

Calendar No. 412

118TH CONGRESS
2D SESSION**S. 4443**

To authorize appropriations for fiscal year 2025 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 3, 2024

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 2025 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 2025”.

- 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

Sec. 301. Improvements relating to conflicts of interest in the Intelligence Innovation Board.
 Sec. 302. National Threat Identification and Prioritization Assessment and National Counterintelligence Strategy.
 Sec. 303. Open Source Intelligence Division of Office of Intelligence and Analysis personnel.
 Sec. 304. Appointment of Director of the Office of Intelligence and Counterintelligence.
 Sec. 305. Improvements to advisory board of National Reconnaissance Office.
 Sec. 306. National Intelligence University acceptance of grants.
 Sec. 307. Protection of Central Intelligence Agency facilities and assets from unmanned aircraft.
 Sec. 308. Limitation on availability of funds for new controlled access programs.
 Sec. 309. Limitation on transfers from controlled access programs.
 Sec. 310. Expenditure of funds for certain intelligence and counterintelligence activities of the Coast Guard.
 Sec. 311. Unauthorized access to intelligence community property.
 Sec. 312. Strengthening of Office of Intelligence and Analysis.
 Sec. 313. Report on sensitive commercially available information.
 Sec. 314. Policy on collection of United States location information.
 Sec. 315. Display of flags, seals, and emblems other than the United States flag.

TITLE IV—COUNTERING FOREIGN THREATS

Subtitle A—People’s Republic of China

Sec. 401. Strategy and outreach on risks posed by People’s Republic of China smartport technology.
 Sec. 402. Assessment of current status of biotechnology of People’s Republic of China.
 Sec. 403. Intelligence sharing with law enforcement agencies on synthetic opioid precursor chemicals originating in People’s Republic of China.
 Sec. 404. Report on efforts of the People’s Republic of China to evade United States transparency and national security regulations.

Sec. 405. Plan for recruitment of Mandarin speakers.

Subtitle B—The Russian Federation

Sec. 411. Assessment of Russian Federation sponsorship of acts of international terrorism.

Sec. 412. Assessment of likely course of war in Ukraine.

Subtitle C—International Terrorism

Sec. 421. Inclusion of Hamas, Hezbollah, Al-Qaeda, and ISIS officials and members among aliens engaged in terrorist activity.

Sec. 422. Assessment and report on the threat of ISIS-Khorasan to the United States.

Sec. 423. Terrorist financing prevention.

Subtitle D—Other Foreign Threats

Sec. 431. Assessment of visa-free travel to and within Western Hemisphere by nationals of countries of concern.

Sec. 432. Study on threat posed by foreign investment in United States agricultural land.

Sec. 433. Assessment of threat posed by citizenship-by-investment programs.

Sec. 434. Mitigating the use of United States components and technology in hostile activities by foreign adversaries.

Sec. 435. Office of Intelligence and Counterintelligence review of visitors and assignees.

Sec. 436. Prohibition on National Laboratories admitting certain foreign nationals.

Sec. 437. Quarterly report on certain foreign nationals encountered at the United States border.

Sec. 438. Assessment of the lessons learned by the intelligence community with respect to the Israel-Hamas war.

Sec. 439. Central Intelligence Agency intelligence assessment on Tren de Aragua.

Sec. 440. Assessment of Maduro regime's economic and security relationships with state sponsors of terrorism and foreign terrorist organizations.

Sec. 441. Continued congressional oversight of Iranian expenditures supporting foreign military and terrorist activities.

TITLE V—EMERGING TECHNOLOGIES

Sec. 501. Strategy to counter foreign adversary efforts to utilize biotechnologies in ways that threaten United States national security.

Sec. 502. Improvements to the roles, missions, and objectives of the National Counterproliferation and Biosecurity Center.

Sec. 503. Enhancing capabilities to detect foreign adversary threats relating to biological data.

Sec. 504. National security procedures to address certain risks and threats relating to artificial intelligence.

Sec. 505. Establishment of Artificial Intelligence Security Center.

Sec. 506. Sense of Congress encouraging intelligence community to increase private sector capital partnerships and partnership with Office of Strategic Capital of Department of Defense to secure enduring technological advantages.

Sec. 507. Intelligence Community Technology Bridge Fund.

- Sec. 508. Enhancement of authority for intelligence community public-private talent exchanges.
- Sec. 509. Enhancing intelligence community ability to acquire emerging technology that fulfills intelligence community needs.
- Sec. 510. Management of artificial intelligence security risks.
- Sec. 511. Protection of technological measures designed to verify authenticity or provenance of machine-manipulated media.
- Sec. 512. Sense of Congress on hostile foreign cyber actors.
- Sec. 513. Designation of state sponsors of ransomware and reporting requirements.
- Sec. 514. Deeming ransomware threats to critical infrastructure a national intelligence priority.

TITLE VI—CLASSIFICATION REFORM

- Sec. 601. Governance of classification and declassification system.
- Sec. 602. Classification and declassification of information.
- Sec. 603. Minimum standards for Executive agency insider threat programs.

TITLE VII—SECURITY CLEARANCES AND INTELLIGENCE COMMUNITY WORKFORCE IMPROVEMENTS

- Sec. 701. Security clearances held by certain former employees of intelligence community.
- Sec. 702. Policy for authorizing intelligence community program of contractor-owned and contractor-operated sensitive compartmented information facilities.
- Sec. 703. Enabling intelligence community integration.
- Sec. 704. Appointment of spouses of certain Federal employees.
- Sec. 705. Plan for staffing the intelligence collection positions of the Central Intelligence Agency.
- Sec. 706. Intelligence community workplace protections.
- Sec. 707. Sense of Congress on Government personnel support for foreign terrorist organizations.

TITLE VIII—WHISTLEBLOWERS

- Sec. 801. Improvements regarding urgent concerns submitted to Inspectors General of the intelligence community.
- Sec. 802. Prohibition against disclosure of whistleblower identity as act of reprisal.
- Sec. 803. Protection for individuals making authorized disclosures to Inspectors General of elements of the intelligence community.
- Sec. 804. Clarification of authority of certain Inspectors General to receive protected disclosures.
- Sec. 805. Whistleblower protections relating to psychiatric testing or examination.
- Sec. 806. Establishing process parity for adverse security clearance and access determinations.
- Sec. 807. Elimination of cap on compensatory damages for retaliatory revocation of security clearances and access determinations.

TITLE IX—ANOMALOUS HEALTH INCIDENTS

- Sec. 901. Additional discretion for Director of Central Intelligence Agency in paying costs of treating qualifying injuries and making payments for qualifying injuries to the brain.

- Sec. 902. Additional discretion for Secretary of State and heads of other Federal agencies in paying costs of treating qualifying injuries and making payments for qualifying injuries to the brain.
- Sec. 903. Improved funding flexibility for payments made by Department of State for qualifying injuries to the brain.

TITLE X—UNIDENTIFIED ANOMALOUS PHENOMENA

- Sec. 1001. Comptroller General of the United States review of All-domain Anomaly Resolution Office.
- Sec. 1002. Sunset of requirements relating to audits of unidentified anomalous phenomena historical record report.
- Sec. 1003. Funding limitations relating to unidentified anomalous phenomena.

TITLE XI—AIR AMERICA

- Sec. 1101. Short title.
- Sec. 1102. Findings.
- Sec. 1103. Definitions.
- Sec. 1104. Award authorized to eligible persons.
- Sec. 1105. Funding limitation.
- Sec. 1106. Time limitation.
- Sec. 1107. Application procedures.
- Sec. 1108. Rule of construction.
- Sec. 1109. Attorneys' and agents' fees.
- Sec. 1110. No judicial review.
- Sec. 1111. Reports to Congress.

