative to those of
23 other countries, particularly with respect to
24 countries that are strategic competitors of the
25 United States;

1 (B) United States science and technology
2 ecosystem elements, including regional and na-
3 tional research development and capacity, tech-
4 nology innovation, and science and engineering
5 education and research workforce, relative to
6 those of other countries, particularly with re-
7 spect to countries that are strategic competitors
8 of the United States;

9 (C) United States technology development,
10 commercialization, and advanced manufacturing
11 ecosystem elements, including supply chain re-
12 siliency, scale-up manufacturing testbeds, ac-
13 cess to venture capital and financing, technical
14 and entrepreneurial workforce, and production,
15 relative to those of other countries, particularly
16 with respect to countries that are strategic com-
17 petitors of the United States;

18 (D) United States competitiveness in tech-
19 nology and innovation sectors critical to na-
20 tional security and economic prosperity relative
21 to other countries, including the availability and
22 scalability of United States technology in such
23 sectors abroad, particularly with respect to
24 countries that are strategic competitors of the
25 United States;

1 (E) trends and trajectories, including rate
2 of change in technologies, related to technology
3 and innovation sectors critical to national secu-
4 rity and economic prosperity;

5 (F) threats to United States national secu-
6 rity interests as a result of any foreign coun-
7 try's dependence on technologies of strategic
8 competitors of the United States; and

9 (G) threats to United States interests
10 based on dependencies on foreign technologies
11 critical to national security and economic pros-
12 perity;

13 (3) solicit input on technology and economic
14 trends, data, and metrics from relevant private sec-
15 tor stakeholders, including entities involved in fi-
16 nancing technology development and commercializa-
17 tion, and engage with academia to inform the anal-
18 yses under paragraph (2); and

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

23 (d) DETERMINATION OF PRIORITIES.—On a periodic
24 basis, the Director of the Office of Science and Technology
25 Policy, the Assistant to the President for Economic Policy,

1 and the Assistant to the President for National Security
2 Affairs shall, in coordination with such heads of Executive
3 agencies as the Director of the Office of Science and Tech-
4 nology Policy and such Assistants jointly consider appro-
5 priate, jointly determine the priorities of the Office with
6 respect to subsection (b)(2)(A), considering, as may be ap-
7 propriate, the strategies and reports under subtitle B of
8 title VI of the Research and Development, Competition,
9 and Innovation Act (Public Law 117–167).

10 (e) ADMINISTRATION.—Subject to the availability of
11 appropriations, to carry out the purposes set forth under
12 subsection (b)(2), the Office shall enter into an agreement
13 with a federally funded research and development center,
14 a university-affiliated research center, or a consortium of
15 federally funded research and development centers and
16 university-affiliated research centers.

17 (f) ACQUISITION, ACCESS, USE, AND HANDLING OF
18 DATA OR INFORMATION.—In carrying out the activities
19 under subsection (c), the Office—

20 (1) shall acquire, access, use, and handle data
21 or information in a manner consistent with applica-
22 ble provisions of law and policy, including laws and
23 policies providing for the protection of privacy and
24 civil liberties, and subject to any restrictions re-
25 quired by the source of the information;

1 (2) shall have access, upon written request, to
2 all information, data, or reports of any Executive
3 agency that the Office determines necessary to carry
4 out the activities under subsection (c), provided that
5 such access is—

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

11 (B) consistent with due regard for the pro-
12 tection from unauthorized disclosure of classi-
13 fied information relating to sensitive intelligence
14 sources and methods or other exceptionally sen-
15 sitive matters; and

16 (3) may obtain commercially available informa-
17 tion that may not be publicly available.

18 (g) DETAILEE SUPPORT.—Consistent with applicable
19 law, including sections 1341, 1517, and 1535 of title 31,
20 United States Code, and section 112 of title 3, United
21 States Code, the head of a department or agency within
22 the executive branch of the Federal Government may de-
23 tail personnel to the Office in order to assist the Office
24 in carrying out any activity under subsection (c), con-
25 sistent with the priorities determined under subsection (d).

1 (h) ANNUAL REPORT.—Not less frequently than once
2 each year, the Office shall submit to Congress a report
3 on the activities of the Office under this section, including
4 a description of the priorities under subsection (d) and any
5 support, disaggregated by Executive agency, provided to
6 the Office consistent with subsection (g) in order to ad-
7 vance those priorities.

8 (i) PLANS.—Before establishing the Office under
9 subsection (b)(1), the President shall submit to the appro-
10 priate committees of Congress a report detailing plans
11 for—

12 (1) the administrative structure of the Office,
13 including—

14 (A) a detailed spending plan that includes
15 administrative costs; and

16 (B) a disaggregation of costs associated
17 with carrying out subsection (e);

18 (2) ensuring consistent and sufficient funding
19 for the Office; and

20 (3) coordination between the Office and rel-
21 evant Executive agencies and offices.

22 (j) AUTHORIZATION OF APPROPRIATIONS.—There is
23 authorized to be appropriated to carry out this section
24 \$20,000,000 for fiscal year 2024.

1 (k) FUNDING.—This section shall be carried out
2 using amounts appropriated on or after the date of the
3 enactment of this Act.

4 **SEC. 502. ASSIGNMENT OF DETAILEES FROM INTEL-**
5 **LIGENCE COMMUNITY TO DEPARTMENT OF**
6 **COMMERCE.**

7 (a) AUTHORITY.—In order to better facilitate the
8 sharing of actionable intelligence on foreign adversary in-
9 tent, capabilities, threats, and operations that pose a
10 threat to the interests or security of the United States,
11 particularly as they relate to the procurement, develop-
12 ment, and use of dual-use and emerging technologies, the
13 Director of National Intelligence may assign or facilitate
14 the assignment of members from across the intelligence
15 community to serve as detailees to the Bureau of Industry
16 and Security of the Department of Commerce.

17 (b) ASSIGNMENT.—Detailees assigned pursuant to
18 subsection (a) shall be drawn from such elements of the
19 intelligence community as the Director considers appro-
20 priate, in consultation with the Secretary of Commerce.

21 (c) EXPERTISE.—The Director shall ensure that
22 detailees assigned pursuant to subsection (a) have subject
23 matter expertise on countries of concern, including China,
24 Iran, North Korea, and Russia, as well as functional areas
25 such as illicit procurement, counterproliferation, emerging

1 and foundational technology, economic and financial intel-
 2 ligence, information and communications technology sys-
 3 tems, supply chain vulnerability, and counterintelligence.

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

8 **SEC. 503. THREATS POSED BY INFORMATION AND COMMU-**
 9 **NICATIONS TECHNOLOGY AND SERVICES**
 10 **TRANSACTIONS AND OTHER ACTIVITIES.**

11 (a) DEFINITIONS.—In this section:

12 (1) COVERED TRANSACTION.—The term “cov-
 13 ered transaction” means a transaction reviewed
 14 under authority established under Executive Order
 15 13873, Executive Order 13984, Executive Order
 16 14034, or any successor order.

17 (2) EMERGING AND FOUNDATIONAL TECH-
 18 NOLOGIES.—The term “emerging and foundational
 19 technologies” means emerging and foundational
 20 technologies described in section 1758(a)(1) of the
 21 Export Control Reform Act of 2018 (50 U.S.C.
 22 4817(a)(1)).

23 (3) EXECUTIVE ORDER 13873.—The term “Ex-
 24 ecutive Order 13873” means Executive Order 13873
 25 (84 Fed. Reg. 22689; relating to securing informa-

1 tion and communications technology and services
2 supply chain).

3 (4) EXECUTIVE ORDER 13984.—The term “Ex-
4 ecutive Order 13984” means Executive Order 13984
5 (86 Fed. Reg. 6837; relating to taking additional
6 steps to address the national emergency with respect
7 to significant malicious cyber-enabled activities).

8 (5) EXECUTIVE ORDER 14034.—The term “Ex-
9 ecutive Order 14034” means Executive Order 14034
10 (84 Fed. Reg. 31423; relating to protecting Ameri-
11 cans’ sensitive data from foreign adversaries).

12 (6) SIGNIFICANT TRANSACTION.—The term
13 “significant transaction” means a covered trans-
14 action that—

15 (A) involves emerging or foundational tech-
16 nologies;

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

19 (C) involves—

20 (i) an individual who acts as an agent,
21 representative, or employee, or any indi-
22 vidual who acts in any other capacity at
23 the order, request, or under the direction
24 or control, of a foreign adversary or of an
25 individual whose activities are directly or

1 indirectly supervised, directed, controlled,
2 financed, or subsidized in whole or in ma-
3 jority part by a foreign adversary;

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

7 (iii) any corporation, partnership, as-
8 sociation, or other organization organized
9 under the laws of a nation-state controlled
10 by a foreign adversary; or

11 (iv) any corporation, partnership, as-
12 sociation, or other organization, wherever
13 organized or doing business, that is owned
14 or controlled by a foreign adversary.

15 (b) THREAT ASSESSMENT BY DIRECTOR OF NA-
16 TIONAL INTELLIGENCE.—

17 (1) IN GENERAL.—The Director of National In-
18 telligence shall expeditiously carry out a threat as-
19 sessment of each significant transaction.

20 (2) IDENTIFICATION OF GAPS.—Each assess-
21 ment required by paragraph (1) shall include the
22 identification of any recognized gaps in the collection
23 of intelligence relevant to the assessment.

24 (3) VIEWS OF INTELLIGENCE COMMUNITY.—
25 The Director of National Intelligence shall seek and

1 incorporate into each assessment required by para-
2 graph (1) the views of all affected or appropriate
3 elements of the intelligence community with respect
4 to the significant transaction or class of significant
5 transactions.

6 (4) PROVISION OF ASSESSMENT.—The Director
7 of National Intelligence shall provide an assessment
8 required by paragraph (1) to such agency heads and
9 committees of Congress as the Director considers
10 appropriate, as necessary, to implement Executive
11 Order 13873, Executive Order 13984, Executive
12 Order 14034, or any successor order.

13 (c) INTERACTION WITH INTELLIGENCE COMMU-
14 NITY.—

15 (1) IN GENERAL.—The Director of National In-
16 telligence shall ensure that the intelligence commu-
17 nity remains engaged in the collection, analysis, and
18 dissemination to such agency heads as the Director
19 considers appropriate of any additional relevant in-
20 formation that may become available during the
21 course of any investigation or review process con-
22 ducted under authority established under Executive
23 Order 13873, Executive Order 13984, Executive
24 Order 14034, or any successor order.

1 (2) ELEMENTS.—The collection, analysis, and
2 dissemination of information described in paragraph
3 (1) shall include routine assessments of the fol-
4 lowing:

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

8 (B) Supply chains and procurement net-
9 works associated with the procurement of
10 emerging and foundational technologies by for-
11 eign adversaries.

12 (C) Emerging and foundational tech-
13 nologies pursued by foreign adversaries, includ-
14 ing information on prioritization, spending, and
15 technology transfer measures.

16 (D) The intent, capability, and operations
17 of the use by malicious cyber actors of infra-
18 structure as a service (IaaS) against the United
19 States.

20 (E) The impact on the intelligence commu-
21 nity of a significant transaction or class of sig-
22 nificant transactions.

23 (d) INFORMATION IN CIVIL ACTIONS.—

24 (1) PROTECTED INFORMATION IN CIVIL AC-
25 TIONS.—If a civil action challenging an action or

1 finding under Executive Order 13873, Executive
2 Order 13984, Executive Order 14034, or any suc-
3 cessor order is brought, and the court determines
4 that protected information in the administrative
5 record relating to the action or finding, including
6 classified or other information subject to privilege or
7 protections under any provision of law, is necessary
8 to resolve the action, that information shall be sub-
9 mitted ex parte and in camera to the court and the
10 court shall maintain that information under seal.
11 This paragraph does not confer or imply any right
12 to judicial review.

13 (2) NONAPPLICABILITY OF USE OF INFORMA-
14 TION PROVISIONS.—The use of information provi-
15 sions of sections 106, 305, 405, and 706 of the For-
16 eign Intelligence Surveillance Act of 1978 (50
17 U.S.C. 1806, 1825, 1845, and 1881e) shall not
18 apply in a civil action described in paragraph (1).

19 (e) RULE OF CONSTRUCTION CONCERNING RIGHT TO
20 ACCESS.—No provision of this section may be construed
21 to create a right to obtain access to information in the
22 possession of the Federal Government that was considered
23 by the Secretary of Commerce under authority established
24 under Executive Order 13873, Executive Order 13984,
25 Executive Order 14034, or any successor order, including

1 any classified information or sensitive but unclassified in-
2 formation.

3 (f) ADMINISTRATIVE RECORD.—The following infor-
4 mation may be included in the administrative record relat-
5 ing to an action or finding described in subsection (d)(1)
6 and shall be submitted only to the court ex parte and in
7 camera:

8 (1) Sensitive security information, as defined in
9 section 1520.5 of title 49, Code of Federal Regula-
10 tions.

11 (2) Privileged law enforcement information.

12 (3) Information obtained or derived from any
13 activity authorized under the Foreign Intelligence
14 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.),
15 except that, with respect to such information, sub-
16 sections (c), (e), (f), (g), and (h) of section 106 (50
17 U.S.C. 1806), subsections (d), (f), (g), (h), and (i)
18 of section 305 (50 U.S.C. 1825), subsections (e),
19 (e), (f), (g), and (h) of section 405 (50 U.S.C.
20 1845), and section 706 (50 U.S.C. 1881e) of that
21 Act shall not apply.

22 (4) Information subject to privilege or protec-
23 tion under any other provision of law, including the
24 Currency and Foreign Transactions Reporting Act
25 of 1970 (31 U.S.C. 5311 et seq.).

1 (g) TREATMENT CONSISTENT WITH SECTION.—Any
 2 information that is part of the administrative record filed
 3 ex parte and in camera under subsection (d)(1), or cited
 4 by the court in any decision in a civil action described in
 5 such subsection, shall be treated by the court consistent
 6 with the provisions of this section. In no event shall such
 7 information be released to the petitioner or as part of the
 8 public record.

9 (h) INAPPLICABILITY OF FREEDOM OF INFORMATION
 10 ACT.—Any information submitted to the Federal Govern-
 11 ment by a party to a covered transaction in accordance
 12 with this section, as well as any information the Federal
 13 Government may create relating to review of the covered
 14 transaction, is exempt from disclosure under section 552
 15 of title 5, United States Code (commonly referred to as
 16 the “Freedom of Information Act”).

17 **SEC. 504. REVISION OF REGULATIONS DEFINING SENSITIVE**
 18 **NATIONAL SECURITY PROPERTY FOR COM-**
 19 **MITTEE ON FOREIGN INVESTMENT IN THE**
 20 **UNITED STATES REVIEWS.**

21 Not later than 180 days after the date of the enact-
 22 ment of this Act, the Secretary of the Treasury shall revise
 23 section 802.211 of title 31, Code of Federal Regulations,
 24 to expand the definition of “covered real estate”, such as
 25 by treating facilities and property of elements of the intel-

1 ligence community and National Laboratories (as defined
2 in section 2 of the Energy Policy Act of 2005 (42 U.S.C.
3 15801)) comparably to military installations.

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

7 (a) DEFINITIONS.—In this section:

8 (1) EMERGING AND FOUNDATIONAL TECH-
9 NOLOGIES.—The term “emerging and foundational
10 technologies” includes technologies identified under
11 section 1758(a)(1) of the Export Control Reform
12 Act of 2018 (50 U.S.C. 4817(a)(1)).

13 (2) FOREIGN ADVERSARY.—The term “foreign
14 adversary” means any foreign government, foreign
15 regime, or foreign nongovernment person determined
16 by the Director of National Intelligence to have en-
17 gaged in a long-term pattern or serious instances of
18 conduct significantly adverse to the national security
19 of the United States or the security and safety of
20 United States persons.

21 (b) COLLECTION, ANALYSIS, AND DISSEMINATION
22 REQUIRED.—

23 (1) IN GENERAL.—The Director of National In-
24 telligence—

1 (A) is authorized to collect, retain, analyze,
2 and disseminate information or intelligence nec-
3 essary to support the missions of the Depart-
4 ment of Commerce, including with respect to
5 the administration of export controls pursuant
6 to the Export Control Reform Act of 2018 (50
7 U.S.C. 4801 et seq.); and

8 (B) shall, through regular consultation
9 with the Secretary of Commerce, ensure that
10 the intelligence community is engaged in such
11 collection, retention, analysis, and dissemina-
12 tion.

13 (2) INFORMATION TO BE COLLECTED, ANA-
14 LYZED, AND DISSEMINATED.—The information to be
15 collected, analyzed, and disseminated under sub-
16 section (a) shall include information relating to the
17 following:

18 (A) The intent, capability, and operations
19 of foreign adversaries with respect to items
20 under consideration to be controlled pursuant to
21 the authority provided by part I of the Export
22 Control Reform Act of 2018 (50 U.S.C. 4811
23 et seq.).