TITLE XII—OTHER MATTERS

- Sec. 1201. Enhanced authorities for amicus curiae under the Foreign Intelligence Surveillance Act of 1978.
- Sec. 1202. Limitation on directives under Foreign Intelligence Surveillance Act of 1978 relating to certain electronic communication service providers.
- Sec. 1203. Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2024.
- Sec. 1204. Privacy and Civil Liberties Oversight Board qualifications.
- Sec. 1205. Parity in pay for staff of the Privacy and Civil Liberties Oversight Board and the intelligence community.
- Sec. 1206. Modification and repeal of reporting requirements.
- Sec. 1207. Technical amendments.

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

1 3 of the National Security Act of 1947 (50 U.S.C.
2 3003).

3 (2) INTELLIGENCE COMMUNITY.—The term
4 “intelligence community” has the meaning given
5 such term in such section.

6 **TITLE I—INTELLIGENCE**
7 **ACTIVITIES**

8 **SEC. 101. AUTHORIZATION OF APPROPRIATIONS.**

9 Funds are hereby authorized to be appropriated for
10 fiscal year 2025 for the conduct of the intelligence and
11 intelligence-related activities of the Federal Government.

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

13 (a) SPECIFICATIONS OF AMOUNTS.—The amounts
14 authorized to be appropriated under section 101 for the
15 conduct of the intelligence activities of the Federal Gov-
16 ernment are those specified in the classified Schedule of
17 Authorizations prepared to accompany this Act.

18 (b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AU-
19 THORIZATIONS.—

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

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

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

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

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

16 (C) as otherwise required by law.

17 **SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT AC-**
 18 **COUNT.**

19 (a) AUTHORIZATION OF APPROPRIATIONS.—There is
 20 authorized to be appropriated for the Intelligence Commu-
 21 nity Management Account of the Director of National In-
 22 telligence for fiscal year 2025 the sum of \$656,573,000.

23 (b) CLASSIFIED AUTHORIZATION OF APPROPRIA-
 24 TIONS.—In addition to amounts authorized to be appro-
 25 priated for the Intelligence Community Management Ac-

1 count by subsection (a), there are authorized to be appro-
2 priated for the Intelligence Community Management Ac-
3 count for fiscal year 2025 such additional amounts as are
4 specified in the classified Schedule of Authorizations re-
5 ferred to in section 102(a).

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

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

13 **TITLE II—CENTRAL INTEL-**
14 **LIGENCE AGENCY RETIRE-**
15 **MENT AND DISABILITY SYS-**
16 **TEM**

17 **SEC. 201. AUTHORIZATION OF APPROPRIATIONS.**

18 There is authorized to be appropriated for the Cen-
19 tral Intelligence Agency Retirement and Disability Fund
20 \$514,000,000 for fiscal year 2025.

TITLE III—INTELLIGENCE COMMUNITY MATTERS

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

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

(1) in paragraph (2)—

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

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

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

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

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

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

1 “(ii) every waiver for a potential con-
 2 flict of interest requires review and ap-
 3 proval by the Director of National Intel-
 4 ligence; and

5 “(iii) for every waiver granted, the
 6 designated agency ethics official shall sub-
 7 mit to the congressional intelligence com-
 8 mittees notice of the waiver.”; and

9 (2) by adding at the end the following:

10 “(3) DEFINITION OF DESIGNATED AGENCY
 11 ETHICS OFFICIAL.—In this subsection, the term
 12 ‘designated agency ethics official’ means the des-
 13 ignated agency ethics official (as defined in section
 14 13101 of title 5, United States Code) in the Office
 15 of the Director of National Intelligence.”.

16 **SEC. 302. NATIONAL THREAT IDENTIFICATION AND**
 17 **PRIORITIZATION ASSESSMENT AND NA-**
 18 **TIONAL COUNTERINTELLIGENCE STRATEGY.**

19 Section 904(f)(3) of the Counterintelligence En-
 20 hancement Act of 2002 (50 U.S.C. 3383(f)(3)) is amend-
 21 ed by striking “National Counterintelligence Executive”
 22 and inserting “Director of the National Counterintel-
 23 ligence and Security Center”.

1 **SEC. 303. OPEN SOURCE INTELLIGENCE DIVISION OF OF-**
2 **FICE OF INTELLIGENCE AND ANALYSIS PER-**
3 **SONNEL.**

4 None of the funds authorized to be appropriated by
5 this Act or otherwise made available for fiscal year 2025
6 for the Office of Intelligence and Analysis of the Depart-
7 ment of Homeland Security may be obligated or expended
8 by the Office to increase, above the staffing level in effect
9 on the day before the date of the enactment of this Act,
10 the number of personnel assigned to the Open Source In-
11 telligence Division who work exclusively or predominantly
12 on domestic terrorism issues.

13 **SEC. 304. APPOINTMENT OF DIRECTOR OF THE OFFICE OF**
14 **INTELLIGENCE AND COUNTERINTEL-**
15 **LIGENCE.**

16 (a) IN GENERAL.—Section 215(c) of the Department
17 of Energy Organization Act (42 U.S.C. 7144b(c)) is
18 amended to read as follows:

19 “(c) DIRECTOR.—

20 “(1) APPOINTMENT.—The head of the Office
21 shall be the Director of the Office of Intelligence and
22 Counterintelligence, who shall be appointed by the
23 President, by and with the advice and consent of the
24 Senate. The Director of the Office shall report di-
25 rectly to the Secretary.

26 “(2) TERM.—

1 “(A) IN GENERAL.—The Director shall
2 serve for a term of 6 years.

3 “(B) REAPPOINTMENT.—The Director
4 shall be eligible for reappointment for 1 or more
5 terms.

6 “(3) QUALIFICATIONS.—The Director shall—

7 “(A) be an employee in the Senior Execu-
8 tive Service, the Senior Intelligence Service, the
9 Senior National Intelligence Service, or any
10 other Service that the Secretary, in coordina-
11 tion with the Director of National Intelligence,
12 considers appropriate; and

13 “(B) have substantial expertise in matters
14 relating to the intelligence community, includ-
15 ing foreign intelligence and counterintel-
16 ligence.”.

17 (b) EFFECTIVE DATE.—The amendment made by
18 this section shall take effect on January 21, 2025.

19 **SEC. 305. IMPROVEMENTS TO ADVISORY BOARD OF NA-**
20 **TIONAL RECONNAISSANCE OFFICE.**

21 Section 106A(d) of the National Security Act of 1947
22 (50 U.S.C. 3041a(d)) is amended—

23 (1) in paragraph (3)(A)—

24 (A) in clause (i)—

1 (i) by striking “five members ap-
 2 pointed by the Director, in consultation
 3 with the Director of National Intelligence
 4 and the Secretary of Defense,” and insert-
 5 ing “up to 8 members appointed by the
 6 Director”; and

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

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

12 (C) by inserting after clause (i) the fol-
 13 lowing:

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

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

22 (3) by inserting after paragraph (4) the fol-
 23 lowing:

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

1 “(A) Mandatory processes for identifying
2 potential conflicts of interest, including the sub-
3 mission of initial and periodic financial disclo-
4 sures by Board members.

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

10 “(C) The establishment of a process and
11 associated protections for any whistleblower al-
12 leging a violation of applicable conflict of inter-
13 est law, Federal contracting law, or other provi-
14 sion of law.”; and

15 (4) in paragraph (8), as redesignated by para-
16 graph (2), by striking “September 30, 2024” and in-
17 serting “August 31, 2027”.