1 (B) Attempts by foreign adversaries to cir-
2 cumvent controls on items imposed pursuant to
3 that part.

4 (C) Supply chains and procurement net-
5 works associated with procurement and develop-
6 ment of emerging and foundational technologies
7 by foreign adversaries.

8 (D) Emerging and foundational tech-
9 nologies pursued by foreign adversaries, includ-
10 ing relevant information on prioritization,
11 spending, and technology transfer measures
12 with respect to such technologies.

13 (E) The scope and application of the ex-
14 port control systems of foreign countries, in-
15 cluding decisions with respect to individual ex-
16 port transactions.

17 (F) Corporate and contractual relation-
18 ships, ownership, and other equity interests, in-
19 cluding monetary capital contributions, cor-
20 porate investments, and joint ventures, result-
21 ing in end uses of items that threaten the na-
22 tional security and foreign policy interests of
23 the United States, as described in the policy set
24 forth in section 1752 of the Export Control Re-
25 form Act of 2018 (50 U.S.C. 4811).

1 (G) The effect of export controls imposed
2 pursuant to part I of that Act (50 U.S.C. 4811
3 et seq.), including—

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

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

11 (c) PROVISION OF ANALYSIS TO DEPARTMENT OF
12 COMMERCE.—Upon the request of the Secretary of Com-
13 merce, the Director of National Intelligence shall expedi-
14 tiously—

15 (1) carry out analysis of any matter relating to
16 the national security of the United States that is rel-
17 evant to a mission of the Department of Commerce;
18 and

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

23 (d) IDENTIFICATION OF SINGLE OFFICE TO SUP-
24 PORT MISSIONS OF DEPARTMENT OF COMMERCE.—The
25 Director of National Intelligence shall identify a single of-

1 fice within the intelligence community to be responsible
2 for supporting the missions of the Department of Com-
3 merce.

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

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

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

24 (3) ADMINISTRATIVE RECORD.—

1 (A) IN GENERAL.—The following informa-
2 tion may be included in the administrative
3 record relating to an action or finding described
4 in paragraph (1) and shall be submitted only to
5 the court ex parte and in camera:

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

9 (ii) Privileged law enforcement infor-
10 mation.

11 (iii) Information obtained or derived
12 from any activity authorized under the
13 Foreign Intelligence Surveillance Act of
14 1978 (50 U.S.C. 1801 et seq.).

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

18 (B) TREATMENT CONSISTENT WITH SEC-
19 TION.—Any information that is part of the ad-
20 ministrative record filed ex parte and in camera
21 under subparagraph (A), or cited by the court
22 in any decision in a civil action described in
23 paragraph (1), shall be treated by the court
24 consistent with the provisions of this subsection.

1 In no event shall such information be released
2 to the petitioner or as part of the public record.

3 (4) NONAPPLICABILITY OF USE OF INFORMA-
4 TION PROVISIONS.—The use of information provi-
5 sions of sections 106, 305, 405, and 706 of the For-
6 eign Intelligence Surveillance Act of 1978 (50
7 U.S.C. 1806, 1825, 1845, and 1881e) shall not
8 apply in a civil action challenging an action or find-
9 ing of the Secretary of Commerce made on the basis
10 of information made available to officials of the De-
11 partment of Commerce pursuant to this section.

12 (5) RULE OF CONSTRUCTION CONCERNING
13 RIGHT TO ACCESS.—No provision of this section
14 shall be construed to create a right to obtain access
15 to information in the possession of the Federal Gov-
16 ernment that was considered in an action or finding
17 of the Secretary of Commerce, including any classi-
18 fied information or sensitive but unclassified infor-
19 mation.

20 (6) EXEMPTION FROM FREEDOM OF INFORMA-
21 TION ACT.—Any information made available to offi-
22 cials of the Department of Commerce pursuant to
23 this section is exempt from disclosure under section
24 552 of title 5, United States Code (commonly re-
25 ferred to as the “Freedom of Information Act”).

1 **SEC. 506. REVIEW REGARDING INFORMATION COLLECTION**
2 **AND ANALYSIS WITH RESPECT TO ECONOMIC**
3 **COMPETITION.**

4 (a) REVIEW.—

5 (1) IN GENERAL.—Not later than 30 days after
6 the date of the enactment of this Act, the Director
7 of National Intelligence shall complete a review of
8 the requirements and access to commercial informa-
9 tion used by elements of the intelligence community
10 for analysis of capital flows, investment security,
11 beneficial ownership of entities, and other trans-
12 actions and functions related to identifying threats,
13 gaps, and opportunities with respect to economic
14 competition with foreign countries, including the
15 People’s Republic of China.

16 (2) ELEMENTS.—The review required by para-
17 graph (1) shall include the following:

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

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

22 (C) The number of such licenses permitted
23 for Federal departments and agencies that are
24 not elements of the intelligence community, in-
25 cluding the Department of Commerce.

26 (b) REPORT; BRIEFING.—

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

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

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

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

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

24 (3) FORM.—The report and briefing required
25 by paragraph (1) may be classified.

1 **Subtitle B—Next-generation En-**
 2 **ergy, Biotechnology, and Artifi-**
 3 **cial Intelligence**

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

7 Section 6503(c)(3) of the Intelligence Authorization
 8 Act for Fiscal Year 2023 (Public Law 117–263) is amend-
 9 ed by adding at the end the following:

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

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

15 “(I) artificial intelligence;

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

19 “(III) biotechnology; and

20 “(ii) that identifies—

21 “(I) competitive practices of the
 22 People’s Republic of China relating to
 23 the technologies described in clause
 24 (i);

1 “(II) opportunities to counter the
2 practices described in subclause (I);

3 “(III) countries the People’s Re-
4 public of China is targeting for ex-
5 ports of civil nuclear technology;

6 “(IV) countries best positioned to
7 utilize civil nuclear technologies from
8 the United States in order to facilitate
9 the commercial export of those tech-
10 nologies;

11 “(V) United States vulnerabilities
12 in the supply chain of these tech-
13 nologies; and

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

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

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

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

25 “(B) PUBLIC UTILITY CONTRACTS.—

1 “(i) IN GENERAL.—A contract for
2 public utility services may be made—

3 “(I) except as provided in sub-
4 clause (II), for a period of not more
5 than 10 years; or

6 “(II) for an executive agency that
7 is, or has a component that is, an ele-
8 ment of the intelligence community
9 (as defined in section 3 of the Na-
10 tional Security Act of 1947 (50
11 U.S.C. 3003)), for a period of not
12 more than 30 years, if the executive
13 agency determines the extended period
14 is in the best interests of national se-
15 curity.

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

20 **SEC. 513. ASSESSMENT OF USING CIVIL NUCLEAR ENERGY**
21 **FOR INTELLIGENCE COMMUNITY CAPABILI-**
22 **TIES.**

23 (a) ASSESSMENT REQUIRED.—The Director of Na-
24 tional Intelligence shall, in consultation with the heads of
25 such other elements of the intelligence community as the

1 Director considers appropriate, conduct an assessment of
2 capabilities identified by the Intelligence Community Con-
3 tinuity Program established pursuant to section E(3) of
4 Intelligence Community Directive 118, or any successor
5 directive, or such other facilities or capabilities as may be
6 determined by the Director to be critical to United States
7 national security, that have unique energy needs—

8 (1) to ascertain the feasibility and advisability
9 of using civil nuclear reactors to meet such needs;
10 and

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

15 (b) REPORT.—Not later than 180 days after the date
16 of the enactment of this Act, the Director shall submit
17 to the congressional intelligence committees a report,
18 which may be in classified form, on the findings of the
19 Director with respect to the assessment conducted pursu-
20 ant to subsection (a).

1 **SEC. 514. POLICIES ESTABLISHED BY DIRECTOR OF NA-**
2 **TIONAL INTELLIGENCE FOR ARTIFICIAL IN-**
3 **TELLIGENCE CAPABILITIES.**

4 (a) IN GENERAL.—Section 6702 of the Intelligence
5 Authorization Act for Fiscal Year 2023 (50 U.S.C.
6 3334m) is amended—

7 (1) in subsection (a), in the matter preceding
8 paragraph (1), by striking “subsection (b)” and in-
9 serting “subsection (c)”;

10 (2) by redesignating subsection (b) as sub-
11 section (c); and

12 (3) by inserting after subsection (a) the fol-
13 lowing:

14 “(b) POLICIES.—

15 “(1) IN GENERAL.—In carrying out subsection
16 (a)(1), not later than 1 year after the date of the
17 enactment of the Intelligence Authorization Act for
18 Fiscal Year 2024, the Director of National Intel-
19 ligence, in consultation with the heads of the ele-
20 ments of the intelligence community, shall establish
21 the policies described in paragraph (2).

22 “(2) POLICIES DESCRIBED.—The policies de-
23 scribed in this paragraph are policies for the acqui-
24 sition, adoption, development, use, coordination, and
25 maintenance of artificial intelligence capabilities
26 that—

1 “(A) establish a lexicon relating to the use
2 of machine learning and artificial intelligence
3 developed or acquired by elements of the intel-
4 ligence community;

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

9 “(i) specifying conditions for the con-
10 tinuous monitoring of artificial intelligence
11 capabilities for performance, including the
12 conditions for retraining or retiring models
13 based on performance;

14 “(ii) documenting performance objec-
15 tives, including specifying how performance
16 objectives shall be developed and contrac-
17 tually enforced for capabilities procured
18 from third parties;

19 “(iii) specifying the manner in which
20 models should be audited, as necessary, in-
21 cluding the types of documentation that
22 should be provided to any auditor; and

23 “(iv) specifying conditions under
24 which models used by elements of the intel-
25 ligence community should be subject to

1 testing and evaluation for vulnerabilities to
2 techniques meant to undermine the avail-
3 ability, integrity, or privacy of an artificial
4 intelligence capability;

5 “(C) establish guidelines for tracking de-
6 pendencies in adjacent systems, capabilities, or
7 processes impacted by the retraining or
8 sunseting of any model described in subpara-
9 graph (B);

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

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

22 “(F) provide guidance on the acquisition
23 and usage of models that have previously been
24 trained by a third party for subsequent modi-
25 fication and usage by such an element.

1 (3) The advanced capabilities of the systems de-
2 scribed in paragraph (1), and their accessibility to a
3 wide range of users, have increased the likelihood
4 and effect of misuse or malfunction of these systems,
5 such as to generate synthetic media for
6 disinformation campaigns, develop or refine malware
7 for computer network exploitation activity, design or
8 develop dual-use biological entities such as toxic
9 small molecules, proteins, or pathogenic organisms,
10 enhance surveillance capabilities in ways that under-
11 mine the privacy of citizens of the United States,
12 and increase the risk of exploitation or malfunction
13 of information technology systems incorporating ar-
14 tificial intelligence systems in mission-critical fields
15 such as health care, critical infrastructure, and
16 transportation.

17 (b) STRATEGY REQUIRED.—Not later than 180 days
18 after the date of the enactment of this Act, the President
19 shall establish a strategy by which vendors and commer-
20 cial users of artificial intelligence systems, as well as inde-
21 pendent researchers and other third parties, may effec-
22 tively notify appropriate elements of the United States
23 Government of—

24 (1) information security risks emanating from
25 artificial intelligence systems, such as the use of an

1 artificial intelligence system to develop or refine ma-
2 licious software;

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

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

17 (4) suspected foreign malign influence (as de-
18 fined by section 119C of the National Security Act
19 of 1947 (50 U.S.C. 3059(f))) activity that appears
20 to be facilitated by an artificial intelligence system;
21 and

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

24 (c) ELEMENTS.—The strategy established pursuant
25 to subsection (b) shall include the following:

1 (1) An outline of a plan for Federal agencies to
 2 engage in industry outreach and public education on
 3 the risks posed by, and directed at, artificial intel-
 4 ligence systems.

5 (2) Use of research and development, stake-
 6 holder outreach, and risk management frameworks
 7 established pursuant to provisions of law in effect on
 8 the day before the date of the enactment of this Act
 9 or Federal agency guidelines.

10 **TITLE VI—WHISTLEBLOWER**
 11 **MATTERS**

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

15 (a) AMENDMENTS TO CHAPTER 4 OF TITLE 5.—

16 (1) APPOINTMENT OF SECURITY OFFICERS.—

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

19 “(i) APPOINTMENT OF SECURITY OFFICERS.—Each
 20 Inspector General under this section, including the des-
 21 ignees of the Inspector General of the Department of De-
 22 fense pursuant to subsection (b)(3), shall appoint within
 23 their offices security officers to provide, on a permanent
 24 basis, confidential, security-related guidance and direction
 25 to an employee of their respective establishment, an em-

1 ployee assigned or detailed to such establishment, or an
2 employee of a contractor of such establishment who in-
3 tends to report to Congress a complaint or information,
4 so that such employee can obtain direction on how to re-
5 port to Congress in accordance with appropriate security
6 practices.”.

7 (2) PROCEDURES.—Subsection (e) of such sec-
8 tion is amended—

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

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

15 “(2) LIMITATION.—

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

22 “(i) before making such a contact,
23 furnishes to the head of the establishment,
24 through the Inspector General (or des-
25 ignee), a statement of the employee’s com-

1 complaint or information and notice of the em-
2 ployee’s intent to contact an intelligence
3 committee or another committee of juris-
4 diction of the Senate or the House of Rep-
5 resentatives directly; and

6 “(ii)(I) obtains and follows, from the
7 head of the establishment, through the In-
8 spector General (or designee), procedural
9 direction on how to contact an intelligence
10 committee or another committee of juris-
11 diction of the Senate or the House of Rep-
12 resentatives in accordance with appropriate
13 security practices; or

14 “(II) obtains and follows such proce-
15 dural direction from the applicable security
16 officer appointed under subsection (i).

17 “(B) LACK OF PROCEDURAL DIRECTION.—

18 If an employee seeks procedural direction under
19 subparagraph (A)(ii) and does not receive such
20 procedural direction within 30 days, or receives
21 insufficient direction to report to Congress a
22 complaint or information, the employee may
23 contact an intelligence committee or any other
24 committee of jurisdiction of the Senate or the
25 House of Representatives directly without ob-

1 taining or following the procedural direction
2 otherwise required under such subparagraph.”;
3 and

4 (C) by redesignating paragraph (3) as
5 paragraph (4); and

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

8 “(3) COMMITTEE MEMBERS AND STAFF.—An
9 employee of an element of the intelligence commu-
10 nity who intends to report to Congress a complaint
11 or information may report such complaint or infor-
12 mation to the Chairman and Vice Chairman or
13 Ranking Member, as the case may be, of an intel-
14 ligence committee or another committee of jurisdic-
15 tion of the Senate or the House of Representatives,
16 a nonpartisan member of the committee staff des-
17 ignated for purposes of receiving complaints or in-
18 formation under this section, or a member of the
19 majority staff and a member of the minority staff of
20 the committee.”.

21 (3) CLARIFICATION OF RIGHT TO REPORT DI-
22 RECTLY TO CONGRESS.—Subsection (b) of such sec-
23 tion is amended by adding at the end the following:

24 “(4) CLARIFICATION OF RIGHT TO REPORT DI-
25 RECTLY TO CONGRESS.—Subject to paragraphs (2)

1 and (3) of subsection (e), an employee of an element
2 of the intelligence community who intends to report
3 to Congress a complaint or information may report
4 such complaint or information directly to Congress,
5 regardless of whether the complaint or information
6 is with respect to an urgent concern—

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

9 “(B) in addition to reporting such com-
10 plaint or information under paragraph (1).”.

11 (b) AMENDMENTS TO NATIONAL SECURITY ACT OF
12 1947.—

13 (1) APPOINTMENT OF SECURITY OFFICERS.—

14 Section 103H(j) of the National Security Act of
15 1947 (50 U.S.C. 3033(j)) is amended by adding at
16 the end the following:

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

21 (2) PROCEDURES.—Subparagraph (D) of sec-
22 tion 103H(k)(5) of such Act (50 U.S.C. 3033(k)(5))
23 is amended—

24 (A) in clause (i), by inserting “or any
25 other committee of jurisdiction of the Senate or

1 the House of Representatives” after “either or
2 both of the congressional intelligence commit-
3 tees”;

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

6 “(ii)(I) Except as provided in subclause (II), an
7 employee may contact a congressional intelligence
8 committee or another committee of jurisdiction di-
9 rectly as described in clause (i) only if the em-
10 ployee—

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

19 “(bb)(AA) obtains and follows, from the
20 Director, through the Inspector General, proce-
21 dural direction on how to contact a congress-
22 sional intelligence committee or another com-
23 mittee of jurisdiction of the Senate or the
24 House of Representatives in accordance with
25 appropriate security practices; or

1 “(BB) obtains and follows such procedural
2 direction from the applicable security officer ap-
3 pointed under section 416(i) of title 5, United
4 States Code.

5 “(II) If an employee seeks procedural di-
6 rection under subclause (I)(bb) and does not re-
7 ceive such procedural direction within 30 days,
8 or receives insufficient direction to report to
9 Congress a complaint or information, the em-
10 ployee may contact a congressional intelligence
11 committee or any other committee of jurisdic-
12 tion of the Senate or the House of Representa-
13 tives directly without obtaining or following the
14 procedural direction otherwise required under
15 such subclause.”;

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

18 (D) by inserting after clause (ii) the fol-
19 lowing:

20 “(iii) An employee of an element of the intel-
21 ligence community who intends to report to Con-
22 gress a complaint or information may report such
23 complaint or information to the Chairman and Vice
24 Chairman or Ranking Member, as the case may be,
25 of a congressional intelligence committee or another

1 committee of jurisdiction of the Senate or the House
2 of Representatives, a nonpartisan member of the
3 committee staff designated for purposes of receiving
4 complaints or information under this section, or a
5 member of the majority staff and a member of the
6 minority staff of the committee.”.

7 (3) CLARIFICATION OF RIGHT TO REPORT DI-
8 RECTLY TO CONGRESS.—Subparagraph (A) of such
9 section is amended—

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

12 (B) by adding at the end the following:

13 “(ii) Subject to clauses (ii) and (iii) of subpara-
14 graph (D), an employee of an element of the intel-
15 ligence community who intends to report to Con-
16 gress a complaint or information may report such
17 complaint or information directly to Congress, re-
18 gardless of whether the complaint or information is
19 with respect to an urgent concern—

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

22 “(II) in addition to reporting such com-
23 plaint or information under clause (i).”.

24 (c) AMENDMENTS TO THE CENTRAL INTELLIGENCE
25 AGENCY ACT OF 1949.—

1 (1) APPOINTMENT OF SECURITY OFFICERS.—
2 Section 17(d)(5) of the Central Intelligence Agency
3 Act of 1949 (50 U.S.C. 3517(d)(5)) is amended by
4 adding at the end the following:

5 “(I) The Inspector General shall appoint within the
6 Office of the Inspector General security officers as re-
7 quired by section 416(i) of title 5, United States Code.”.

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

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

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

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

20 “(aa) before making such a contact, furnishes
21 to the Director, through the Inspector General, a
22 statement of the employee’s complaint or informa-
23 tion and notice of the employee’s intent to contact
24 an intelligence committee or another committee of

1 jurisdiction of the Senate or the House of Rep-
2 resentatives directly; and

3 “(bb)(AA) obtains and follows, from the Direc-
4 tor, through the Inspector General, procedural direc-
5 tion on how to contact an intelligence committee or
6 another committee of jurisdiction of the Senate or
7 the House of Representatives in accordance with ap-
8 propriate security practices; or

9 “(BB) obtains and follows such procedural di-
10 rection from the applicable security officer appointed
11 under section 416(i) of title 5, United States Code.

12 “(II) If an employee seeks procedural direction
13 under subclause (I)(bb) and does not receive such
14 procedural direction within 30 days, or receives in-
15 sufficient direction to report to Congress a complaint
16 or information, the employee may contact an intel-
17 ligence committee or another committee of jurisdic-
18 tion of the Senate or the House of Representatives
19 directly without obtaining or following the proce-
20 dural direction otherwise required under such sub-
21 clause.”;

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

24 (D) by inserting after clause (ii) the fol-
25 lowing:

1 “(iii) An employee of the Agency who intends to re-
2 port to Congress a complaint or information may report
3 such complaint or information to the Chairman and Vice
4 Chairman or Ranking Member, as the case may be, of an
5 intelligence committee or another committee of jurisdic-
6 tion of the Senate or the House of Representatives, a non-
7 partisan member of the committee staff designated for
8 purposes of receiving complaints or information under this
9 section, or a member of the majority staff and a member
10 of the minority staff of the committee.”.

11 (3) CLARIFICATION OF RIGHT TO REPORT DI-
12 RECTLY TO CONGRESS.—Subparagraph (A) of such
13 section is amended—

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

16 (B) by adding at the end the following:

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

23 “(I) in lieu of reporting such complaint or in-
24 formation under clause (i); or

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

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

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

12 (a) **IN GENERAL.**—Section 1104 of the National Se-
13 curity Act of 1947 (50 U.S.C. 3234) is amended—

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

15 (A) in subparagraph (I), by striking “; or”
16 and inserting a semicolon;

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

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

21 “(J) a knowing and willful disclosure re-
22 vealing the identity or other personally identifi-
23 able information of an employee or contractor
24 employee so as to identify the employee or con-
25 tractor employee as an employee or contractor

1 employee who has made a lawful disclosure de-
2 scribed in subsection (b) or (c); or”;

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

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

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

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

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

18 “(A) the personnel action was unavoidable
19 under section 103H(g)(3)(A) of this Act (50
20 U.S.C. 3033(g)(3)(A)), section 17(e)(3)(A) of
21 the Central Intelligence Agency Act of 1949 (50
22 U.S.C. 3517(e)(3)(A)), section 407(b) of title 5,
23 United States Code, or section 420(b)(2)(B) of
24 such title;

1 “(B) the personnel action was made to an
2 official of the Department of Justice responsible
3 for determining whether a prosecution should
4 be undertaken; or

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

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

11 “(5) EMPLOYEE.—The term ‘employee’, with
12 respect to an agency or a covered intelligence com-
13 munity element, includes an individual who has been
14 detailed to such agency or covered intelligence com-
15 munity element.”.

16 (c) PRIVATE RIGHT OF ACTION FOR UNLAWFUL DIS-
17 CLOSURE OF WHISTLEBLOWER IDENTITY.—Subsection
18 (g) of such section, as redesignated by subsection (a)(2)
19 of this section, is amended to read as follows:

20 “(g) ENFORCEMENT.—

21 “(1) IN GENERAL.—Except as otherwise pro-
22 vided in this subsection, the President shall provide
23 for the enforcement of this section.

24 “(2) HARMONIZATION WITH OTHER ENFORCE-
25 MENT.—To the fullest extent possible, the President

1 shall provide for enforcement of this section in a
2 manner that is consistent with the enforcement of
3 section 2302(b)(8) of title 5, United States Code, es-
4 pecially with respect to policies and procedures used
5 to adjudicate alleged violations of such section.

6 “(3) PRIVATE RIGHT OF ACTION FOR DISCLO-
7 SURES OF WHISTLEBLOWER IDENTITY IN VIOLATION
8 OF PROHIBITION AGAINST REPRISALS.—Subject to
9 paragraph (4), in a case in which an employee of an
10 agency takes a personnel action described in sub-
11 section (a)(3)(J) against an employee of a covered
12 intelligence community element as a reprisal in vio-
13 lation of subsection (b) or in a case in which an em-
14 ployee or contractor employee takes a personnel ac-
15 tion described in subsection (a)(3)(J) against an-
16 other contractor employee as a reprisal in violation
17 of subsection (c), the employee or contractor em-
18 ployee against whom the personnel action was taken
19 may, consistent with section 1221 of title 5, United
20 States Code, bring a private action for all appro-
21 priate remedies, including injunctive relief and com-
22 pensatory and punitive damages, in an amount not
23 to exceed \$250,000, against the agency of the em-
24 ployee or contracting agency of the contractor em-

1 ployee who took the personnel action, in a Federal
2 district court of competent jurisdiction.

3 “(4) REQUIREMENTS.—

4 “(A) REVIEW BY INSPECTOR GENERAL
5 AND BY EXTERNAL REVIEW PANEL.—Before
6 the employee or contractor employee may bring
7 a private action under paragraph (3), the em-
8 ployee or contractor employee shall exhaust ad-
9 ministrative remedies by—

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

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

19 “(B) PERIOD TO BRING ACTION.—The em-
20 ployee or contractor employee may bring a pri-
21 vate right of action under paragraph (3) during
22 the 180-day period beginning on the date on
23 which the employee or contractor employee is
24 notified of the final disposition of their claim
25 under section 1106.”.

1 **SEC. 603. ESTABLISHING PROCESS PARITY FOR ADVERSE**
2 **SECURITY CLEARANCE AND ACCESS DETER-**
3 **MINATIONS.**

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

7 “(C) CONTRIBUTING FACTOR.—

8 “(i) IN GENERAL.—Subject to clause
9 (iii), in determining whether the adverse
10 security clearance or access determination
11 violated paragraph (1), the agency shall
12 find that paragraph (1) was violated if the
13 individual has demonstrated that a disclo-
14 sure described in paragraph (1) was a con-
15 tributing factor in the adverse security
16 clearance or access determination taken
17 against the individual.

18 “(ii) CIRCUMSTANTIAL EVIDENCE.—

19 An individual under clause (i) may dem-
20 onstrate that the disclosure was a contrib-
21 uting factor in the adverse security clear-
22 ance or access determination taken against
23 the individual through circumstantial evi-
24 dence, such as evidence that—

1 “(I) the official making the de-
2 termination knew of the disclosure;
3 and

4 “(II) the determination occurred
5 within a period such that a reasonable
6 person could conclude that the dislo-
7 sure was a contributing factor in the
8 determination.

9 “(iii) DEFENSE.—In determining
10 whether the adverse security clearance or
11 access determination violated paragraph
12 (1), the agency shall not find that para-
13 graph (1) was violated if, after a finding
14 that a disclosure was a contributing factor,
15 the agency demonstrates by clear and con-
16 vincing evidence that it would have made
17 the same security clearance or access de-
18 termination in the absence of such dislo-
19 sure.”.

20 **SEC. 604. ELIMINATION OF CAP ON COMPENSATORY DAM-**
21 **AGES FOR RETALIATORY REVOCATION OF SE-**
22 **CURITY CLEARANCES AND ACCESS DETER-**
23 **MINATIONS.**

24 Section 3001(j)(4)(B) of the Intelligence Reform and
25 Terrorism Prevention Act of 2004 (50 U.S.C.

1 3341(j)(4)(B)) is amended, in the second sentence, by
2 striking “not to exceed \$300,000”.

3 **SEC. 605. MODIFICATION AND REPEAL OF REPORTING RE-**
4 **QUIREMENTS.**

5 (a) MODIFICATION OF FREQUENCY OF WHISTLE-
6 BLOWER NOTIFICATIONS TO INSPECTOR GENERAL OF
7 THE INTELLIGENCE COMMUNITY.—Section 5334(a) of the
8 Damon Paul Nelson and Matthew Young Pollard Intel-
9 ligence Authorization Act for Fiscal Years 2018, 2019,
10 and 2020 (Public Law 116–92; 50 U.S.C. 3033 note) is
11 amended by striking “in real time” and inserting “month-
12 ly”.

13 (b) REPEAL OF REQUIREMENT FOR INSPECTORS
14 GENERAL REVIEWS OF ENHANCED PERSONNEL SECU-
15 RITY PROGRAMS.—

16 (1) IN GENERAL.—Section 11001 of title 5,
17 United States Code, is amended—

18 (A) by striking subsection (d); and

19 (B) by redesignating subsection (e) as sub-
20 section (d).

21 (2) TECHNICAL CORRECTIONS.—Subsection (d)
22 of section 11001 of such title, as redesignated by
23 paragraph (1)(B), is amended—

24 (A) in paragraph (3), by adding “and”
25 after the semicolon at the end; and

1 (B) in paragraph (4), by striking “; and”
 2 and inserting a period.

3 **TITLE VII—CLASSIFICATION**
 4 **REFORM**

5 **Subtitle A—Classification Reform**
 6 **Act of 2023**

7 **CHAPTER 1—SHORT TITLE; DEFINITIONS**

8 **SEC. 701. SHORT TITLE.**

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

11 **SEC. 702. DEFINITIONS.**

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

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

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

20 **“Subtitle A—Definitions**

21 **“SEC. 800. DEFINITIONS.**

22 “In this title:

23 “(1) **AGENCY.**—The term ‘agency’ means any
 24 Executive agency as defined in section 105 of title
 25 5, United States Code, any military department as

1 defined in section 102 of such title, and any other
2 entity in the executive branch of the Federal Gov-
3 ernment that comes into the possession of classified
4 information.

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

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

19 “(4) CLASSIFIED INFORMATION.—The term
20 ‘classified information’ means information that has
21 been classified.

22 “(5) COMPUTER.—The term ‘computer’ means
23 any electronic, magnetic, optical, electrochemical, or
24 other high-speed data processing device performing
25 logical, arithmetic, or storage functions, and includes

1 any data storage facility or communications facility
2 directly related to or operating in conjunction with
3 such device and any data or other information
4 stored or contained in such device.

5 “(6) CONSUMER REPORTING AGENCY.—The
6 term ‘consumer reporting agency’ has the meaning
7 given such term in section 603 of the Consumer
8 Credit Protection Act (15 U.S.C. 1681a).

9 “(7) DECLASSIFY, DECLASSIFIED, DECLAS-
10 SIFICATION.—The terms ‘declassify’, ‘declassified’,
11 and ‘declassification’ refer to the process by which
12 information that has been classified is determined to
13 no longer require protection from unauthorized dis-
14 closure pursuant to this title.

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

19 “(9) EMPLOYEE.—The term ‘employee’ includes
20 any person who receives a salary or compensation of
21 any kind from the United States Government, is a
22 contractor of the United States Government or an
23 employee thereof, is an unpaid consultant of the
24 United States Government, or otherwise acts for or

1 on behalf of the United States Government, except
2 as otherwise determined by the President.

3 “(10) EXECUTIVE AGENT FOR CLASSIFICATION
4 AND DECLASSIFICATION.—The term ‘Executive
5 Agent for Classification and Declassification’ means
6 the Executive Agent for Classification and Declassification established by section 811(a).

8 “(11) FINANCIAL AGENCY AND HOLDING COM-
9 PANY.—The terms ‘financial agency’ and ‘financial
10 institution’ have the meanings given to such terms
11 in section 5312(a) of title 31, United States Code,
12 and the term ‘holding company’ has the meaning
13 given to such term in section 1101(6) of the Right
14 to Financial Privacy Act of 1978 (12 U.S.C. 3401).

15 “(12) FOREIGN POWER AND AGENT OF A FOR-
16 EIGN POWER.—The terms ‘foreign power’ and ‘agent
17 of a foreign power’ have the meanings given such
18 terms in section 101 of the Foreign Intelligence Sur-
19 veillance Act of 1978 (50 U.S.C. 1801).

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

1 “(14) INFORMATION SECURITY OVERSIGHT OF-
2 FICE.—The term ‘Information Security Oversight
3 Office’ means the Information Security Oversight
4 Office established by section 814(a).

5 “(15) ORIGINAL CLASSIFICATION AUTHOR-
6 ITY.—The term ‘original classification authority’
7 means an individual authorized in writing, either by
8 the President, the Vice President, or by agency
9 heads or other officials designated by the President,
10 to classify information in the first instance.

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

19 “(17) STATE.—The term ‘State’ means each of
20 the several States of the United States, the District
21 of Columbia, the Commonwealth of Puerto Rico, the
22 Commonwealth of the Northern Mariana Islands,
23 the United States Virgin Islands, Guam, American
24 Samoa, the Republic of the Marshall Islands, the
25 Federated States of Micronesia, and the Republic of

1 Palau, and any other possession of the United
2 States.

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

5 (3) by striking section 805.

6 **CHAPTER 2—GOVERNANCE AND AC-**
7 **COUNTABILITY FOR REFORM OF THE**
8 **SECURITY CLASSIFICATION SYSTEM**

9 **SEC. 711. EXECUTIVE AGENT FOR CLASSIFICATION AND DE-**
10 **CLASSIFICATION.**

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

14 **“Subtitle C—Security Classification**
15 **Governance**

16 **“SEC. 811. EXECUTIVE AGENT FOR CLASSIFICATION AND**
17 **DECLASSIFICATION.**

18 “(a) ESTABLISHMENT.—There is in the executive
19 branch of the Federal Government an Executive Agent for
20 Classification and Declassification who shall be respon-
21 sible for promoting programs, processes, and systems re-
22 lating to classification and declassification, including de-
23 veloping technical solutions for automating declassification
24 review and directing resources for such purposes in the
25 Federal Government.

1 “(b) DESIGNATION.—The Director of National Intel-
2 ligence shall serve as the Executive Agent for Classifica-
3 tion and Declassification.

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

6 “(1) To promote classification and declassifica-
7 tion programs, processes, and systems with the goal
8 of ensuring that declassification activities keep pace
9 with classification activities and that classified infor-
10 mation is declassified at such time as it no longer
11 meets the standard for classification.