18 **SEC. 306. NATIONAL INTELLIGENCE UNIVERSITY ACCEPT-**
19 **ANCE OF GRANTS.**

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

1 **“§ 1035. National Intelligence University acceptance**
2 **of grants**

3 “(a) AUTHORITY.—The Director of National Intel-
4 ligence may authorize the President of the National Intel-
5 ligence University to accept qualifying research grants.

6 “(b) QUALIFYING GRANTS.—A qualifying research
7 grant under this section is a grant that is awarded on a
8 competitive basis by an entity referred to in subsection (c)
9 for a research project with a scientific, literary, or edu-
10 cational purpose.

11 “(c) ENTITIES FROM WHICH GRANTS MAY BE AC-
12 CEPTED.—A qualifying research grant may be accepted
13 under this section only from a Federal agency or from a
14 corporation, fund, foundation, educational institution, or
15 similar entity that is organized and operated primarily for
16 scientific, literary, or educational purposes.

17 “(d) ADMINISTRATION OF GRANT FUNDS.—

18 “(1) ESTABLISHMENT OF ACCOUNT.—The Di-
19 rector shall establish an account for administering
20 funds received as qualifying research grants under
21 this section.

22 “(2) USE OF FUNDS.—The President of the
23 University shall use the funds in the account estab-
24 lished pursuant to paragraph (1) in accordance with
25 applicable provisions of the regulations and the
26 terms and conditions of the grants received.

1 “(e) RELATED EXPENSES.—Subject to such limita-
 2 tions as may be provided in appropriations Acts, appro-
 3 priations available for the National Intelligence University
 4 may be used to pay expenses incurred by the University
 5 in applying for, and otherwise pursuing, the award of
 6 qualifying research grants.

7 “(f) REGULATIONS.—The Director of National Intel-
 8 ligence shall prescribe regulations for the administration
 9 of this section.”.

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

“Sec. 1035. National Intelligence University acceptance of grants.”.

14 **SEC. 307. PROTECTION OF CENTRAL INTELLIGENCE AGEN-**
 15 **CY FACILITIES AND ASSETS FROM UN-**
 16 **MANNED AIRCRAFT.**

17 The Central Intelligence Agency Act of 1949 (50
 18 U.S.C. 3501 et seq.) is amended by inserting after section
 19 15 the following new section (and conforming the table
 20 of contents at the beginning of such Act accordingly):

21 **“SEC. 15A. PROTECTION OF CERTAIN FACILITIES AND AS-**
 22 **SETS FROM UNMANNED AIRCRAFT.**

23 “(a) DEFINITIONS.—In this section:

24 “(1) BUDGET.—The term ‘budget’, with respect
 25 to a fiscal year, means the budget for that fiscal

1 year that is submitted to Congress by the President
2 under section 1105(a) of title 31, United States
3 Code.

4 “(2) CONGRESSIONAL INTELLIGENCE COMMIT-
5 TEES.—The term ‘congressional intelligence commit-
6 tees’ means—

7 “(A) the Select Committee on Intelligence
8 of the Senate;

9 “(B) the Permanent Select Committee on
10 Intelligence of the House of Representatives;

11 “(C) the Subcommittee on Defense of the
12 Committee on Appropriations of the Senate;
13 and

14 “(D) the Subcommittee on Defense of the
15 Committee on Appropriations of the House of
16 Representatives.

17 “(3) CONGRESSIONAL JUDICIARY COMMIT-
18 TEES.—The term ‘congressional judiciary commit-
19 tees’ means—

20 “(A) the Committee on the Judiciary of
21 the Senate; and

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

24 “(4) CONGRESSIONAL TRANSPORTATION AND
25 INFRASTRUCTURE COMMITTEES.—The term ‘con-

1 gressional transportation and infrastructure commit-
2 tees’ means—

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

5 “(B) the Committee on Transportation
6 and Infrastructure of the House of Representa-
7 tives.

8 “(5) COVERED FACILITY OR ASSET.—The term
9 ‘covered facility or asset’ means property owned,
10 leased, or controlled by the Agency, property con-
11 trolled and occupied by the Federal Highway Admin-
12 istration, located immediately adjacent to the head-
13 quarters compound of the Agency, and property
14 owned, leased, or controlled by the Office of the Di-
15 rector of National Intelligence where the property—

16 “(A) is identified as high-risk and a poten-
17 tial target for unlawful unmanned aircraft ac-
18 tivity by the Director, in coordination with the
19 Secretary of Transportation, with respect to po-
20 tentially impacted airspace, through a risk-
21 based assessment for purposes of this section;

22 “(B) is located in the United States and
23 beneath airspace that is prohibited or restricted
24 by the Federal Aviation Administration;

1 “(C) is a property of which Congress has
2 been notified is covered under this paragraph;
3 and

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

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

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

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

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

22 “(10) RISK-BASED ASSESSMENT.—The term
23 ‘risk-based assessment’ includes an evaluation of
24 threat information specific to a covered facility or
25 asset and, with respect to potential impacts on the

1 safety and efficiency of the National Airspace Sys-
2 tem and the needs of national security at each cov-
3 ered facility or asset identified by the Director, an
4 evaluation of each of the following factors:

5 “(A) Potential impacts to safety, efficiency,
6 and use of the National Airspace System, in-
7 cluding potential effects on manned aircraft and
8 unmanned aircraft systems, aviation safety, air-
9 port operations, infrastructure, and air naviga-
10 tion services relating to the use of any system
11 or technology for carrying out the actions de-
12 scribed in subsection (c)(1).

13 “(B) Options for mitigating any identified
14 impacts to the National Airspace System relat-
15 ing to the use of any system or technology, in-
16 cluding minimizing when possible the use of any
17 system or technology that disrupts the trans-
18 mission of radio or electronic signals, for car-
19 rying out the actions described in subsection
20 (c)(1).

21 “(C) Potential consequences of the effects
22 of any actions taken under subsection (c)(1) to
23 the National Airspace System and infrastruc-
24 ture if not mitigated.

1 “(D) The ability to provide reasonable ad-
2 vance notice to aircraft operators consistent
3 with the safety of the National Airspace System
4 and the needs of national security.

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

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

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

18 “(12) UNMANNED AIRCRAFT; UNMANNED AIR-
19 CRAFT SYSTEM.—The terms ‘unmanned aircraft’
20 and ‘unmanned aircraft system’ have the meanings
21 given those terms in section 44801 of title 49,
22 United States Code.

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

1 “(b) AUTHORITY.—Notwithstanding section 46502 of
2 title 49, United States Code, or sections 32, 1030, and
3 1367 and chapters 119 and 206 of title 18, United States
4 Code, or section 705 of the Communications Act of 1934
5 (47 U.S.C. 605), the Director may take, and may author-
6 ize Agency personnel with assigned duties that include the
7 security or protection of people, facilities, or assets within
8 the United States to take—

9 “(1) such actions described in subsection (c)(1)
10 that are necessary to mitigate a credible threat (as
11 defined by the Director, in consultation with the
12 Secretary of Transportation) that an unmanned air-
13 craft system or unmanned aircraft poses to the safe-
14 ty or security of a covered facility or asset; and

15 “(2) such actions described in subsection (c)(3).

16 “(c) ACTIONS.—

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

19 “(A) During the operation of the un-
20 manned aircraft system, detect, identify, mon-
21 itor, and track the unmanned aircraft system or
22 unmanned aircraft, without prior consent, in-
23 cluding by means of intercept or other access of
24 a wire communication, an oral communication,
25 or an electronic communication used to control

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

3 “(B) Warn the operator of the unmanned
4 aircraft system or unmanned aircraft, including
5 by passive or active and by direct or indirect
6 physical, electronic, radio, or electromagnetic
7 means.