12 “(2) To promote classification and declassifica-
13 tion programs, processes, and systems that ensure
14 secure management of and tracking of classified
15 records.

16 “(3) To promote the establishment of a fed-
17 erated classification and declassification system to
18 streamline, modernize, and oversee declassification
19 across agencies.

20 “(4) To direct resources to develop, coordinate,
21 and implement a federated classification and declas-
22 sification system that includes technologies that
23 automate declassification review and promote con-
24 sistency in declassification determinations across the
25 executive branch of the Federal Government.

1 “(5) To work with the Director of the Office of
2 Management and Budget in developing a line item
3 for classification and declassification in each budget
4 of the President that is submitted for a fiscal year
5 under section 1105(a) of title 31, United States
6 Code.

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

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

11 “(B) goal-oriented classification and de-
12 classification pilot programs.

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

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

20 “(9) To direct the implementation across agen-
21 cies of the most effective programs and approaches
22 relating to classification and declassification.

23 “(10) To establish, oversee, and enforce acquisi-
24 tion and contracting policies relating to classification
25 and declassification programs.

1 “(11) In coordination with the Information Se-
2 curity Oversight Office—

3 “(A) to issue policies and directives to the
4 heads of agencies relating to directing resources
5 and making technological investments in classi-
6 fication and declassification that include sup-
7 port for a federated system;

8 “(B) to ensure implementation of the poli-
9 cies and directives issued under subparagraph
10 (A);

11 “(C) to collect information on classification
12 and declassification practices and policies across
13 agencies, including training, accounting, chal-
14 lenges to effective declassification, and costs as-
15 sociated with classification and declassification;

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

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

22 “(12) To work with appropriate agencies to
23 oversee the implementation of policies, procedures,
24 and processes governing the submission of materials
25 for pre-publication review by persons obligated to

1 submit materials for such review by the terms of a
2 nondisclosure agreement signed in accordance with
3 Executive Order 12968 (50 U.S.C. 3161 note; relat-
4 ing to access to classified information), or successor
5 order, and to ensure such policies, procedures, and
6 processes—

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

10 “(B) produce timely and consistent deter-
11 minations across agencies; and

12 “(C) incorporate mechanisms for the time-
13 ly appeal of such determinations.

14 “(d) CONSULTATION WITH EXECUTIVE COMMITTEE
15 ON CLASSIFICATION AND DECLASSIFICATION PROGRAMS
16 AND TECHNOLOGY.—In making decisions under this sec-
17 tion, the Executive Agent for Classification and Declassification shall consult with the Executive Committee on
18 Classification and Declassification Programs and Tech-
19 nology established under section 102(a).

21 “(e) COORDINATION WITH THE NATIONAL DECLASSIFICATION CENTER.—In implementing a federated classification and declassification system, the Executive Agent
22 for Classification and Declassification shall act in coordi-
23 nation with the National Declassification Center estab-
24 lished under section 102(a).
25

1 lished by section 3.7(a) of Executive Order 13526 (50
2 U.S.C. 3161 note; relating to classified national security
3 information), or successor order.

4 “(f) STANDARDS AND DIRECTIVES OF THE INFORMA-
5 TION SECURITY OVERSIGHT OFFICE.—The programs,
6 policies, and systems promoted by the Executive Agent for
7 Classification and Declassification shall be consistent with
8 the standards and directives established by the Informa-
9 tion Security Oversight Office.

10 “(g) ANNUAL REPORT.—

11 “(1) IN GENERAL.—Not later than the end of
12 the first full fiscal year beginning after the date of
13 the enactment of the Classification Reform Act of
14 2023 and not less frequently than once each fiscal
15 year thereafter, the Executive Agent for Classifica-
16 tion and Declassification shall submit to Congress
17 and make available to the public a report on the im-
18 plementation of classification and declassification
19 programs and processes in the most recently com-
20 pleted fiscal year.

21 “(2) COORDINATION.—Each report submitted
22 and made available under paragraph (1) shall be co-
23 ordinated with the annual report of the Information
24 Security Oversight Office issued pursuant to section
25 814(d).

1 “(3) CONTENTS.—Each report submitted and
2 made available under subsection (a) shall include,
3 for the period covered by the report, the following:

4 “(A) The costs incurred by the Federal
5 Government for classification and declassifica-
6 tion.

7 “(B) A description of information systems
8 of the Federal Government and technology pro-
9 grams, processes, and systems of agencies re-
10 lated to classification and declassification.

11 “(C) A description of the policies and di-
12 rectives issued by the Executive Agent for Clas-
13 sification and Declassification and other activi-
14 ties of the Executive Agent for Classification
15 and Declassification.

16 “(D) A description of the challenges posed
17 to agencies in implementing the policies and di-
18 rectives of the Executive Agent for Classifica-
19 tion and Declassification as well as relevant im-
20 plementing policies of the agencies.

21 “(E) A description of pilot programs and
22 new investments in programs, processes, and
23 systems relating to classification and declas-
24 sification and metrics of effectiveness for such
25 programs, processes, and systems.

1 “(F) A description of progress and chal-
2 lenges in achieving the goal described in (c)(1).

3 “(h) FUNDING.—

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

7 “(A) \$5,000,000 for fiscal year 2024.

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

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

17 **SEC. 712. EXECUTIVE COMMITTEE ON CLASSIFICATION**
18 **AND DECLASSIFICATION PROGRAMS AND**
19 **TECHNOLOGY.**

20 Subtitle C of title VIII of the National Security Act
21 of 1947 (50 U.S.C. 3161 et seq.), as added by section
22 711, is further amended by adding at the end the fol-
23 lowing:

1 **“SEC. 812. EXECUTIVE COMMITTEE ON CLASSIFICATION**
2 **AND DECLASSIFICATION PROGRAMS AND**
3 **TECHNOLOGY.**

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

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

13 “(c) **MEMBERSHIP.**—

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

16 “(A) The Director of National Intelligence.

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

19 “(C) The Secretary of Energy.

20 “(D) The Secretary of State.

21 “(E) The Director of the National Declassi-
22 fication Center.

23 “(F) The Director of the Information Se-
24 curity Oversight Board.

25 “(G) The Director of the Office of Man-
26 agement and Budget.

1 “(H) Such other members as the Executive
2 Agent for Classification and Declassification
3 considers appropriate.

4 “(2) CHAIRPERSON.—The President shall ap-
5 point the chairperson of the Committee.”.

6 **SEC. 713. ADVISORY BODIES FOR EXECUTIVE AGENT FOR**
7 **CLASSIFICATION AND DECLASSIFICATION.**

8 Subtitle C of title VIII of the National Security Act
9 of 1947 (50 U.S.C. 3161 et seq.), as added by section
10 711 and amended by section 712, is further amended by
11 adding at the end the following:

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

14 “The following are hereby advisory bodies for the Ex-
15 ecutive Agent for Classification and Declassification:

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

19 “(2) The Office of the Historian of the Depart-
20 ment of State.

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

23 “(4) The Office of the Chief Historian of the
24 Central Intelligence Agency.”.

1 **SEC. 714. INFORMATION SECURITY OVERSIGHT OFFICE.**

2 Subtitle C of title VIII of the National Security Act
3 of 1947 (50 U.S.C. 3161 et seq.), as added by section
4 711 and amended by sections 712 and 713, is further
5 amended by adding at the end the following:

6 **“SEC. 814. INFORMATION SECURITY OVERSIGHT OFFICE.**

7 “(a) ESTABLISHMENT.—

8 “(1) IN GENERAL.—There is hereby established
9 in the executive branch of the Federal Government
10 an office to ensure the Government protects and
11 provides proper access to information to advance the
12 national and public interest by standardizing and as-
13 sessing the management of classified and controlled
14 unclassified information through oversight, policy de-
15 velopment, guidance, education, and reporting.

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

20 “(b) DIRECTOR.—There is in the Office a director
21 who shall be the head of the Office and who shall be ap-
22 pointed by the President.

23 “(c) DUTIES.—The duties of the director of the Of-
24 fice, which the director shall carry out in coordination with
25 the Executive Agent for Classification and Declassifica-
26 tion, are as follows:

1 “(1) To develop directives to implement a uni-
2 form system across the United States Government
3 for classifying, safeguarding, declassifying, and
4 downgrading of national security information.

5 “(2) To oversee implementation of such direc-
6 tives by agencies through establishment of strategic
7 goals and objectives and periodic assessment of
8 agency performance vis-à-vis such goals and objec-
9 tives.

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

14 “(e) FUNDING.—

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

18 “(A) \$5,000,000 for fiscal year 2024.

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

22 “(2) BUDGET ESTIMATES.—In each budget that
23 the President submits to Congress for a fiscal year
24 under section 1105(a) of title 31, United States
25 Code, the President shall include an estimate of the

1 amounts required to carry out this section in that
2 fiscal year.”.

3 **CHAPTER 3—REDUCING**
4 **OVERCLASSIFICATION**

5 **SEC. 721. CLASSIFICATION AND DECLASSIFICATION OF IN-**
6 **FORMATION.**

7 (a) IN GENERAL.—Title VIII of the National Secu-
8 rity Act of 1947, as amended by chapter 2 of this subtitle,
9 is further amended by adding at the end the following:

10 **“Subtitle D—Classification and**
11 **Declassification**

12 **“SEC. 821. CLASSIFICATION AND DECLASSIFICATION OF IN-**
13 **FORMATION.**

14 “(a) IN GENERAL.—The President may, in accord-
15 ance with this title, protect from unauthorized disclosure
16 any information owned by, produced by or for, or under
17 the control of the executive branch when there is a demon-
18 strable need to do so in order to protect the national secu-
19 rity of the United States.

20 “(b) ESTABLISHMENT OF STANDARDS AND PROCE-
21 DURES FOR CLASSIFICATION AND DECLASSIFICATION.—

22 “(1) GOVERNMENTWIDE PROCEDURES.—

23 “(A) CLASSIFICATION.—The President
24 shall, to the extent necessary, establish cat-
25 gories of information that may be classified

1 and procedures for classifying information
2 under subsection (a).

3 “(B) DECLASSIFICATION.—At the same
4 time the President establishes categories and
5 procedures under subparagraph (A), the Presi-
6 dent shall establish procedures for declassifying
7 information that was previously classified.

8 “(C) MINIMUM REQUIREMENTS.—The pro-
9 cedures established pursuant to subparagraphs
10 (A) and (B) shall—

11 “(i) permit the classification of infor-
12 mation only in cases in which the informa-
13 tion meets the standard set forth in sub-
14 section (c) and require the declassification
15 of information that does not meet such
16 standard;

17 “(ii) provide for no more than two lev-
18 els of classification;

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

22 “(iv) provide for the automatic declas-
23 sification of classified records with perma-
24 nent historical value in accordance with
25 subsection (e); and

1 “(v) provide for the timely review of
2 materials submitted for pre-publication re-
3 view in accordance with subsection (g).

4 “(2) NOTICE AND COMMENT.—

5 “(A) NOTICE.—The President shall pub-
6 lish in the Federal Register notice regarding
7 the categories and procedures proposed to be
8 established under paragraph (1).

9 “(B) COMMENT.—The President shall pro-
10 vide an opportunity for interested persons to
11 submit comments on the categories and proce-
12 dures covered by subparagraph (A).

13 “(C) DEADLINE.—The President shall
14 complete the establishment of categories and
15 procedures under this subsection not later than
16 60 days after publishing notice in the Federal
17 Register under subparagraph (A). Upon com-
18 pletion of the establishment of such categories
19 and procedures, the President shall publish in
20 the Federal Register notice regarding such cat-
21 egories and procedures.

22 “(3) MODIFICATION.—In the event the Presi-
23 dent determines to modify any categories or proce-
24 dures established under paragraph (1), subpara-

1 graphs (A) and (B) of paragraph (2) shall apply to
2 the modification of such categories or procedures.

3 “(4) AGENCY STANDARDS AND PROCEDURES.—

4 “(A) IN GENERAL.—The head of each
5 agency shall establish a single set of consoli-
6 dated standards and procedures to permit such
7 agency to classify and declassify information
8 created by such agency in accordance with the
9 categories and procedures established by the
10 President under this section and otherwise to
11 carry out this title.

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

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

23 “(c) STANDARD FOR CLASSIFICATION AND DECLAS-
24 SIFICATION.—

1 “(1) IN GENERAL.—Subject to paragraphs (2)
2 and (3), information may be classified under this
3 title, and classified information under review for de-
4 classification under this title may remain classified,
5 only if the harm to national security that might rea-
6 sonably be expected from disclosure of such informa-
7 tion outweighs the public interest in disclosure of
8 such information.

9 “(2) DEFAULT RULES.—

10 “(A) DEFAULT WITH RESPECT TO CLASSI-
11 FICATION.—In the event of significant doubt as
12 to whether the harm to national security that
13 might reasonably be expected from the disclo-
14 sure of information would outweigh the public
15 interest in the disclosure of such information,
16 such information shall not be classified.

17 “(B) DEFAULT WITH RESPECT TO DE-
18 CLASSIFICATION.—In the event of significant
19 doubt as to whether the harm to national secu-
20 rity that might reasonably be expected from the
21 disclosure of information previously classified
22 under this title would outweigh the public inter-
23 est in the disclosure of such information, such
24 information shall be declassified.

1 “(3) CRITERIA.—For purposes of this sub-
2 section, in determining the harm to national security
3 that might reasonably be expected from disclosure of
4 information, and the public interest in the disclosure
5 of information, the official making the determination
6 shall consider the following:

7 “(A) With regard to the harm to national
8 security that might reasonably be expected from
9 disclosure of information, whether or not disclo-
10 sure of the information would—

11 “(i) reveal the identity of a confiden-
12 tial human source, or reveal information
13 about the application of an intelligence
14 source or method, or reveal the identity of
15 a human intelligence source when the un-
16 authorized disclosure of that source would
17 clearly and demonstrably damage the na-
18 tional security interests of the United
19 States;

20 “(ii) reveal information that would as-
21 sist in the development or use of weapons
22 of mass destruction;

23 “(iii) reveal information that would
24 impair United States cryptologic systems
25 or activities;

1 “(iv) reveal information that would
2 impair the application of state-of-the-art
3 technology within a United States weapons
4 system;

5 “(v) reveal actual United States mili-
6 tary war plans that remain in effect;

7 “(vi) reveal information that would se-
8 riously and demonstrably impair relations
9 between the United States and a foreign
10 government, or seriously and demonstrably
11 undermine ongoing diplomatic activities of
12 the United States;

13 “(vii) reveal information that would
14 clearly and demonstrably impair the cur-
15 rent ability of United States Government
16 officials to protect the President, Vice
17 President, and other officials for whom
18 protection services, in the interest of na-
19 tional security, are authorized;

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

24 “(ix) violate a statute, treaty, or inter-
25 national agreement.

1 “(B) With regard to the public interest in
2 disclosure of information—

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

7 “(ii) whether or not disclosure of the
8 information would assist the United States
9 criminal justice system in holding persons
10 responsible for criminal acts or acts con-
11 trary to the Constitution;

12 “(iii) whether or not disclosure of the
13 information would assist Congress, or any
14 committee or subcommittee thereof, in car-
15 rying out its oversight responsibilities with
16 regard to the executive branch or in ade-
17 quately informing itself of executive branch
18 policies and activities in order to carry out
19 its legislative responsibilities;

20 “(iv) whether the disclosure of the in-
21 formation would assist Congress or the
22 public in understanding the interpretation
23 of the Federal Government of a provision
24 of law, including Federal regulations, Pres-

1 idential directives, statutes, case law, and
2 the Constitution of the United States; or

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

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

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

15 “(i) identify himself or herself; and

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

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

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

1 “(ii) use a concise notation, or similar
2 means, to document the basis for that deci-
3 sion.

4 “(5) CLASSIFICATION PROHIBITIONS AND LIM-
5 TATIONS.—

6 “(A) IN GENERAL.—In no case shall infor-
7 mation be classified, continue to be maintained
8 as classified, or fail to be declassified in order—

9 “(i) to conceal violations of law, ineffi-
10 ciency, or administrative error;

11 “(ii) to prevent embarrassment to a
12 person, organization, or agency;

13 “(iii) to restrain competition; or

14 “(iv) to prevent or delay the release of
15 information that does not require protec-
16 tion in the interest of national security.

17 “(B) BASIC SCIENTIFIC RESEARCH.—Basic
18 scientific research information not clearly re-
19 lated to national security shall not be classified.

20 “(C) RECLASSIFICATION.—Information
21 may not be reclassified after being declassified
22 and release to the public under proper authority
23 unless personally approved by the President
24 based on a determination that such reclassifica-

1 tion is required to prevent significant and de-
2 monstrable damage to national security;

3 “(d) DECLASSIFICATION OF INFORMATION CLASSI-
4 FIED UNDER ACT.—

5 “(1) IN GENERAL.—No information may re-
6 main classified indefinitely.

7 “(2) MAXIMUM PERIOD OF CLASSIFICATION.—
8 Except as provided in paragraphs (3), (4), and (5),
9 information may not remain classified under this
10 title after the date that is 25 years after the date
11 of the original classification of the information.

12 “(3) EARLIER DECLASSIFICATION.—When
13 classifying information under this title, an agency
14 official may provide for the declassification of the in-
15 formation as of a date or event that is earlier than
16 the date otherwise provided for under paragraph (2).

17 “(4) LATER DECLASSIFICATION.—When
18 classifying information under this title, an agency
19 official may provide for the declassification of the in-
20 formation on the date that is 50 years after the date
21 of the classification if the head of the agency—

22 “(A) determines that there is no likely set
23 of circumstances under which declassification
24 would occur within the time otherwise provided
25 for under paragraph (2);

1 “(B)(i) obtains the concurrence of the di-
2 rector of the Information Security Oversight
3 Office in the determination; or

4 “(ii) seeks but is unable to obtain concur-
5 rence under clause (i), obtains the concurrence
6 of the President; and

7 “(C) submits to the President a certifi-
8 cation of the determination.

9 “(5) POSTPONEMENT OF DECLASSIFICATION.—

10 “(A) IN GENERAL.—The declassification of
11 any information or category of information that
12 would otherwise be declassified under para-
13 graph (2) or (4) may be postponed, but only
14 with the personal approval of the President
15 based on a determination that such postpone-
16 ment is required to prevent significant and de-
17 monstrable damage to the national security of
18 the United States.

19 “(B) GENERAL DURATION OF POSTPONE-
20 MENT.—Information the declassification of
21 which is postponed under this paragraph may
22 remain classified not longer than 10 years after
23 the date of the postponement, unless such clas-
24 sification is renewed by the President.

1 “(C) CONGRESSIONAL NOTIFICATION.—
2 Within 30 days of any postponement or renewal
3 of a postponement under this paragraph, the
4 President shall provide written notification to
5 Congress of such postponement or renewal that
6 describes the significant and demonstrable dam-
7 age to the national security of the United
8 States that justifies such postponement or re-
9 newal.

10 “(6) BASIS FOR DETERMINATIONS.—An agency
11 official making a determination under this sub-
12 section with respect to the duration of classification
13 of information, or the declassification of information,
14 shall make the determination required under sub-
15 section (c) with respect to classification or declas-
16 sification in accordance with an assessment of the
17 criteria specified in paragraph (3) of such subsection
18 (c) that is current as of the determination.

19 “(e) AUTOMATIC DECLASSIFICATION OF CLASSIFIED
20 RECORDS.—

21 “(1) IN GENERAL.—Except as provided in para-
22 graph (2), all classified records that are more than
23 50 years old and have been determined to have per-
24 manent historical value under title 44, United States
25 Code, shall be automatically declassified on Decem-

1 ber 31 of the year that is 50 years after the date
2 on which the records were created, whether or not
3 the records have been reviewed.

4 “(2) POSTPONEMENT.—

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

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

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

19 “(B) PRESIDENTIAL POSTPONEMENT.—

20 The President may postpone automatic declas-
21 sification under paragraph (1) of specific
22 records or information if the President deter-
23 mines that such postponement is required to
24 prevent significant and demonstrable damage to
25 the national security of the United States.

1 “(C) GENERAL DURATION OF POSTPONE-
2 MENT.—A period of postponement of automatic
3 declassification under this paragraph shall not
4 exceed 10 years after the date of the postpone-
5 ment, unless renewed by the agency head who
6 postponed the automatic declassification or the
7 President.

8 “(D) CONGRESSIONAL NOTIFICATION.—
9 Within 30 days of any postponement or renewal
10 of a postponement under this paragraph, the
11 President or the head of the agency responsible
12 for the postponement shall provide written noti-
13 fication to Congress of such postponement or
14 renewal that describes the justification for such
15 postponement or renewal.

16 “(f) DECLASSIFICATION OF CURRENT CLASSIFIED
17 INFORMATION.—

18 “(1) PROCEDURES.—The President shall estab-
19 lish procedures for declassifying information that
20 was classified before the date of the enactment of
21 the Classification Reform Act of 2023. Such proce-
22 dures shall, to the maximum extent practicable, be
23 consistent with the provisions of this section.

24 “(2) AUTOMATIC DECLASSIFICATION.—The pro-
25 cedures established under paragraph (1) shall in-

1 clude procedures for the automatic declassification
2 of information referred to in paragraph (1) that has
3 remained classified for more than 25 years as of
4 such date.

5 “(3) NOTICE AND COMMENT.—

6 “(A) NOTICE.—The President shall pub-
7 lish notice in the Federal Register of the proce-
8 dures proposed to be established under this sub-
9 section.

10 “(B) COMMENT.—The President shall pro-
11 vide an opportunity for interested persons to
12 submit comments on the procedures covered by
13 subparagraph (A).

14 “(C) DEADLINE.—The President shall
15 complete the establishment of procedures under
16 this subsection not later than 60 days after
17 publishing notice in the Federal Register under
18 subparagraph (A). Upon completion of the es-
19 tablishment of such procedures, the President
20 shall publish in the Federal Register notice re-
21 garding such procedures.

22 “(g) PRE-PUBLICATION REVIEW.—

23 “(1) IN GENERAL.—The head of each agency
24 that requires personnel to sign a nondisclosure
25 agreement in accordance with Executive Order

1 12968 (50 U.S.C. 3161 note; relating to access to
2 classified information), or successor order, providing
3 for the submittal of materials for pre-publication re-
4 view, shall establish a process for the timely review
5 of such materials consistent with the requirements
6 of this title.

7 “(2) REQUIREMENTS.—Each process estab-
8 lished under paragraph (1) shall include the fol-
9 lowing:

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

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

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

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

19 (b) CONFORMING AMENDMENT TO FOIA.—Section
20 552(b)(1) of title 5, United States Code, is amended to
21 read as follows:

22 “(1)(A) specifically authorized to be classified
23 under the title VIII of the National Security Act of
24 1947, or specifically authorized under criteria estab-

1 lished by an Executive order to be kept secret in the
2 interest of national security; and

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

5 (c) EFFECTIVE DATE.—

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

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

1 **SEC. 722. DECLASSIFICATION WORKING CAPITAL FUNDS.**

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

5 **“SEC. 822. DECLASSIFICATION WORKING CAPITAL FUNDS.**

6 “(a) DEFINITION OF COVERED AGENCY.—In this
7 section, the term ‘covered agency’ means an agency that
8 has original classification authority.

9 “(b) PROGRAMS REQUIRED.—Not later than 90 days
10 after the date of the enactment of the Classification Re-
11 form Act of 2023, each head of a covered agency shall
12 establish a program for the automatic declassification of
13 classified records that have permanent historical value.

14 “(c) ESTIMATES.—Each head of a covered agency
15 shall ensure that the program established by the head pur-
16 suant to subsection (b) includes a mechanism for esti-
17 mating the number of classified records generated by each
18 subcomponent of the covered agency each fiscal year.

19 “(d) DECLASSIFICATION WORKING CAPITAL
20 FUNDS.—

21 “(1) ESTABLISHMENT.—For each covered
22 agency, there is established in the Treasury of the
23 United States a fund to be known as the ‘Declassi-
24 fication Working Capital Fund’ of the respective
25 covered agency.

1 “(2) CONTENTS OF FUNDS.—Each fund estab-
2 lished under paragraph (1) shall consist of the fol-
3 lowing:

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

6 “(B) Amounts appropriated to the fund.

7 “(3) AVAILABILITY AND USE OF FUNDS.—Sub-
8 ject to the concurrence of the Executive Agent for
9 Classification and Declassification, amounts in a
10 fund of a covered agency established by paragraph
11 (1) shall be available, without fiscal year limitation,
12 to promote and implement technological and auto-
13 mated solutions that are interoperable across cov-
14 ered agencies to support the programs of covered
15 agencies established pursuant to subsection (b).

16 “(e) TRANSFERS TO THE FUNDS.—Each head of a
17 covered agency shall issue regulations for the covered
18 agency, subject to review and approval by the Executive
19 Agent for Classification and Declassification, that require
20 each subcomponent of the covered agency to transfer, on
21 a periodic basis, to the fund established for the covered
22 agency under subsection (c)(1), an amount for a period
23 that bears the same ratio to the total amount transferred
24 to the fund by all subcomponents of the covered agency
25 for that period as the ratio of—

1 “(1) the estimate for the subcomponent pursu-
2 ant to the mechanism required by subsection (c) for
3 that period; bears to

4 “(2) the aggregate of all of the estimates for all
5 subcomponents of the Executive agency under such
6 mechanism for the same period.”.

7 **SEC. 723. TRANSPARENCY OFFICERS.**

8 Section 1062(a) of the Intelligence Reform and Ter-
9 rorism Prevention Act of 2004 (42 U.S.C. 2000ee–1(a))
10 is amended—

11 (1) in paragraph (3), by striking “; and” and
12 inserting a semicolon;

13 (2) in paragraph (4)(C), by striking the period
14 at the end and inserting “; and”;

15 (3) by adding at the end the following:

16 “(5) assist the head of such department, agen-
17 cy, or element and other officials of such depart-
18 ment, agency, or element in identifying records of
19 significant public interest and prioritizing appro-
20 priate review of such records in order to facilitate
21 the public disclosure of such records in redacted or
22 unredacted form.”;

23 (4) in paragraph (4), by redesignating subpara-
24 graphs (A) through (C) as clauses (i) through (iii),

1 respectively, and indenting such clauses 2 ems to the
2 right;

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

7 (6) in the matter before subparagraph (A), as
8 redesignated by paragraph (5), by striking “The At-
9 torney General” and inserting the following:

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

12 (7) by adding at the end the following:

13 “(2) DETERMINING PUBLIC INTEREST IN DIS-
14 CLOSURE.—In assisting the head of a department,
15 agency, or element and other officials of such de-
16 partment, agency, or element in identifying records
17 of significant public interest under subparagraph
18 (E) of paragraph (1), a senior officer designated
19 under such paragraph shall consider—

20 “(A) whether or not disclosure of the infor-
21 mation would better enable United States citi-
22 zens to hold Federal Government officials ac-
23 countable for their actions and policies;

24 “(B) whether or not disclosure of the in-
25 formation would assist the United States crimi-

1 nal justice system in holding persons respon-
2 sible for criminal acts or acts contrary to the
3 Constitution;

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

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

18 “(E) whether or not disclosure of the in-
19 formation would bring about any other signifi-
20 cant benefit, including an increase in public
21 awareness or understanding of Government ac-
22 tivities or an enhancement of Federal Govern-
23 ment efficiency.”.

1 **CHAPTER 4—PREVENTING MISHANDLING**
2 **OF CLASSIFIED INFORMATION**

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

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

8 **“Subtitle E—Protection of**
9 **Classified Information**

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

12 “(a) DEFINITIONS.—In this section:

13 “(1) ARCHIVIST, DOCUMENTARY MATERIAL,
14 PRESIDENTIAL RECORDS, PERSONAL RECORDS.—

15 The terms ‘Archivist’, ‘documentary material’, ‘Pres-
16 idential records’, and ‘personal records’ have the
17 meanings given such terms in section 2201 of title
18 44, United States Code.

19 “(2) COMMINGLED OR UNCATEGORIZED
20 RECORDS.—

21 “(A) IN GENERAL.—Except as provided in
22 subparagraph (B), the term ‘commingled or
23 uncategorized records’ means all documentary
24 materials not categorized as Presidential
25 records or personal records upon their creation

1 or receipt and filed separately pursuant to sec-
2 tion 2203(d) of title 44, United States Code.

3 “(B) EXCEPTION.—The term ‘commingled
4 or uncategorized records’ does not include docu-
5 mentary materials that are—

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

9 “(ii) stocks of publications and sta-
10 tionery; or

11 “(iii) extra copies of documents pro-
12 duced only for convenience of reference,
13 when such copies are clearly so identified.

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

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

22 “(1) categorizes the commingled or
23 uncategorized records as personal records in accord-
24 ance with subsection (c); or

1 “(2) determines the commingled or
2 uncategorized records are—

3 “(A) official records of an agency;

4 “(B) stocks of publications and stationery;

5 or

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

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

15 “(1) the Archivist performs a security review of
16 the commingled or uncategorized records that is rea-
17 sonably designed to identify records that contain
18 standard markings indicating that records contain
19 classified information;

20 “(2) the President obtains written confirmation
21 from the Archivist that the review conducted pursu-
22 ant to paragraph (1) did not identify any records
23 that contain standard markings indicating that
24 records contain classified information or, if such

1 markings were improperly applied, that such mark-
2 ings have been corrected; and

3 “(3) the President obtains written confirmation
4 from the Archivist that the Archivist is not aware of
5 any other requirement that would preclude catego-
6 rizing the commingled or uncategorized records as
7 personal records.

8 “(d) REVIEW OF COMMINGLED OR UNCATEGORIZED
9 RECORDS OF FORMER PRESIDENTS AND VICE PRESI-
10 DENTS.—

11 “(1) REQUESTS FOR REVIEW.—During the
12 180-day period following the end of the term of of-
13 fice of a former President or Vice President—

14 “(A) the former President or Vice Presi-
15 dent may request that the Archivist review the
16 categorization of any commingled or
17 uncategorized records created or received dur-
18 ing the term of the former President or Vice
19 President; and

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

23 “(2) ACTIONS UPON COMPLETION OF RE-
24 VIEW.—If, pursuant to a review under paragraph
25 (1), the Archivist determines that any commingled

1 or uncategorized records reviewed are improperly
2 categorized, the Archivist shall—

3 “(A) submit to the President a rec-
4 ommendation to correct the categorization of
5 the records; and

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

8 **SEC. 732. MANDATORY COUNTERINTELLIGENCE RISK AS-**
9 **SESSMENTS.**

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

13 **“SEC. 832. MANDATORY COUNTERINTELLIGENCE RISK AS-**
14 **SESSMENTS.**

15 “(a) MISHANDLING OR UNAUTHORIZED DISCLOSURE
16 OF CLASSIFIED INFORMATION DEFINED.—In this section,
17 the term ‘mishandling or unauthorized disclosure of classi-
18 fied information’ means any unauthorized storage, reten-
19 tion, communication, confirmation, acknowledgment, or
20 physical transfer of classified information.

21 “(b) ASSESSMENTS.—The Director of the National
22 Counterintelligence and Security Center shall prepare a
23 written assessment of the risk to national security from
24 any mishandling or unauthorized disclosure of classified
25 information involving the conduct of the President, Vice

1 President, or an official listed in Level I of the Executive
2 Schedule under section 5312 of title 5, United States
3 Code, within 90 days of the detection of such mishandling
4 or unauthorized disclosure.

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

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

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

18 **SEC. 733. MINIMUM STANDARDS FOR EXECUTIVE AGENCY**

19 **INSIDER THREAT PROGRAMS.**

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

24 (b) ESTABLISHMENT OF INSIDER THREAT PRO-
25 GRAMS.—Each head of an agency with access to classified

1 information shall establish an insider threat program to
2 protect classified information from unauthorized disclo-
3 sure.

4 (c) MINIMUM STANDARDS.—In carrying out an in-
5 sider threat program established by the head of an agency
6 pursuant to subsection (b), the head of the agency shall—

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

9 (2) monitor user activity on all classified net-
10 works in order to detect activity indicative of insider
11 threat behavior;

12 (3) build and maintain an insider threat ana-
13 lytic and response capability to review, assess, and
14 respond to information obtained pursuant to para-
15 graph (2); and

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

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

1 of agencies with respect to the requirements of this sec-
 2 tion.

3 **CHAPTER 5—OTHER MATTERS**

4 **SEC. 741. PROHIBITIONS.**

5 (a) WITHHOLDING INFORMATION FROM CON-
 6 GRESS.—Nothing in this subtitle or an amendment made
 7 by this subtitle shall be construed to authorize the with-
 8 holding of information from Congress.

9 (b) JUDICIAL REVIEW.—Except in the case of the
 10 amendment to section 552 of title 5, United States Code,
 11 made by section 721(b), no person may seek or obtain ju-
 12 dicial review of any provision of this subtitle or any action
 13 taken under a provision of this subtitle.

14 **SEC. 742. CONFORMING AMENDMENT.**

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

18 **SEC. 743. CLERICAL AMENDMENT.**

19 The table of contents for the National Security Act
 20 of 1947 is amended by striking the items relating to title
 21 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.

“Sec. 802. Requests by authorized investigative agencies.

“Sec. 803. Security Executive Agent.

“Sec. 804. Exceptions.