8 “(C) Disrupt control of the unmanned air-
9 craft system or unmanned aircraft, without
10 prior consent, including by disabling the un-
11 manned aircraft system or unmanned aircraft
12 by intercepting, interfering, or causing inter-
13 ference with wire, oral, electronic, or radio com-
14 munications used to control the unmanned air-
15 craft system or unmanned aircraft.

16 “(D) Seize or exercise control over the un-
17 manned aircraft system or unmanned aircraft.

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

20 “(F) Use reasonable force, if necessary, to
21 seize or otherwise disable, damage, or destroy
22 the unmanned aircraft system or unmanned air-
23 craft.

1 “(2) COORDINATION.—The Director shall de-
2 velop the actions described in paragraph (1) in co-
3 ordination with the Secretary of Transportation.

4 “(3) RESEARCH, TESTING, TRAINING, AND
5 EVALUATION.—

6 “(A) IN GENERAL.—The Director shall
7 conduct research, testing, training on, and eval-
8 uation of any equipment, including any elec-
9 tronic equipment, to determine the capability
10 and utility of the equipment prior to the use of
11 the equipment for any action described in para-
12 graph (1).

13 “(B) PERSONNEL.—Personnel and con-
14 tractors who do not have assigned duties that
15 include the security or protection of people, fa-
16 cilities, or assets may engage in research, test-
17 ing, training, and evaluation activities pursuant
18 to subparagraph (A).

19 “(4) FAA COORDINATION.—The Director shall
20 coordinate with the Administrator of the Federal
21 Aviation Administration on any action described in
22 paragraph (1) or (3) so the Administrator may en-
23 sure that unmanned aircraft system detection and
24 mitigation systems do not adversely affect or inter-
25 fere with safe airport operations, navigation, air

1 traffic services, or the safe and efficient operation of
2 the National Airspace System.

3 “(d) FORFEITURE.—Any unmanned aircraft system
4 or unmanned aircraft that is seized pursuant to subsection
5 (b) as described in subsection (c)(1) is subject to forfeiture
6 to the United States.

7 “(e) REGULATIONS AND GUIDANCE.—

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

12 “(2) COORDINATION.—

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

17 “(B) AVIATION SAFETY.—The Director
18 shall coordinate with the Secretary of Transpor-
19 tation and the Administrator of the Federal
20 Aviation Administration before issuing any
21 guidance, or otherwise implementing this sec-
22 tion, so the Administrator may ensure that un-
23 manned aircraft system detection and mitiga-
24 tion systems do not adversely affect or interfere
25 with safe airport operations, navigation, air

1 traffic services, or the safe and efficient oper-
2 ation of the National Airspace System.

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

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

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

17 “(3) records of such communications are main-
18 tained only for as long as necessary, and in no event
19 for more than 180 days, unless the Director deter-
20 mines that maintenance of such records for a longer
21 period is necessary for the investigation or prosecu-
22 tion of a violation of law, to fulfill a duty, responsi-
23 bility, or function of the Agency, is required under
24 Federal law, or for the purpose of any litigation; and

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

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

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

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

15 “(D) would support the enforcement activi-
16 ties of a regulatory agency of the Federal Gov-
17 ernment in connection with a criminal or civil
18 investigation of, or any regulatory, statutory, or
19 other enforcement action relating to, an action
20 described in subsection (b);

21 “(E) is necessary to protect against dan-
22 gerous or unauthorized activity by unmanned
23 aircraft systems or unmanned aircraft;

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

1 “(G) is otherwise required by law.

2 “(g) BUDGET.—

3 “(1) IN GENERAL.—The Director shall submit
4 to the congressional intelligence committees, as a
5 part of the budget request of the Agency for each
6 fiscal year after fiscal year 2025, a consolidated
7 funding display that identifies the funding source for
8 the actions described in subsection (c)(1) within the
9 Agency.

10 “(2) FORM.—Each funding display submitted
11 pursuant to paragraph (1) shall be in unclassified
12 form, but may contain a classified annex.

13 “(h) SEMIANNUAL BRIEFINGS AND NOTIFICA-
14 TIONS.—

15 “(1) BRIEFINGS.—Not later than 180 days
16 after the date of the enactment of the Intelligence
17 Authorization Act for Fiscal Year 2025 and semi-
18 annually thereafter, the Director shall provide the
19 congressional intelligence committees, the congress-
20 sional judiciary committees, and the congressional
21 transportation and infrastructure committees a
22 briefing on the activities carried out pursuant to this
23 section during the period covered by the briefing.

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

4 “(3) CONTENTS.—Each briefing under para-
5 graph (1) shall include, for the period covered by the
6 briefing, the following:

7 “(A) Policies, programs, and procedures to
8 mitigate or eliminate the effects of the activities
9 described in paragraph (1) to the National Air-
10 space System and other critical national trans-
11 portation infrastructure.

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

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

24 “(D) A description of options considered
25 and steps taken to mitigate any identified ef-

fects on the National Airspace System relating to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

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

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

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

“(H) An assessment of whether any gaps or insufficiencies remain in statutes, regulations, and policies that impede the ability of the Agency to counter the threat posed by the mali-

1 cious use of unmanned aircraft systems and un-
2 manned aircraft and any recommendations to
3 remedy such gaps or insufficiencies.

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

7 “(5) NOTIFICATION.—

8 “(A) IN GENERAL.—Within 30 days of de-
9 ploying any new technology to carry out the ac-
10 tions described in subsection (c)(1), the Direc-
11 tor shall submit to the congressional intelligence
12 committees a notification of the deployment of
13 such technology.

14 “(B) CONTENTS.—Each notification sub-
15 mitted pursuant to subparagraph (A) shall in-
16 clude a description of options considered to
17 mitigate any identified effects on the National
18 Airspace System relating to the use of any sys-
19 tem or technology, including the minimization
20 of the use of any technology that disrupts the
21 transmission of radio or electronic signals, for
22 carrying out the actions described in subsection
23 (c)(1).

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

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

4 “(2) to vest in the Secretary of Transportation
5 or the Administrator of the Federal Aviation Admin-
6 istration any authority of the Director.

7 “(j) TERMINATION.—

8 “(1) IN GENERAL.—Except as provided in para-
9 graph (2), the authority to carry out this section
10 with respect to the actions specified in subpara-
11 graphs (B) through (F) of subsection (c)(1), shall
12 terminate on the date that is 4 years after the date
13 of the enactment of the Intelligence Authorization
14 Act for Fiscal Year 2025.

15 “(2) EXTENSION.—The President may extend
16 by 1 year the termination date specified in para-
17 graph (1) if, before termination, the President cer-
18 tifies to Congress that such extension is in the na-
19 tional security interests of the United States.

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

1 **SEC. 308. LIMITATION ON AVAILABILITY OF FUNDS FOR**
 2 **NEW CONTROLLED ACCESS PROGRAMS.**

3 None of the funds authorized to be appropriated by
 4 this Act or otherwise made available for fiscal year 2025
 5 for the National Intelligence Program may be obligated
 6 or expended for any controlled access program (as defined
 7 in section 501A(d) of the National Security Act of 1947
 8 (50 U.S.C. 3091a(d))), or a compartment or subcompartment
 9 therein, that is established on or after the date of
 10 the enactment of this Act, until the head of the element
 11 of the intelligence community responsible for the establish-
 12 ment of such program, compartment, or subcompartment,
 13 submits the notification required by section 501A(b) of the
 14 National Security Act of 1947 (50 U.S.C. 3091a(b)).