“Subtitle C—Security Classification Governance

“Sec. 811. Executive Agent for Classification and Declassification.

“Sec. 812. Executive Committee on Classification and Declassification Programs and Technology.

“Sec. 813. Advisory bodies for Executive Agent for Classification and Declassification.

“Sec. 814. Information Security Oversight Office.

“Subtitle D—Classification and Declassification

“Sec. 821. Classification and declassification of information.

“Sec. 822. Declassification working capital funds.

“Subtitle E—Protection of Classified Information

“Sec. 831. Security review of certain records of the President and Vice President.

“Sec. 832. Mandatory counterintelligence risk assessments.”.

1 **Subtitle B—Sensible Classification**
 2 **Act of 2023**

3 **SEC. 751. SHORT TITLE.**

4 This subtitle may be cited as the “Sensible Classifica-
 5 tion Act of 2023”.

6 **SEC. 752. DEFINITIONS.**

7 In this subtitle:

8 (1) AGENCY.—The term “agency” has the
 9 meaning given the term “Executive agency” in sec-
 10 tion 105 of title 5, United States Code.

11 (2) CLASSIFICATION.—The term “classifica-
 12 tion” means the act or process by which information
 13 is determined to be classified information.

14 (3) CLASSIFIED INFORMATION.—The term
 15 “classified information” means information that has

1 been determined pursuant to Executive Order 12958
2 (50 U.S.C. 3161 note; relating to classified national
3 security information), or successor order, to require
4 protection against unauthorized disclosure and is
5 marked to indicate its classified status when in doc-
6 umentary form.

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

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

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

20 (7) INFORMATION.—The term “information”
21 means any knowledge that can be communicated or
22 documentary material, regardless of its physical
23 form or characteristics, that is owned by, is pro-
24 duced by or for, or is under the control of the
25 United States Government.

1 (8) ORIGINATE, ORIGINATING, AND ORIGI-
2 NATED.—The term “originate”, “originating”, and
3 “originated”, with respect to classified information
4 and an authority, means the authority that classified
5 the information in the first instance.

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

14 (10) SECURITY CLEARANCE.—The term “secu-
15 rity clearance” means an authorization to access
16 classified information.

17 (11) UNAUTHORIZED DISCLOSURE.—The term
18 “unauthorized disclosure” means a communication
19 or physical transfer of classified information to an
20 unauthorized recipient.

21 (12) UNCLASSIFIED INFORMATION.—The term
22 “unclassified information” means information that is
23 not classified information.

1 **SEC. 753. FINDINGS AND SENSE OF THE SENATE.**

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

4 (1) According to a report released by the Office
5 of the Director of Intelligence in 2020 titled “Fiscal
6 Year 2019 Annual Report on Security Clearance De-
7 terminations”, more than 4,000,000 individuals have
8 been granted eligibility for a security clearance.

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

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

14 (1) the classification system of the Federal Gov-
15 ernment is in urgent need of reform;

16 (2) the number of people with access to classi-
17 fied information is exceedingly high and must be jus-
18 tified or reduced;

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

22 (4) classification should be limited to the min-
23 imum necessary to protect national security while
24 balancing the public’s interest in disclosure.

1 **SEC. 754. CLASSIFICATION AUTHORITY.**

2 (a) IN GENERAL.—The authority to classify informa-
3 tion originally may be exercised only by—

4 (1) the President and, in the performance of ex-
5 ecutive duties, the Vice President;

6 (2) the head of an agency or an official of any
7 agency authorized by the President pursuant to a
8 designation of such authority in the Federal Reg-
9 ister; and

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

13 (b) SCOPE OF AUTHORITY.—An individual author-
14 ized by this section to classify information originally at
15 a specified level may also classify the information origi-
16 nally at a lower level.

17 (c) DELEGATION OF ORIGINAL CLASSIFICATION AU-
18 THORITY.—An official of the Federal Government may be
19 delegated original classification authority subject to the
20 following:

21 (1) Delegation of original classification author-
22 ity shall be limited to the minimum required to ad-
23 minister this section. Agency heads shall be respon-
24 sible for ensuring that designated subordinate offi-
25 cials have a demonstrable and continuing need to ex-
26 ercise this authority.

1 (2) Authority to originally classify information
2 at the level designated as “Top Secret” may be dele-
3 gated only by the President, in the performance of
4 executive duties, the Vice President, or an agency
5 head or official designated pursuant to subsection
6 (a)(2).

7 (3) Authority to originally classify information
8 at the level designated as “Secret” or “Confidential”
9 may be delegated only by the President, in the per-
10 formance of executive duties, the Vice President, or
11 an agency head or official designated pursuant to
12 subsection (a)(2), or the senior agency official de-
13 scribed in section 5.4(d) of Executive Order 13526
14 (50 U.S.C. 3161 note; relating to classified national
15 security information), or successor order, provided
16 that official has been delegated “Top Secret” origi-
17 nal classification authority by the agency head.

18 (4) Each delegation of original classification au-
19 thority shall be in writing and the authority shall
20 not be redelegated except as provided by paragraphs
21 (1), (2), and (3). Each delegation shall identify the
22 official by name or position title.

23 (d) TRAINING REQUIRED.—

24 (1) IN GENERAL.—An individual may not be
25 delegated original classification authority under this

1 section unless the individual has first received train-
2 ing described in paragraph (2).

3 (2) TRAINING DESCRIBED.—Training described
4 in this paragraph is training on original classifica-
5 tion that includes instruction on the proper safe-
6 guarding of classified information and of the crimi-
7 nal, civil, and administrative sanctions that may be
8 brought against an individual who fails to protect
9 classified information from unauthorized disclosure.

10 (e) EXCEPTIONAL CASES.—

11 (1) IN GENERAL.—When an employee, con-
12 tractor, licensee, certificate holder, or grantee of an
13 agency who does not have original classification au-
14 thority originates information believed by that em-
15 ployee, contractor, licensee, certificate holder, or
16 grantee to require classification, the information
17 shall be protected in a manner consistent with Exec-
18 utive Order 13526 (50 U.S.C. 3161 note; relating to
19 classified national security information), or successor
20 order.

21 (2) TRANSMITTAL.—An employee, contractor,
22 licensee, certificate holder, or grantee described in
23 paragraph (1), who originates information described
24 in such paragraph, shall promptly transmit such in-
25 formation to—

1 (A) the agency that has appropriate sub-
2 ject matter interest and classification authority
3 with respect to this information; or

4 (B) if it is not clear which agency has ap-
5 propriate subject matter interest and classifica-
6 tion authority with respect to the information,
7 the Director of the Information Security Over-
8 sight Office.

9 (3) AGENCY DECISIONS.—An agency that re-
10 ceives information pursuant to paragraph (2)(A) or
11 (4) shall decide within 30 days whether to classify
12 this information.

13 (4) INFORMATION SECURITY OVERSIGHT OF-
14 FICE ACTION.—If the Director of the Information
15 Security Oversight Office receives information under
16 paragraph (2)(B), the Director shall determine the
17 agency having appropriate subject matter interest
18 and classification authority and forward the infor-
19 mation, with appropriate recommendations, to that
20 agency for a classification determination.

21 **SEC. 755. PROMOTING EFFICIENT DECLASSIFICATION RE-**
22 **VIEW.**

23 (a) IN GENERAL.—Whenever an agency is processing
24 a request pursuant to section 552 of title 5, United States
25 Code (commonly known as the “Freedom of Information

1 Act”) or the mandatory declassification review provisions
2 of Executive Order 13526 (50 U.S.C. 3161 note; relating
3 to classified national security information), or successor
4 order, and identifies responsive classified records that are
5 more than 25 years of age as of December 31 of the year
6 in which the request is received, the head of the agency
7 shall review the record and process the record for declas-
8 sification and release by the National Declassification
9 Center of the National Archives and Records Administra-
10 tion.

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

12 (1) regardless of whether or not the record de-
13 scribed in such subsection is in the legal custody of
14 the National Archives and Records Administration;
15 and

16 (2) without regard for any other provisions of
17 law or existing agreements or practices between
18 agencies.

19 **SEC. 756. TRAINING TO PROMOTE SENSIBLE CLASSIFICA-**
20 **TION.**

21 (a) DEFINITIONS.—In this section:

22 (1) OVER-CLASSIFICATION.—The term “over-
23 classification” means classification at a level that ex-
24 ceeds the minimum level of classification that is suf-

1 ficient to protect the national security of the United
2 States.

3 (2) SENSIBLE CLASSIFICATION.—The term
4 “sensible classification” means classification at a
5 level that is the minimum level of classification that
6 is sufficient to protect the national security of the
7 United States.

8 (b) TRAINING REQUIRED.—Each head of an agency
9 with classification authority shall conduct training for em-
10 ployees of the agency with classification authority to dis-
11 courage over-classification and to promote sensible classi-
12 fication.

13 **SEC. 757. IMPROVEMENTS TO PUBLIC INTEREST DECLASSI-**
14 **SIFICATION BOARD.**

15 Section 703 of the Public Interest Declassification
16 Act of 2000 (50 U.S.C. 3355a) is amended—

17 (1) in subsection (c), by adding at the end the
18 following:

19 “(5) A member of the Board whose term has expired
20 may continue to serve until a successor is appointed and
21 sworn in.”; and

22 (2) in subsection (f)—

23 (A) by inserting “(1)” before “Any em-
24 ployee”; and

25 (B) by adding at the end the following:

1 “(2)(A) In addition to any employees detailed to the
2 Board under paragraph (1), the Board may hire not more
3 than 12 staff members.

4 “(B) There are authorized to be appropriated to
5 carry out subparagraph (A) such sums as are necessary
6 for fiscal year 2024 and each fiscal year thereafter.”.

7 **SEC. 758. IMPLEMENTATION OF TECHNOLOGY FOR CLASSI-**
8 **FICATION AND DECLASSIFICATION.**

9 (a) IN GENERAL.—Not later than 1 year after the
10 date of the enactment of this Act, the Administrator of
11 the Office of Electronic Government (in this section re-
12 ferred to as the “Administrator”) shall, in consultation
13 with the Secretary of Defense, the Director of the Central
14 Intelligence Agency, the Director of National Intelligence,
15 the Public Interest Declassification Board, the Director of
16 the Information Security Oversight Office, and the head
17 of the National Declassification Center of the National Ar-
18 chives and Records Administration—

19 (1) research a technology-based solution—

20 (A) utilizing machine learning and artifi-
21 cial intelligence to support efficient and effec-
22 tive systems for classification and declassifica-
23 tion; and

1 (B) to be implemented on an interoperable
2 and federated basis across the Federal Govern-
3 ment; and

4 (2) submit to the President a recommendation
5 regarding a technology-based solution described in
6 paragraph (1) that should be adopted by the Federal
7 Government.

8 (b) STAFF.—The Administrator may hire sufficient
9 staff to carry out subsection (a).

10 (c) REPORT.—Not later than 540 days after the date
11 of the enactment of this Act, the President shall submit
12 to Congress a classified report on the technology-based so-
13 lution recommended by the Administrator under sub-
14 section (a)(2) and the President’s decision regarding its
15 adoption.

16 **SEC. 759. STUDIES AND RECOMMENDATIONS ON NECES-**
17 **SITY OF SECURITY CLEARANCES.**

18 (a) AGENCY STUDIES ON NECESSITY OF SECURITY
19 CLEARANCES.—

20 (1) STUDIES REQUIRED.—The head of each
21 agency that grants security clearances to personnel
22 of such agency shall conduct a study on the neces-
23 sity of such clearances.

24 (2) REPORTS REQUIRED.—

1 (A) IN GENERAL.—Not later than 1 year
2 after the date of the enactment of this Act,
3 each head of an agency that conducts a study
4 under paragraph (1) shall submit to Congress
5 a report on the findings of the agency head
6 with respect to such study, which the agency
7 head may classify as appropriate.

8 (B) REQUIRED ELEMENTS.—Each report
9 submitted by the head of an agency under sub-
10 paragraph (A) shall include, for such agency,
11 the following:

12 (i) The number of personnel eligible
13 for access to information up to the “Top
14 Secret” level.

15 (ii) The number of personnel eligible
16 for access to information up to the “Se-
17 cret” level.

18 (iii) Information on any reduction in
19 the number of personnel eligible for access
20 to classified information based on the
21 study conducted under paragraph (1).

22 (iv) A description of how the agency
23 head will ensure that the number of secu-
24 rity clearances granted by such agency will
25 be kept to the minimum required for the

1 conduct of agency functions, commensurate
2 with the size, needs, and mission of the
3 agency.

4 (3) INDUSTRY.—This subsection shall apply to
5 the Secretary of Defense in the Secretary’s capacity
6 as the Executive Agent for the National Industrial
7 Security Program, and the Secretary shall treat con-
8 tractors, licensees, and grantees as personnel of the
9 Department of Defense for purposes of the studies
10 and reports required by this subsection.

11 (b) DIRECTOR OF NATIONAL INTELLIGENCE REVIEW
12 OF SENSITIVE COMPARTMENTED INFORMATION.—The
13 Director of National Intelligence shall—

14 (1) review the number of personnel eligible for
15 access to sensitive compartmented information; and

16 (2) submit to Congress a report on how the Di-
17 rector will ensure that the number of such personnel
18 is limited to the minimum required.

19 (c) AGENCY REVIEW OF SPECIAL ACCESS PRO-
20 GRAMS.—Each head of an agency who is authorized to es-
21 tablish a special access program by Executive Order
22 13526 (50 U.S.C. 3161 note; relating to classified na-
23 tional security information), or successor order, shall—

1 (1) review the number of personnel of the agen-
2 cy eligible for access to such special access pro-
3 grams; and

4 (2) submit to Congress a report on how the
5 agency head will ensure that the number of such
6 personnel is limited to the minimum required.

7 (d) SECRETARY OF ENERGY REVIEW OF Q AND L
8 CLEARANCES.—The Secretary of Energy shall—

9 (1) review the number of personnel of the De-
10 partment of Energy granted Q and L access; and

11 (2) submit to Congress a report on how the
12 Secretary will ensure that the number of such per-
13 sonnel is limited to the minimum required

14 (e) INDEPENDENT REVIEWS.—Not later than 180
15 days after the date on which a study is completed under
16 subsection (a) or a review is completed under subsections
17 (b) through (d), the Director of the Information Security
18 Oversight Office of the National Archives and Records Ad-
19 ministration, the Director of National Intelligence, and the
20 Public Interest Declassification Board shall each review
21 the study or review, as the case may be.

1 **TITLE VIII—SECURITY CLEAR-**
2 **ANCE AND TRUSTED WORK-**
3 **FORCE**

4 **SEC. 801. REVIEW OF SHARED INFORMATION TECHNOLOGY**
5 **SERVICES FOR PERSONNEL VETTING.**

6 Not later than 1 year after the date of the enactment
7 of this Act, the Director of National Intelligence shall sub-
8 mit to the congressional intelligence committees a review
9 of the extent to which the intelligence community can use
10 information technology services shared among the intel-
11 ligence community for purposes of personnel vetting, in-
12 cluding with respect to human resources, suitability, and
13 security.

14 **SEC. 802. TIMELINESS STANDARD FOR RENDERING DETER-**
15 **MINATIONS OF TRUST FOR PERSONNEL VET-**
16 **TING.**

17 (a) **TIMELINESS STANDARD.**—

18 (1) **IN GENERAL.**—The President shall, acting
19 through the Security Executive Agent and the Suit-
20 ability and Credentialing Executive Agent, establish
21 and publish in the Federal Register new timeliness
22 performance standards for processing personnel vet-
23 ting trust determinations in accordance with the
24 Federal personnel vetting performance management
25 standards.

1 (2) QUINQUENNIAL REVIEWS.—Not less fre-
2 quently than once every 5 years, the President shall,
3 acting through the Security Executive Agent and the
4 Suitability and Credentialing Executive Agent—

5 (A) review the standards established pur-
6 suant to paragraph (1); and

7 (B) pursuant to such review—

8 (i) update such standards as the
9 President considers appropriate; and

10 (ii) publish in the Federal Register
11 such updates as may be made pursuant to
12 clause (i).

13 (3) CONFORMING AMENDMENT.—Section 3001
14 of the Intelligence Reform and Terrorism Prevention
15 Act of 2004 (50 U.S.C. 3341) is amended by strik-
16 ing subsection (g).

17 (b) QUARTERLY REPORTS ON IMPLEMENTATION.—

18 (1) IN GENERAL.—Not less frequently than
19 quarterly, the Security Executive Agent and the
20 Suitability and Credentialing Executive Agent shall
21 jointly make available to the public a quarterly re-
22 port on the compliance of Executive agencies (as de-
23 fined in section 105 of title 5, United States Code)
24 with the standards established pursuant to sub-
25 section (a).