15 **SEC. 309. LIMITATION ON TRANSFERS FROM CONTROLLED**
 16 **ACCESS PROGRAMS.**

17 Section 501A(b) of the National Security Act of 1947
 18 (50 U.S.C. 3091a(b)) is amended—

19 (1) in the subsection heading, by striking “LIM-
 20 ITATION ON ESTABLISHMENT” and inserting “LIMI-
 21 TATIONS”;

22 (2) by striking “A head” and inserting the fol-
 23 lowing:

24 “(1) ESTABLISHMENT.—A head”; and

25 (3) by adding at the end the following:

1 “(2) TRANSFERS.—A head of an element of the
 2 intelligence community may not transfer a capability
 3 from a controlled access program, including from a
 4 compartment or subcompartment therein to a com-
 5 partment or subcompartment of another controlled
 6 access program, to a special access program (as de-
 7 fined in section 1152(g) of the National Defense Au-
 8 thorization Act for Fiscal Year 1994 (50 U.S.C.
 9 3348(g))), or to anything else outside the controlled
 10 access program, until the head submits to the appro-
 11 priate congressional committees and congressional
 12 leadership notice of the intent of the head to make
 13 such transfer.”.

14 **SEC. 310. EXPENDITURE OF FUNDS FOR CERTAIN INTEL-**
 15 **LIGENCE AND COUNTERINTELLIGENCE AC-**
 16 **TIVITIES OF THE COAST GUARD.**

17 The Commandant of the Coast Guard may use up
 18 to 1 percent of the amounts made available for the Na-
 19 tional Intelligence Program (as such term is defined in
 20 section 3 of the National Security Act of 1947 (50 U.S.C.
 21 3003)) for each fiscal year for intelligence and counter-
 22 intelligence activities of the Coast Guard relating to ob-
 23 jects of a confidential, extraordinary, or emergency nature,
 24 which amounts may be accounted for solely on the certifi-
 25 cation of the Commandant and each such certification

1 shall be considered to be a sufficient voucher for the
2 amount contained in the certification.

3 **SEC. 311. UNAUTHORIZED ACCESS TO INTELLIGENCE COM-**
4 **MUNITY PROPERTY.**

5 (a) IN GENERAL.—The National Security Act of
6 1947 (50 U.S.C. 3001 et seq.) is amended by adding at
7 the end the following:

8 **“SEC. 1115. UNAUTHORIZED ACCESS TO INTELLIGENCE**
9 **COMMUNITY PROPERTY.**

10 “(a) IN GENERAL.—It shall be unlawful, within the
11 jurisdiction of the United States, without authorization to
12 access any property that—

13 “(1) is under the jurisdiction of an element of
14 the intelligence community; and

15 “(2) has been clearly marked as closed or re-
16 stricted.

17 “(b) PENALTIES.—Any person who violates sub-
18 section (a) shall—

19 “(1) in the case of the first offense, be fined
20 under title 18, United States Code, imprisoned for
21 not more than 180 days, or both;

22 “(2) in the case of the second offense, be fined
23 under such title, imprisoned for not more than 3
24 years, or both; and

1 “(3) in the case of the third or subsequent of-
 2 fense, be fined under such title, imprisoned for not
 3 more than 10 years, or both.”.

4 (b) CLERICAL AMENDMENT.—The table of contents
 5 preceding section 2 of such Act is amended by adding at
 6 the end the following:

“Sec. 1115. Unauthorized access to intelligence community property.”.

7 **SEC. 312. STRENGTHENING OF OFFICE OF INTELLIGENCE**
 8 **AND ANALYSIS.**

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

11 **“§ 311. Office of Economic Intelligence and Security**

12 “(a) DEFINITIONS.—In this section, the terms ‘coun-
 13 terintelligence’, ‘foreign intelligence’, and ‘intelligence
 14 community’ have the meanings given such terms in section
 15 3 of the National Security Act of 1947 (50 U.S.C. 3003).

16 “(b) ESTABLISHMENT.—There is established within
 17 the Office of Terrorism and Financial Intelligence of the
 18 Department of the Treasury, the Office of Economic Intel-
 19 ligence and Security (in this section referred to as the ‘Of-
 20 fice’), which shall—

21 “(1) be responsible for the receipt, analysis, col-
 22 lation, and dissemination of foreign intelligence and
 23 foreign counterintelligence information relating to
 24 the operation and responsibilities of the Department
 25 of the Treasury and other Federal agencies exe-

1 cutting economic statecraft tools that do not include
 2 any elements that are elements of the intelligence
 3 community;

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

8 “(3) have such other related duties and authori-
 9 ties as may be assigned by the Secretary for pur-
 10 poses of the responsibilities described in paragraph
 11 (1), subject to the authority, direction, and control
 12 of the Secretary, in consultation with the Director of
 13 National Intelligence.

14 “(c) ASSISTANT SECRETARY FOR ECONOMIC INTEL-
 15 LIGENCE AND SECURITY.—The Office shall be headed by
 16 an Assistant Secretary, who shall be appointed by the
 17 President, by and with the advice and consent of the Sen-
 18 ate. The Assistant Secretary shall report directly to the
 19 Undersecretary for Terrorism and Financial Crimes.”.

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

“311. Office of Economic Intelligence and Security.”.

24 (c) CONFORMING AMENDMENT.—Section 3(4)(J) of
 25 the National Security Act of 1947 (50 U.S.C. 3003(4)(J))

1 is amended by striking “Office of Intelligence and Anal-
 2 ysis” and inserting “Office of Economic Intelligence and
 3 Security”.

4 (d) REFERENCES.—Any reference in a law, regula-
 5 tion, document, paper, or other record of the United
 6 States to the Office of Intelligence and Analysis of the
 7 Department of the Treasury shall be deemed a reference
 8 to the Office of Economic Intelligence and Security of the
 9 Department of the Treasury.

10 **SEC. 313. REPORT ON SENSITIVE COMMERCIALLY AVAIL-**
 11 **ABLE INFORMATION.**

12 (a) DEFINITIONS.—

13 (1) COMMERCIALLY AVAILABLE INFORMA-
 14 TION.—The term “commercially available informa-
 15 tion” means—

16 (A) any data or other information of the
 17 type customarily made available or obtainable
 18 and sold, leased, or licensed to members of the
 19 general public or to non-governmental entities
 20 for purposes other than governmental purposes;
 21 or

22 (B) data and information for exclusive gov-
 23 ernment use knowingly and voluntarily provided
 24 by, procured from, or made accessible by cor-

1 porate entities on their own initiative or at the
2 request of a government entity.

3 (2) PERSONALLY IDENTIFIABLE INFORMA-
4 TION.—The term “personally identifiable informa-
5 tion” means information that, alone or when com-
6 bined with other information regarding an indi-
7 vidual, can be used to distinguish or trace the iden-
8 tity of such individual.

9 (3) SENSITIVE ACTIVITIES.—The term “sen-
10 sitive activities” means activities that, over an ex-
11 tended period of time—

12 (A) establish a pattern of life;

13 (B) reveal personal affiliations, pref-
14 erences, or identifiers;

15 (C) facilitate prediction of future acts;

16 (D) enable targeting activities;

17 (E) reveal the exercise of individual rights
18 and freedoms, including the rights to freedom
19 of speech and of the press, to free exercise of
20 religion, to peaceably assemble, including mem-
21 bership or participation in organizations or as-
22 sociations, and to petition the government; or

23 (F) reveal any other activity the disclosure
24 of which could cause substantial harm, embar-
25 rassment, inconvenience, or unfairness to the

1 United States person who engaged in the activ-
2 ity.

3 (4) SENSITIVE COMMERCIALY AVAILABLE IN-
4 FORMATION.—The term “sensitive commercially
5 available information”—

6 (A) means commercially available informa-
7 tion that is known or reasonably expected to
8 contain—

9 (i) a substantial volume of personally
10 identifiable information regarding United
11 States persons; or

12 (ii) a greater than de minimis volume
13 of sensitive data;

14 (B) shall not include—

15 (i) newspapers or other periodicals;

16 (ii) weather reports;

17 (iii) books;

18 (iv) journal articles or other published
19 works;

20 (v) public filings or records;

21 (vi) documents or databases similar to
22 those described in clauses (i) through (v),
23 whether accessed through a subscription or
24 accessible free of cost; or

1 (vii) limited data samples made avail-
2 able to elements of the intelligence commu-
3 nity for the purposes of allowing such ele-
4 ments to determine whether to purchase
5 the full dataset and not accessed, retained,
6 or used for any other purpose.

7 (5) SENSITIVE DATA.—The term “sensitive
8 data” means data that—

9 (A)(i) captures personal attributes, condi-
10 tions, or identifiers that are traceable to 1 or
11 more specific United States persons, either
12 through the dataset or by correlating the
13 dataset with other available information; and

14 (ii) concerns the race or ethnicity, political
15 opinions, religious beliefs, sexual orientation,
16 gender identity, medical or genetic information,
17 financial data, or any other data with respect to
18 such specific United States person or United
19 States persons the disclosure of which would
20 have the potential to cause substantial harm,
21 embarrassment, inconvenience, or unfairness to
22 the United States person or United States per-
23 sons described by the data; or

24 (B) captures the sensitive activities of 1 or
25 more United States persons.

1 (6) UNITED STATES PERSON.—The term
2 “United States person” means—

3 (A) a United States citizen or an alien law-
4 fully admitted for permanent residence to the
5 United States;

6 (B) an unorganized association substan-
7 tially composed of United States citizens or per-
8 manent resident aliens; or

9 (C) an entity organized under the laws of
10 the United States or of any jurisdiction within
11 the United States, with the exception of any
12 such entity directed or controlled by a foreign
13 government.

14 (b) REPORT.—

15 (1) IN GENERAL.—Not later than 60 days after
16 the date of the enactment of this Act, and annually
17 thereafter, the head of each element of the intel-
18 ligence community shall submit to the congressional
19 intelligence committees a report on the access to,
20 collection, processing, and use of sensitive commer-
21 cially available information by the respective ele-
22 ment.

23 (2) CONTENTS.—

24 (A) IN GENERAL.—For each dataset con-
25 taining sensitive commercially available infor-

1 mation accessed, collected, processed, or used
2 by the element concerned for purposes other
3 than research and development, a report re-
4 quired by paragraph (1) shall include the fol-
5 lowing:

6 (i) A description of the nature and
7 volume of the sensitive commercially avail-
8 able information accessed or collected by
9 the element.

10 (ii) A description of the mission or ad-
11 ministrative need or function for which the
12 sensitive commercially available informa-
13 tion is accessed or collected, and of the na-
14 ture, scope, reliability, and timeliness of
15 the dataset required to fulfill such mission
16 or administrative need or function.

17 (iii) A description of the purpose of
18 the access, collection, or processing, and
19 the intended use of the sensitive commer-
20 cially available information.

21 (iv) An identification of the legal au-
22 thority for the collection or access, and
23 processing of the sensitive commercially
24 available information.

1 (v) An identification of the source of
2 the sensitive commercially available infor-
3 mation and the persons from whom the
4 sensitive commercially available informa-
5 tion was accessed or collected.

6 (vi) A description of the mechanics of
7 the access, collection, and processing of the
8 sensitive commercially available informa-
9 tion, including the Federal entities that
10 participated in the procurement process.

11 (vii) A description of the method by
12 which the element has limited the access to
13 and collection and processing of the sen-
14 sitive commercially available information to
15 the maximum extent feasible consistent
16 with the need to fulfill the mission or ad-
17 ministrative need.

18 (viii) An assessment of whether the
19 mission or administrative need can be ful-
20 filled if reasonably available privacy-en-
21 hancing techniques, such as filtering or
22 anonymizing, the application of traditional
23 safeguards, including access limitations
24 and retention limits, differential privacy
25 techniques, or other information-masking

1 techniques, such as restrictions or correla-
2 tion, are implemented with respect to in-
3 formation concerning United States per-
4 sons.

5 (ix) An assessment of the privacy and
6 civil liberties risks associated with access-
7 ing, collecting, or processing the data and
8 the methods by which the element miti-
9 gates such risks.

10 (x) An assessment of the applicability
11 of section 552a of title 5, United States
12 Code (commonly referred to as the “Pri-
13 vacy Act of 1974”), if any.

14 (xi) To the extent feasible, an assess-
15 ment of the original source of the data and
16 the method through which the dataset was
17 generated and aggregated, and whether
18 any element of the intelligence community
19 previously accessed or collected the same
20 or similar sensitive commercially available
21 information from the source.

22 (xii) An assessment of the quality and
23 integrity of the data, including, as appro-
24 priate, whether the sensitive commercially
25 available information reflects any under-

1 lying biases or inferences, and efforts to
2 ensure that any intelligence products cre-
3 ated with the data are consistent with the
4 standards of the intelligence community
5 for accuracy and objectivity.

6 (xiii) An assessment of the security,
7 operational, and counterintelligence risks
8 associated with the means of accessing or
9 collecting the data, and recommendations
10 for how the element could mitigate such
11 risks.

12 (xiv) A description of the system in
13 which the data is retained and processed
14 and how the system is properly secured
15 while allowing for effective implementation,
16 management, and audit, as practicable, of
17 relevant privacy and civil liberties protec-
18 tions.

19 (xv) An assessment of security risks
20 posed by the system architecture of ven-
21 dors providing sensitive commercially avail-
22 able information or access to such sensitive
23 commercially available information, access
24 restrictions for the data repository of each
25 such vendor, and the vendor's access to

1 query terms and, if any, relevant safe-
2 guards.

3 (xvi) A description of procedures to
4 restrict access to the sensitive commer-
5 cially available information.

6 (xvii) A description of procedures for
7 conducting, approving, documenting, and
8 auditing queries, searches, or correlations
9 with respect to the sensitive commercially
10 available information.

11 (xviii) A description of procedures for
12 restricting dissemination of the sensitive
13 commercially available information, includ-
14 ing deletion of information of United
15 States persons returned in response to a
16 query or other search unless the informa-
17 tion is assessed to be associated or poten-
18 tially associated with the documented mis-
19 sion-related justification for the query or
20 search.

21 (xix) A description of masking and
22 other privacy-enhancing techniques used by
23 the element to protect sensitive commer-
24 cially available information.

1 (xx) A description of any retention
2 and deletion policies.

3 (xxi) A determination of whether
4 unevaluated data or information has been
5 made available to other elements of the in-
6 telligence community or foreign partners
7 and, if so, identification of those elements
8 or partners.

9 (xxii) A description of any licensing
10 agreements or contract restrictions with
11 respect to the sensitive commercially avail-
12 able information.

13 (xxiii) A data management plan for
14 the lifecycle of the data, from access or col-
15 lection to disposition.

16 (xxiv) For any item required by
17 clauses (i) through (xxiii) that cannot be
18 completed due to exigent circumstances re-
19 lating to collecting, accessing, processing,
20 or using sensitive commercially available
21 information, a description of such exigent
22 circumstances.

23 (B) RESEARCH AND DEVELOPMENT
24 DATA.—For each dataset containing sensitive
25 commercially available information accessed,

1 collected, processed, or used by the element con-
 2 cerned solely for research and development pur-
 3 poses, a report required by paragraph (1) may
 4 be limited to a description of the oversight by
 5 the element of such access, collection, process,
 6 and use.