1 (2) DISAGGREGATION.—Each report made
2 available pursuant to paragraph (1) shall
3 disaggregate data by appropriate category of per-
4 sonnel risk and between Government and contractor
5 personnel.

6 (c) COMPLEMENTARY STANDARDS FOR INTEL-
7 LIGENCE COMMUNITY.—The Director of National Intel-
8 ligence may, in consultation with the Security, Suitability,
9 and Credentialing Performance Accountability Council es-
10 tablished pursuant to Executive Order 13467 (50 U.S.C.
11 3161 note; relating to reforming processes related to suit-
12 ability for Government employment, fitness for contractor
13 employees, and eligibility for access to classified national
14 security information) establish for the intelligence commu-
15 nity standards complementary to those established pursu-
16 ant to subsection (a).

17 **SEC. 803. ANNUAL REPORT ON PERSONNEL VETTING**
18 **TRUST DETERMINATIONS.**

19 (a) DEFINITION OF PERSONNEL VETTING TRUST
20 DETERMINATION.—In this section, the term “personnel
21 vetting trust determination” means any determination
22 made by an executive branch agency as to whether an indi-
23 vidual can be trusted to perform job functions or to be
24 granted access necessary for a position.

1 (b) ANNUAL REPORT.—Not later than March 30,
2 2024, and annually thereafter for 5 years, the Director
3 of National Intelligence, acting as the Security Executive
4 Agent, and the Director of the Office of Personnel Man-
5 agement, acting as the Suitability and Credentialing Exec-
6 utive Agent, in coordination with the Security, Suitability,
7 and Credentialing Performance Accountability Council,
8 shall jointly make available to the public a report on spe-
9 cific types of personnel vetting trust determinations made
10 during the fiscal year preceding the fiscal year in which
11 the report is made available, disaggregated by the fol-
12 lowing:

13 (1) Determinations of eligibility for national se-
14 curity-sensitive positions, separately noting—

15 (A) the number of individuals granted ac-
16 cess to national security information; and

17 (B) the number of individuals determined
18 to be eligible for but not granted access to na-
19 tional security information.

20 (2) Determinations of suitability or fitness for
21 a public trust position.

22 (3) Status as a Government employee, a con-
23 tractor employee, or other category.

24 (c) ELIMINATION OF REPORT REQUIREMENT.—Sec-
25 tion 3001 of the Intelligence Reform and Terrorism Pre-

1 vention Act of 2004 (50 U.S.C. 3341) is amended by strik-
2 ing subsection (h).

3 **SEC. 804. SURVEY TO ASSESS STRENGTHS AND WEAK-**
4 **NESSES OF TRUSTED WORKFORCE 2.0.**

5 Not later than 1 year after the date of the enactment
6 of this Act, and once every 2 years thereafter until 2029,
7 the Comptroller General of the United States shall admin-
8 ister a survey to such sample of Federal agencies, Federal
9 contractors, and other persons that require security clear-
10 ances to access classified information as the Comptroller
11 General considers appropriate to assess—

12 (1) the strengths and weaknesses of the imple-
13 mentation of the Trusted Workforce 2.0 initiative;
14 and

15 (2) the effectiveness of vetting Federal per-
16 sonnel while managing risk during the onboarding of
17 such personnel.

18 **SEC. 805. PROHIBITION ON DENIAL OF ELIGIBILITY FOR**
19 **ACCESS TO CLASSIFIED INFORMATION SOLE-**
20 **LY BECAUSE OF PAST USE OF CANNABIS.**

21 (a) DEFINITIONS.—In this section:

22 (1) CANNABIS.—The term “cannabis” has the
23 meaning given the term “marihuana” in section 102
24 of the Controlled Substances Act (21 U.S.C. 802).

1 (2) ELIGIBILITY FOR ACCESS TO CLASSIFIED
2 INFORMATION.—The term “eligibility for access to
3 classified information” has the meaning given the
4 term in the procedures established pursuant to sec-
5 tion 801(a) of the National Security Act of 1947 (50
6 U.S.C. 3161(a)).

7 (b) PROHIBITION.—Notwithstanding any other provi-
8 sion of law, the head of an element of the intelligence com-
9 munity may not make a determination to deny eligibility
10 for access to classified information to an individual based
11 solely on the use of cannabis by the individual prior to
12 the submission of the application for a security clearance
13 by the individual.

14 **TITLE IX—ANOMALOUS HEALTH** 15 **INCIDENTS**

16 **SEC. 901. IMPROVED FUNDING FLEXIBILITY FOR PAY-** 17 **MENTS MADE BY THE CENTRAL INTEL-** 18 **LIGENCE AGENCY FOR QUALIFYING INJU-** 19 **RIES TO THE BRAIN.**

20 Section 19A(d) of the Central Intelligence Agency
21 Act of 1949 (50 U.S.C. 3519b(d)) is amended by striking
22 paragraph (3) and inserting the following new paragraph:

23 “(3) FUNDING.—

1 “(A) IN GENERAL.—Payment under para-
2 graph (2) in a fiscal year may be made using
3 any funds—

4 “(i) appropriated in advance specifi-
5 cally for payments under such paragraph;
6 or

7 “(ii) reprogrammed in accordance
8 with section 504 of the National Security
9 Act of 1947 (50 U.S.C. 3094).

10 “(B) BUDGET.—For each fiscal year, the
11 Director shall include with the budget justifica-
12 tion materials submitted to Congress in support
13 of the budget of the President for that fiscal
14 year pursuant to section 1105(a) of title 31,
15 United States Code, an estimate of the funds
16 required in that fiscal year to make payments
17 under paragraph (2).”.

18 **SEC. 902. CLARIFICATION OF REQUIREMENTS TO SEEK**
19 **CERTAIN BENEFITS RELATING TO INJURIES**
20 **TO THE BRAIN.**

21 (a) IN GENERAL.—Section 19A(d) of the Central In-
22 telligence Agency Act of 1949 (50 U.S.C. 3519b(d)) is
23 amended by adding at the end of paragraph (5) the fol-
24 lowing new sentence: “A covered dependent, covered em-
25 ployee, or covered individual shall not be required to seek

1 any other benefit furnished by the United States Govern-
2 ment to be eligible for the payment authorized under para-
3 graph (2).”.

4 (b) REGULATIONS.—Not later than 90 days after the
5 date of the enactment of this Act, the Director of the Cen-
6 tral Intelligence Agency shall—

7 (1) revise the regulations of the Expanded Care
8 Program of the Central Intelligence Agency to con-
9 form with the amendment made by subsection (a);
10 and

11 (2) submit to the congressional intelligence
12 committees copies of such regulations, as revised
13 pursuant to paragraph (1).

14 **SEC. 903. INTELLIGENCE COMMUNITY IMPLEMENTATION**
15 **OF HAVANA ACT OF 2021 AUTHORITIES.**

16 (a) REGULATIONS.—Except as provided in subsection
17 (c), not later than 180 days after the date of the enact-
18 ment of this Act, each head of an element of the intel-
19 ligence community that has not already done so shall—

20 (1) issue regulations and procedures to imple-
21 ment the authorities provided by section 19A(d) of
22 the Central Intelligence Agency Act of 1949 (50
23 U.S.C. 3519b(d)) and section 901(i) of title IX of
24 division J of the Further Consolidated Appropria-
25 tions Act, 2020 (22 U.S.C. 2680b(i)) to provide pay-

1 ments under such sections, to the degree that such
2 authorities are applicable to the head of the element;
3 and

4 (2) submit to the congressional intelligence
5 committees copies of such regulations.

6 (b) REPORTING.—Not later than 210 days after the
7 date of the enactment of this Act, each head of an element
8 of the intelligence community shall submit to the congress-
9 sional intelligence committees a report on—

10 (1) the estimated number of individuals associ-
11 ated with their element that may be eligible for pay-
12 ment under the authorities described in subsection
13 (a)(1);

14 (2) an estimate of the obligation that the head
15 of the intelligence community element expects to
16 incur in fiscal year 2025 as a result of establishing
17 the regulations pursuant to subsection (a)(1); and

18 (3) any perceived barriers or concerns in imple-
19 menting such authorities.

20 (c) ALTERNATIVE REPORTING.—Not later than 180
21 days after the date of the enactment of this Act, each head
22 of an element of the intelligence community (other than
23 the Director of the Central Intelligence Agency) who be-
24 lieves that the authorities described in subsection (a)(1)
25 are not currently relevant for individuals associated with

1 their element, or who are not otherwise in position to issue
2 the regulations and procedures required by subsection
3 (a)(1) shall provide written and detailed justification to
4 the congressional intelligence committees to explain this
5 position.

6 **SEC. 904. REPORT AND BRIEFING ON CENTRAL INTEL-**
7 **LIGENCE AGENCY HANDLING OF ANOMA-**
8 **LOUS HEALTH INCIDENTS.**

9 (a) DEFINITIONS.—In this section:

10 (1) AGENCY.—The term “Agency” means the
11 Central Intelligence Agency.

12 (2) QUALIFYING INJURY.—The term “quali-
13 fying injury” has the meaning given such term in
14 section 19A(d)(1) of the Central Intelligence Agency
15 Act of 1949 (50 U.S.C. 3519b(d)(1)).

16 (b) IN GENERAL.—Not later than 60 days after the
17 date of the enactment of this Act, the Director of the Cen-
18 tral Intelligence Agency shall submit to the congressional
19 intelligence committees a report on the handling of anoma-
20 lous health incidents by the Agency.

21 (c) CONTENTS.—The report required by subsection
22 (b) shall include the following:

23 (1) HAVANA ACT IMPLEMENTATION.—

24 (A) An explanation of how the Agency de-
25 termines whether a reported anomalous health

1 incident resulted in a qualifying injury or a
2 qualifying injury to the brain.

3 (B) The number of participants of the Ex-
4 panded Care Program of the Central Intel-
5 ligence Agency who—

6 (i) have a certified qualifying injury or
7 a certified qualifying injury to the brain;
8 and

9 (ii) as of September 30, 2023, applied
10 to the Expanded Care Program due to a
11 reported anomalous health incident.

12 (C) A comparison of the number of anoma-
13 lous health incidents reported by applicants to
14 the Expanded Care Program that occurred in
15 the United States and that occurred in a for-
16 eign country.

17 (D) The specific reason each applicant was
18 approved or denied for payment under the Ex-
19 panded Care Program.

20 (E) The number of applicants who were
21 initially denied payment but were later ap-
22 proved on appeal.

23 (F) The average length of time, from the
24 time of application, for an applicant to receive
25 a determination from the Expanded Care Pro-

1 gram, aggregated by qualifying injuries and
2 qualifying injuries to the brain.

3 (2) PRIORITY CASES.—

4 (A) A detailed list of priority cases of
5 anomalous health incidents, including, for each
6 incident, locations, dates, times, and cir-
7 cumstances.

8 (B) For each priority case listed in accord-
9 ance with subparagraph (A), a detailed expla-
10 nation of each credible alternative explanation
11 that the Agency assigned to the incident, in-
12 cluding—

13 (i) how the incident was discovered;

14 (ii) how the incident was assigned
15 within the Agency; and

16 (iii) whether an individual affected by
17 the incident is provided an opportunity to
18 appeal the credible alternative explanation.

19 (C) For each priority case of an anomalous
20 health incident determined to be largely con-
21 sistent with the definition of “anomalous health
22 incident” established by the National Academy
23 of Sciences and for which the Agency does not
24 have a credible alternative explanation, a de-
25 tailed description of such case.

1 (3) ANOMALOUS HEALTH INCIDENT SEN-
2 SORS.—

3 (A) A list of all types of sensors that the
4 Agency has developed or deployed with respect
5 to reports of anomalous health incidents, in-
6 cluding, for each type of sensor, the deployment
7 location, the date and the duration of the em-
8 ployment of such type of sensor, and, if applica-
9 ble, the reason for removal.

10 (B) A list of entities to which the Agency
11 has provided unrestricted access to data associ-
12 ated with anomalous health incidents.

13 (C) A list of requests for support the
14 Agency has received from elements of the Fed-
15 eral Government regarding sensor development,
16 testing, or deployment, and a description of the
17 support provided in each case.

18 (D) A description of all emitter signatures
19 obtained by sensors associated with anomalous
20 health incidents in Agency holdings since 2016,
21 including—

22 (i) the identification of any of such
23 emitters that the Agency prioritizes as a
24 threat; and

1 (ii) an explanation of such
2 prioritization.

3 (d) ADDITIONAL SUBMISSIONS.—Concurrent with
4 the submission of the report required by subsection (b),
5 the Director of the Central Intelligence Agency shall sub-
6 mit to the congressional intelligence committees—

7 (1) a template of each form required to apply
8 for the Expanded Care Program, including with re-
9 spect to payments for a qualifying injury or a quali-
10 fying injury to the brain;

11 (2) copies of internal guidance used by the
12 Agency to adjudicate claims for the Expanded Care
13 Program, including with respect to payments for a
14 qualifying injury to the brain;

15 (3) the case file of each applicant to the Ex-
16 panded Care Program who applied due to a reported
17 anomalous health incident, including supporting
18 medical documentation, with name and other identi-
19 fying information redacted;

20 (4) copies of all informational and instructional
21 materials provided to employees of and other individ-
22 uals affiliated with the Agency with respect to apply-
23 ing for the Expanded Care Program; and

24 (5) copies of Agency guidance provided to em-
25 ployees of and other individuals affiliated with the

1 Agency with respect to reporting and responding to
2 a suspected anomalous health incident, and the roles
3 and responsibilities of each element of the Agency
4 tasked with responding to a report of an anomalous
5 health incident.

6 (e) BRIEFING.—Not later than 90 days after the date
7 of the enactment of this Act, the Director of the Central
8 Intelligence Agency shall brief the congressional intel-
9 ligence committees on the report.

10 **TITLE X—ELECTION SECURITY**

11 **SEC. 1001. STRENGTHENING ELECTION CYBERSECURITY** 12 **TO UPHOLD RESPECT FOR ELECTIONS** 13 **THROUGH INDEPENDENT TESTING ACT OF** 14 **2023.**

15 (a) SHORT TITLE.—This section may be cited as the
16 “Strengthening Election Cybersecurity to Uphold Respect
17 for Elections through Independent Testing Act of 2023”
18 or the “SECURE IT Act of 2023”.

19 (b) REQUIRING PENETRATION TESTING AS PART OF
20 THE TESTING AND CERTIFICATION OF VOTING SYS-
21 TEMS.—Section 231 of the Help America Vote Act of
22 2002 (52 U.S.C. 20971) is amended by adding at the end
23 the following new subsection:

24 “(e) REQUIRED PENETRATION TESTING.—

1 “(1) IN GENERAL.—Not later than 180 days
2 after the date of the enactment of this subsection,
3 the Commission shall provide for the conduct of pen-
4 etration testing as part of the testing, certification,
5 decertification, and recertification of voting system
6 hardware and software by accredited laboratories
7 under this section.

8 “(2) ACCREDITATION.—The Director of the
9 National Institute of Standards and Technology
10 shall recommend to the Commission entities the Di-
11 rector proposes be accredited to carry out penetra-
12 tion testing under this subsection and certify compli-
13 ance with the penetration testing-related guidelines
14 required by this subsection. The Commission shall
15 vote on the accreditation of any entity recommended.
16 The requirements for such accreditation shall be a
17 subset of the requirements for accreditation of lab-
18 oratories under subsection (b) and shall only be
19 based on consideration of an entity’s competence to
20 conduct penetration testing under this subsection.”.

21 (c) INDEPENDENT SECURITY TESTING AND COORDI-
22 NATED CYBERSECURITY VULNERABILITY DISCLOSURE
23 PROGRAM FOR ELECTION SYSTEMS.—

24 (1) IN GENERAL.—Subtitle D of title II of the
25 Help America Vote Act of 2002 (42 U.S.C. 15401

1 et seq.) is amended by adding at the end the fol-
2 lowing new part:

3 **“PART 7—INDEPENDENT SECURITY TESTING AND**
4 **COORDINATED CYBERSECURITY VULNER-**
5 **ABILITY DISCLOSURE PILOT PROGRAM FOR**
6 **ELECTION SYSTEMS**

7 **“SEC. 297. INDEPENDENT SECURITY TESTING AND COORDI-**
8 **NATED CYBERSECURITY VULNERABILITY**
9 **DISCLOSURE PILOT PROGRAM FOR ELEC-**
10 **TION SYSTEMS.**

11 “(a) IN GENERAL.—

12 “(1) ESTABLISHMENT.—The Commission, in
13 consultation with the Secretary, shall establish an
14 Independent Security Testing and Coordinated Vul-
15 nerability Disclosure Pilot Program for Election Sys-
16 tems (VDP–E) (in this section referred to as the
17 ‘program’) in order to test for and disclose cyberse-
18 curity vulnerabilities in election systems.

19 “(2) DURATION.—The program shall be con-
20 ducted for a period of 5 years.

21 “(3) REQUIREMENTS.—In carrying out the pro-
22 gram, the Commission, in consultation with the Sec-
23 retary, shall—

24 “(A) establish a mechanism by which an
25 election systems vendor may make their election

1 system (including voting machines and source
2 code) available to cybersecurity researchers par-
3 ticipating in the program;

4 “(B) provide for the vetting of cybersecu-
5 rity researchers prior to their participation in
6 the program, including the conduct of back-
7 ground checks;

8 “(C) establish terms of participation
9 that—

10 “(i) describe the scope of testing per-
11 mitted under the program;

12 “(ii) require researchers to—

13 “(I) notify the vendor, the Com-
14 mission, and the Secretary of any cy-
15 bersecurity vulnerability they identify
16 with respect to an election system;
17 and

18 “(II) otherwise keep such vulner-
19 ability confidential for 180 days after
20 such notification;

21 “(iii) require the good-faith participa-
22 tion of all participants in the program;

23 “(iv) require an election system ven-
24 dor, after receiving notification of a critical
25 or high vulnerability (as defined by the

1 National Institute of Standards and Tech-
2 nology) in an election system of the ven-
3 dor, to—

4 “(I) send a patch or propound
5 some other fix or mitigation for such
6 vulnerability to the appropriate State
7 and local election officials, in con-
8 sultation with the researcher who dis-
9 covered it; and

10 “(II) notify the Commission and
11 the Secretary that such patch has
12 been sent to such officials;

13 “(D) in the case where a patch or fix to
14 address a vulnerability disclosed under subpara-
15 graph (C)(ii)(I) is intended to be applied to a
16 system certified by the Commission, provide—

17 “(i) for the expedited review of such
18 patch or fix within 90 days after receipt by
19 the Commission; and

20 “(ii) if such review is not completed
21 by the last day of such 90-day period, that
22 such patch or fix shall be deemed to be
23 certified by the Commission; and

24 “(E) 180 days after the disclosure of a
25 vulnerability under subparagraph (C)(ii)(I), no-

1 tify the Director of the Cybersecurity and In-
2 frastructure Security Agency of the vulner-
3 ability for inclusion in the database of Common
4 Vulnerabilities and Exposures.

5 “(4) VOLUNTARY PARTICIPATION; SAFE HAR-
6 BOR.—

7 “(A) VOLUNTARY PARTICIPATION.—Par-
8 ticipation in the program shall be voluntary for
9 election systems vendors and researchers.

10 “(B) SAFE HARBOR.—When conducting
11 research under this program, such research and
12 subsequent publication shall be considered to
13 be:

14 “(i) Authorized in accordance with
15 section 1030 of title 18, United States
16 Code (commonly known as the ‘Computer
17 Fraud and Abuse Act’), (and similar state
18 laws), and the election system vendor will
19 not initiate or support legal action against
20 the researcher for accidental, good-faith
21 violations of the program.

22 “(ii) Exempt from the anti-circumven-
23 tion rule of section 1201 of title 17, United
24 States Code (commonly known as the ‘Dig-
25 ital Millennium Copyright Act’), and the

1 election system vendor will not bring a
2 claim against a researcher for circumven-
3 tion of technology controls.

4 “(C) RULE OF CONSTRUCTION.—Nothing
5 in this paragraph may be construed to limit or
6 otherwise affect any exception to the general
7 prohibition against the circumvention of techno-
8 logical measures under subparagraph (A) of
9 section 1201(a)(1) of title 17, United States
10 Code, including with respect to any use that is
11 excepted from that general prohibition by the
12 Librarian of Congress under subparagraphs (B)
13 through (D) of such section 1201(a)(1).

14 “(5) EXEMPT FROM DISCLOSURE.—Cybersecu-
15 rity vulnerabilities discovered under the program
16 shall be exempt from section 552 of title 5, United
17 States Code (commonly referred to as the ‘Freedom
18 of Information Act’).

19 “(6) DEFINITIONS.—In this subsection:

20 “(A) CYBERSECURITY VULNERABILITY.—
21 The term ‘cybersecurity vulnerability’ means,
22 with respect to an election system, any security
23 vulnerability that affects the election system.

24 “(B) ELECTION INFRASTRUCTURE.—The
25 term ‘election infrastructure’ means—

1 “(i) storage facilities, polling places,
2 and centralized vote tabulation locations
3 used to support the administration of elec-
4 tions for public office; and

5 “(ii) related information and commu-
6 nications technology, including—

7 “(I) voter registration databases;

8 “(II) election management sys-
9 tems;

10 “(III) voting machines;

11 “(IV) electronic mail and other
12 communications systems (including
13 electronic mail and other systems of
14 vendors who have entered into con-
15 tracts with election agencies to sup-
16 port the administration of elections,
17 manage the election process, and re-
18 port and display election results); and

19 “(V) other systems used to man-
20 age the election process and to report
21 and display election results on behalf
22 of an election agency.

23 “(C) ELECTION SYSTEM.—The term ‘elec-
24 tion system’ means any information system that
25 is part of an election infrastructure, including

1 any related information and communications
2 technology described in subparagraph (B)(ii).

3 “(D) ELECTION SYSTEM VENDOR.—The
4 term ‘election system vendor’ means any person
5 providing, supporting, or maintaining an elec-
6 tion system on behalf of a State or local elec-
7 tion official.

8 “(E) INFORMATION SYSTEM.—The term
9 ‘information system’ has the meaning given the
10 term in section 3502 of title 44, United States
11 Code.

12 “(F) SECRETARY.—The term ‘Secretary’
13 means the Secretary of Homeland Security.

14 “(G) SECURITY VULNERABILITY.—The
15 term ‘security vulnerability’ has the meaning
16 given the term in section 102 of the Cybersecu-
17 rity Information Sharing Act of 2015 (6 U.S.C.
18 1501).”.

19 (2) CLERICAL AMENDMENT.—The table of con-
20 tents of such Act is amended by adding at the end
21 of the items relating to subtitle D of title II the fol-
22 lowing:

“PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSE-
CURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS

“Sec. 297. Independent security testing and coordinated cybersecurity vulner-
ability disclosure program for election systems.”.

1 **SEC. 1002. PROTECTING BALLOT MEASURES FROM FOR-**
2 **EIGN INFLUENCE ACT OF 2023.**

3 (a) **SHORT TITLE.**—This section may be cited as the
4 “Protecting Ballot Measures from Foreign Influence Act
5 of 2023”.

6 (b) **IN GENERAL.**—Section 319(a)(1)(A) of the Fed-
7 eral Election Campaign Act of 1971 (52 U.S.C.
8 30121(a)(1)(A)) is amended by inserting “, or a State or
9 local ballot initiative or ballot referendum” after “elec-
10 tion”.

11 (c) **EFFECTIVE DATE.**—The amendment made by
12 subsection (b) shall apply with respect to contributions
13 and donations made on or after the date of enactment of
14 this Act.

15 **TITLE XI—OTHER MATTERS**

16 **SEC. 1101. MODIFICATION OF REPORTING REQUIREMENT**
17 **FOR ALL-DOMAIN ANOMALY RESOLUTION OF-**
18 **FICE.**

19 Section 1683(k)(1) of the National Defense Author-
20 ization Act for Fiscal Year 2022 (50 U.S.C. 3373(k)(1)),
21 as amended by section 6802(a) of the Intelligence Author-
22 ization Act for Fiscal Year 2023 (Public Law 117–263),
23 is amended—

24 (1) in the heading, by striking “DIRECTOR OF
25 NATIONAL INTELLIGENCE AND SECRETARY OF DE-

1 FENSE” and inserting “ALL-DOMAIN ANOMALY RES-
2 OLUTION OFFICE”; and

3 (2) in subparagraph (A), by striking “Director
4 of National Intelligence and the Secretary of De-
5 fense shall jointly” and inserting “Director of the
6 Office shall”.

7 **SEC. 1102. MODIFICATIONS TO NOTIFICATION ON THE PRO-**
8 **VISION OF DEFENSE SENSITIVE SUPPORT.**

9 (a) MODIFICATION OF WHEN NOTIFICATION IS RE-
10 QUIRED.—Paragraph (3) of section 1055(b) of the Na-
11 tional Defense Authorization Act for Fiscal Year 2017
12 (Public Law 114–328; 10 U.S.C. 113 note) is amended—

13 (1) in the paragraph heading, by inserting
14 “AND EXTRAORDINARY SECURITY PROTECTIONS”
15 after “SUPPORT”;

16 (2) in the matter preceding subparagraph (A),
17 by inserting “or requires extraordinary security pro-
18 tections” after “time-sensitive”;

19 (3) in subparagraph (A), by inserting “or after
20 the activity supported concludes” after “providing
21 the support”; and

22 (4) in subparagraph (B)—

23 (A) by inserting “or after the activity sup-
24 ported concludes” after “providing such sup-
25 port”; and

1 (B) by inserting “or after the activity sup-
2 ported concludes” after “providing the sup-
3 port”.

4 (b) EXEMPTION.—Such section is amended by adding
5 at the end the following:

6 “(6) EXEMPTION.—The requirements of this
7 subsection shall not apply to the provision of defense
8 sensitive support for travel of the following:

9 “(A) The Director of National Intelligence.

10 “(B) The Principal Deputy Director of Na-
11 tional Intelligence.

12 “(C) The Director of the Central Intel-
13 ligence Agency.

14 “(D) The Deputy Director of the Central
15 Intelligence Agency.”.

16 **SEC. 1103. MODIFICATION OF CONGRESSIONAL OVERSIGHT**
17 **OF SPECIAL ACCESS PROGRAMS.**

18 Section 3236 of the National Nuclear Security Ad-
19 ministration Act (50 U.S.C. 2426) is amended—

20 (1) by striking “congressional defense commit-
21 tees” each place it appears and inserting “appro-
22 priate congressional committees”; and

23 (2) by adding at the end the following sub-
24 section:

1 “(g) APPROPRIATE CONGRESSIONAL COMMITTEES
2 DEFINED.—In this section, the term ‘appropriate congress-
3 sional committees’ means—

4 “(1) the congressional defense committees;

5 “(2) the Select Committee on Intelligence of the
6 Senate; and

7 “(3) the Permanent Select Committee on Intel-
8 ligence of the House of Representatives.”.

9 **SEC. 1104. FUNDING LIMITATIONS RELATING TO UNIDENTI-
10 FIED ANOMALOUS PHENOMENA.**

11 (a) DEFINITIONS.—In this section:

12 (1) APPROPRIATE COMMITTEES OF CON-
13 GRESS.—The term “appropriate committees of Con-
14 gress” means—

15 (A) the Select Committee on Intelligence,
16 the Committee on Armed Services, and the
17 Committee on Appropriations of the Senate;
18 and

19 (B) the Permanent Select Committee on
20 Intelligence, the Committee on Armed Services,
21 and the Committee on Appropriations of the
22 House of Representatives.

23 (2) CONGRESSIONAL LEADERSHIP.—The term
24 “congressional leadership” means—

25 (A) the majority leader of the Senate;

1 (B) the minority leader of the Senate;

2 (C) the Speaker of the House of Rep-
3 resentatives; and

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

6 (3) DIRECTOR.—The term “Director” means
7 the Director of the All-domain Anomaly Resolution
8 Office.

9 (4) UNIDENTIFIED ANOMALOUS PHENOMENA.—
10 The term “unidentified anomalous phenomena” has
11 the meaning given such term in section 1683(n) of
12 the National Defense Authorization Act for Fiscal
13 Year 2022 (50 U.S.C. 3373(n)), as amended by sec-
14 tion 6802(a) of the Intelligence Authorization Act
15 for Fiscal Year 2023 (Public Law 117–263).

16 (b) SENSE OF CONGRESS.—It is the sense of Con-
17 gress that, due to the increasing potential for technology
18 surprise from foreign adversaries and to ensure sufficient
19 integration across the United States industrial base and
20 avoid technology and security stovepipes—

21 (1) the United States industrial base must re-
22 tain its global lead in critical advanced technologies;
23 and

24 (2) the Federal Government must expand
25 awareness about any historical exotic technology

1 antecedents previously provided by the Federal Gov-
2 ernment for research and development purposes.

3 (c) LIMITATIONS.—

4 (1) IN GENERAL.—No amount authorized to be
5 appropriated or appropriated by this Act or any
6 other Act may be obligated or expended, directly or
7 indirectly, in part or in whole, for, on, in relation to,
8 or in support of activities involving unidentified
9 anomalous phenomena protected under any form of
10 special access or restricted access limitations that
11 have not been formally, officially, explicitly, and spe-
12 cifically described, explained, and justified to the ap-
13 propriate committees of Congress, congressional
14 leadership, and the Director, including for any ac-
15 tivities relating to the following:

16 (A) Recruiting, employing, training, equip-
17 ping, and operations of, and providing security
18 for, government or contractor personnel with a
19 primary, secondary, or contingency mission of
20 capturing, recovering, and securing unidentified
21 anomalous phenomena craft or pieces and com-
22 ponents of such craft.

23 (B) Analyzing such craft or pieces or com-
24 ponents thereof, including for the purpose of
25 determining properties, material composition,

1 method of manufacture, origin, characteristics,
2 usage and application, performance, operational
3 modalities, or reverse engineering of such craft
4 or component technology.

5 (C) Managing and providing security for
6 protecting activities and information relating to
7 unidentified anomalous phenomena from disclo-
8 sure or compromise.

9 (D) Actions relating to reverse engineering
10 or replicating unidentified anomalous phe-
11 nomena technology or performance based on
12 analysis of materials or sensor and observa-
13 tional information associated with unidentified
14 anomalous phenomena.

15 (E) The development of propulsion tech-
16 nology, or aerospace craft that uses propulsion
17 technology, systems, or subsystems, that is
18 based on or derived from or inspired by inspec-
19 tion, analysis, or reverse engineering of recov-
20 ered unidentified anomalous phenomena craft
21 or materials.

22 (F) Any aerospace craft that uses propul-
23 sion technology other than chemical propellants,
24 solar power, or electric ion thrust.

1 (2) FUTURE APPROPRIATIONS.—Paragraph (1)
2 shall apply with respect to an amount appropriated
3 after the date of the enactment of this Act, unless
4 such paragraph is specifically waived for such
5 amount, or such amount is specifically exempted
6 from such paragraph, by an Act enacted after the
7 date of the enactment of this Act.

8 (d) NOTIFICATION AND REPORTING.—Any person
9 currently or formerly under contract with the Federal
10 Government that has in their possession material or infor-
11 mation provided by or derived from the Federal Govern-
12 ment relating to unidentified anomalous phenomena that
13 formerly or currently is protected by any form of special
14 access or restricted access shall—

15 (1) not later than 60 days after the date of the
16 enactment of this Act, notify the Director of such
17 possession; and

18 (2) not later than 180 days after the date of
19 the enactment of this Act, make available to the Di-
20 rector for assessment, analysis, and inspection—

21 (A) all such material and information; and

22 (B) a comprehensive list of all non-earth
23 origin or exotic unidentified anomalous phe-
24 nomena material.

1 (e) LIABILITY.—No criminal or civil action may lie
2 or be maintained in any Federal or State court against
3 any person for receiving material or information described
4 in subsection (d) if that person complies with the notifica-
5 tion and reporting provisions described in such subsection.

6 (f) LIMITATION REGARDING INDEPENDENT RE-
7 SEARCH AND DEVELOPMENT.—

8 (1) IN GENERAL.—Consistent with Department
9 of Defense Instruction Number 3204.01 (dated Au-
10 gust 20, 2014, incorporating change 2, dated July
11 9, 2020; relating to Department policy for oversight
12 of independent research and development), inde-
13 pendent research and development funding relating
14 to material or information described in subsection
15 (c) shall not be allowable as indirect expenses for
16 purposes of contracts covered by such instruction,
17 unless such material and information is made avail-
18 able to the Director in accordance with subsection
19 (d).

20 (2) EFFECTIVE DATE AND APPLICABILITY.—
21 Paragraph (1) shall take effect on the date that is
22 60 days after the date of the enactment of this Act
23 and shall apply with respect to funding from
24 amounts appropriated before, on, or after such date.

1 (g) NOTICE TO CONGRESS.—Not later than 30 days
2 after the date on which the Director has received a notifi-
3 cation under paragraph (1) of subsection (d) or informa-
4 tion or material under paragraph (2) of such subsection,
5 the Director shall provide written notification of such re-
6 ceipt to the appropriate committees of Congress and con-
7 gressional leadership.

Calendar No. 106

118TH CONGRESS
1ST Session
S. 2103

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.

JUNE 22, 2023

Read twice and placed on the calendar