7 (c) PUBLIC REPORT.—The Director of National In-
 8 telligence shall make available to the public, once every
 9 2 years, a report on the policies and procedures of the
 10 intelligence community with respect to access to and col-
 11 lection, processing, and safeguarding of sensitive commer-
 12 cially available information.

13 **SEC. 314. POLICY ON COLLECTION OF UNITED STATES LO-**
 14 **CATION INFORMATION.**

15 (a) DEFINITIONS.—In this section:

16 (1) UNITED STATES LOCATION INFORMA-
 17 TION.—The term “United States location informa-
 18 tion” means information derived or otherwise cal-
 19 culated from the transmission or reception of a radio
 20 signal that reveals the approximate or actual geo-
 21 graphic location of a customer, subscriber, user, or
 22 device in the United States, or, if the customer, sub-
 23 scriber, or user is known to be a United States per-
 24 son, outside the United States.

1 (2) UNITED STATES PERSON.—The term
2 “United States person” has the meaning given that
3 term in section 101 of the Foreign Intelligence Sur-
4 veillance Act of 1978 (50 U.S.C. 1801).

5 (b) IN GENERAL.—Not later than 180 days after the
6 date of the enactment of this Act, the Director of National
7 Intelligence, in coordination with the Attorney General,
8 shall issue a policy on the collection of United States loca-
9 tion information by the intelligence community.

10 (c) CONTENT.—The policy required by subsection (a)
11 shall address the filtering, segregation, use, dissemination,
12 masking, and retention of United States location informa-
13 tion.

14 (d) FORM; PUBLIC AVAILABILITY.—The policy re-
15 quired by subsection (a)—

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

18 (2) may include a classified annex, which the
19 Director of National Intelligence shall submit to the
20 congressional intelligence committees.

21 **SEC. 315. DISPLAY OF FLAGS, SEALS, AND EMBLEMS OTHER**
22 **THAN THE UNITED STATES FLAG.**

23 (a) DEFINITIONS.—In this section:

1 (1) EXECUTIVE AGENCY.—The term “Executive
2 agency” has the meaning given such term in section
3 105 of title 5, United States Code.

4 (2) NATIONAL INTELLIGENCE PROGRAM.—The
5 term “National Intelligence Program” has the mean-
6 ing given such term in section 3 of the National Se-
7 curity Act of 1947 (50 U.S.C. 3003).

8 (b) IN GENERAL.—Any flag, seal, or emblem that is
9 not the United States flag and is flown, draped, projected,
10 or otherwise displayed as a visual and symbolic representa-
11 tion at a property, office, or other official location of an
12 element of the intelligence community—

13 (1) shall be smaller than the official United
14 States flag; and

15 (2) if flown, may not be displayed higher than
16 or above the United States flag.

17 (c) LIMITATION ON AVAILABILITY OF FUNDS FOR
18 DISPLAYING AND FLYING FLAGS.—None of the funds au-
19 thorized to be appropriated by this Act or otherwise made
20 available for fiscal year 2025 for the National Intelligence
21 Program, may be obligated or expended to fly or display
22 a flag over a facility of an element of the intelligence com-
23 munity other than the following:

24 (1) The United States flag.

25 (2) The POW/MIA flag.

1 (3) The Hostage and Wrongful Detainee flag,
2 pursuant to section 904 of title 36, United States
3 Code.

4 (4) The flag of a State, insular area, or the
5 District of Columbia at a domestic location.

6 (5) The flag of an Indian Tribal Government.

7 (6) The official branded flag of an Executive
8 agency.

9 (7) The flag of an element, flag officer, or gen-
10 eral officer of the Armed Forces.

11 **TITLE IV—COUNTERING**
12 **FOREIGN THREATS**
13 **Subtitle A—People’s Republic of**
14 **China**

15 **SEC. 401. STRATEGY AND OUTREACH ON RISKS POSED BY**
16 **PEOPLE’S REPUBLIC OF CHINA SMARTPORT**
17 **TECHNOLOGY.**

18 (a) STRATEGY AND OUTREACH REQUIRED.—The Di-
19 rector of the National Counterintelligence and Security
20 Center shall develop a strategy and conduct outreach to
21 United States industry, including shipping companies,
22 port operators, and logistics firms, on the risks of
23 smartport technology of the People’s Republic of China
24 and other related risks posed by entities of the People’s
25 Republic of China, including LOGINK, China Ocean Ship-

ping Company, Limited (COSCO), China Communications Construction Company, Limited (CCCC), China Media Group (CMG), and Shanghai Zhenhua Heavy Industries Company Limited (ZPMC), to the national security of the United States, the security of United States supply chains, and commercial activity, including with respect to delays, interruption, and lockout of access to systems and technologies that enable the free flow of commerce.

(b) CONSISTENCY WITH STATUTES AND EXECUTIVE ORDERS.—The Director shall carry out subsection (a) in a manner that is consistent with the following:

(1) Part 6 of title 33, Code of Federal Regulations, as amended by Executive Order 14116 (89 Fed. Reg. 13971; relating to amending regulations relating to the safeguarding of vessels, harbors, ports, and waterfront facilities of the United States.

(2) Executive Order 14017 (86 Fed. Reg. 11849; relating to America’s supply chains), or successor order.

(3) Section 825 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118–31).

(c) COORDINATION.—The Director shall carry out subsection (a) in coordination with the Commandant of the Coast Guard, the Director of the Federal Bureau of

1 Investigation, the Commander of the Office of Naval Intel-
2 ligence, and such other heads of Federal agencies as the
3 Director considers appropriate.

4 **SEC. 402. ASSESSMENT OF CURRENT STATUS OF BIO-**
5 **TECHNOLOGY OF PEOPLE'S REPUBLIC OF**
6 **CHINA.**

7 (a) ASSESSMENT.—Not later than 30 days after the
8 date of the enactment of this Act, the Director of National
9 Intelligence shall, in consultation with the Director of the
10 National Counterproliferation and Biosecurity Center and
11 such heads of elements of the intelligence community as
12 the Director of National Intelligence considers appro-
13 priate, conduct an assessment of the current status of the
14 biotechnology of the People's Republic of China, which
15 shall include an assessment of how the People's Republic
16 of China is supporting the biotechnology sector through
17 both licit and illicit means, such as foreign direct invest-
18 ment, subsidies, talent recruitment, or other efforts.

19 (b) REPORT.—

20 (1) IN GENERAL.—Not later than 30 days after
21 the date on which the Director of National Intelligence
22 completes the assessment required by subsection (a),
23 the Director shall submit to the congressional intel-
24 ligence committees a report on the findings of the
25 Director with respect to the assessment.

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

4 **SEC. 403. INTELLIGENCE SHARING WITH LAW ENFORCE-**
5 **MENT AGENCIES ON SYNTHETIC OPIOID PRE-**
6 **CURSOR CHEMICALS ORIGINATING IN PEO-**
7 **PLE’S REPUBLIC OF CHINA.**

8 (a) STRATEGY REQUIRED.—The Director of National
9 Intelligence shall, in consultation with the head of the Of-
10 fice of National Security Intelligence of the Drug Enforce-
11 ment Administration, the Under Secretary of Homeland
12 Security for Intelligence and Analysis, and the heads of
13 such other agencies as the Director considers appropriate,
14 develop a strategy to ensure robust intelligence sharing re-
15 lating to the illicit trafficking of synthetic opioid precursor
16 chemicals from the People’s Republic of China and other
17 source countries.

18 (b) MECHANISM FOR COLLABORATION.—The Direc-
19 tor shall develop a mechanism so that subject matter ex-
20 perts in elements of the Federal Government other than
21 elements in the intelligence community, including those
22 without security clearances, can share information with
23 the intelligence community relating to illicit trafficking de-
24 scribed in subsection (a).

1 **SEC. 404. REPORT ON EFFORTS OF THE PEOPLE'S REPUB-**
2 **LIC OF CHINA TO EVADE UNITED STATES**
3 **TRANSPARENCY AND NATIONAL SECURITY**
4 **REGULATIONS.**

5 (a) REPORT REQUIRED.—The Director of National
6 Intelligence shall submit to the congressional intelligence
7 committees a report on efforts of the People's Republic
8 of China to evade the following:

9 (1) Identification under section 1260H of the
10 William M. (Mac) Thornberry National Defense Au-
11 thorization Act for Fiscal Year 2021 (Public Law
12 116–283; 10 U.S.C. 113 note).

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

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

18 (B) Section 889 of the John S. McCain
19 National Defense Authorization Act for Fiscal
20 Year 2019 (Public Law 115–232; 41 U.S.C.
21 3901 note prec.).

22 (C) The list of specially designated nation-
23 als and blocked persons maintained by the Of-
24 fice of Foreign Assets Control of the Depart-
25 ment of the Treasury (commonly known as the
26 “SDN list”).

1 (D) The Entity List maintained by the
2 Bureau of Industry and Security of the Depart-
3 ment of Commerce and set forth in Supplement
4 No. 4 to part 744 of title 15, Code of Federal
5 Regulations.

6 (E) Commercial or dual-use export controls
7 under the Export Control Reform Act of 2018
8 (50 U.S.C. 4801 et seq.) and the Export Ad-
9 ministration Regulations.

10 (F) Executive Order 14105 (88 Fed. Reg.
11 54867; relating to addressing United States in-
12 vestments in certain national security tech-
13 nologies and products in countries of concern),
14 or successor order.

15 (G) Import restrictions on products made
16 with forced labor implemented by U.S. Customs
17 and Border Protection pursuant to Public Law
18 117–78 (22 U.S.C. 6901 note).

19 (b) FORM.—The report submitted pursuant to sub-
20 section (a) shall be submitted in unclassified form.

21 **SEC. 405. PLAN FOR RECRUITMENT OF MANDARIN SPEAK-**
22 **ERS.**

23 (a) IN GENERAL.—Not later than 180 days after the
24 date of the enactment of this Act, the Director of National
25 Intelligence shall submit to the appropriate congressional

1 committees a comprehensive plan to prioritize the recruit-
 2 ment and training of individuals who speak Mandarin Chi-
 3 nese for each element of the intelligence community.

4 (b) APPROPRIATE CONGRESSIONAL COMMITTEES.—
 5 In this section, the term “appropriate congressional com-
 6 mittees” means—

- 7 (1) the Select Committee on Intelligence and
- 8 the Committee on the Judiciary of the Senate; and
- 9 (2) the Permanent Select Committee on Intel-
- 10 ligence and the Committee on the Judiciary of the
- 11 House of Representatives.

12 **Subtitle B—The Russian** 13 **Federation**

14 **SEC. 411. ASSESSMENT OF RUSSIAN FEDERATION SPON-** 15 **SORSHIP OF ACTS OF INTERNATIONAL TER-** 16 **RORISM.**

17 (a) DEFINITIONS.—In this section—

18 (1) APPROPRIATE CONGRESSIONAL COMMIT-
 19 TEES.—The term “appropriate congressional com-
 20 mittees” means—

- 21 (A) the Select Committee on Intelligence,
- 22 the Committee on Foreign Relations, and the
- 23 Committee on Armed Services of the Senate;
- 24 and

1 (B) the Permanent Select Committee on
2 Intelligence, the Committee on Foreign Affairs,
3 and the Committee on Armed Services of the
4 House of Representatives.

5 (2) FOREIGN TERRORIST ORGANIZATION.—The
6 term “foreign terrorist organization” means an or-
7 ganization that has been designated as a foreign ter-
8 rorist organization by the Secretary of State, pursu-
9 ant to section 219 of the Immigration and Nation-
10 ality Act (8 U.S.C. 1189).

11 (3) SPECIALLY DESIGNATED GLOBAL TER-
12 RORIST ORGANIZATION.—The term “specially des-
13 ignated global terrorist organization” means an or-
14 ganization that has been designated as a specially
15 designated global terrorist by the Secretary of State
16 or the Secretary, pursuant to Executive Order
17 13224 (50 U.S.C. 1701 note; relating to blocking
18 property and prohibiting transactions with persons
19 who commit, threaten to commit, or support ter-
20 rorism).

21 (4) STATE SPONSOR OF TERRORISM.—The term
22 “state sponsor of terrorism” means a country the
23 government of which the Secretary of State has de-
24 termined has repeatedly provided support for acts of
25 international terrorism, for purposes of—

1 (A) section 1754(c)(1)(A)(i) of the Export
2 Control Reform Act of 2018 (50 U.S.C.
3 4813(c)(1)(A)(i));

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

6 (C) section 40(d) of the Arms Export Con-
7 trol Act (22 U.S.C. 2780(d)); or

8 (D) any other provision of law.

9 (b) ASSESSMENT REQUIRED.—Not later than 180
10 days after the date of the enactment of this Act, the Direc-
11 tor of National Intelligence shall conduct and submit to
12 the appropriate congressional committees an assessment
13 on the extent to which the Russian Federation—

14 (1) provides support for acts of international
15 terrorism; and

16 (2) cooperates with the antiterrorism efforts of
17 the United States.

18 (c) ELEMENTS.—The assessment required by sub-
19 section (b) shall include the following:

20 (1) A list of all instances in which the Russian
21 Federation, or an official of the Russian Federation,
22 has failed to show support for or cooperate with the
23 United States on international efforts to combat ter-
24 rorism, such as apprehending, prosecuting, or extra-
25 diting suspected and known terrorists, including

1 members of foreign terrorist organizations, and
2 sharing intelligence to deter terrorist attacks.

3 (2) A list of all instances in which the Russian
4 Federation, or an official of the Russian Federation,
5 has provided financial, material, technical, or lethal
6 support to foreign terrorist organizations, specially
7 designated global terrorist organizations, state spon-
8 sors of terrorism, or for acts of international ter-
9 rorism.

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

13 (A) the international proliferation of nu-
14 clear explosive devices to persons;

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

17 (C) the efforts of a person to use, develop,
18 produce, stockpile, or otherwise acquire chem-
19 ical, biological, or radiological weapons.

20 (4) A determination of whether the activities of
21 the Wagner Group constitute acts of international
22 terrorism and whether such activities continue under
23 any of the successor entities of the Wagner Group,
24 including Afrika Corps.

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

4 (e) BRIEFINGS.—Not later than 30 days after sub-
5 mission of the assessment required by subsection (b), the
6 Director of National Intelligence shall provide a classified
7 briefing to the appropriate congressional committees on
8 the methodology and findings of the assessment.

9 **SEC. 412. ASSESSMENT OF LIKELY COURSE OF WAR IN**
10 **UKRAINE.**

11 (a) IN GENERAL.—Not later than 90 days after the
12 date of the enactment of this Act, the Director of National
13 Intelligence, in collaboration with the Director of the De-
14 fense Intelligence Agency and the Director of the Central
15 Intelligence Agency, shall submit to the congressional in-
16 telligence committees an assessment of the likely course
17 of the war in Ukraine through December 31, 2025.

18 (b) ELEMENTS.—The assessment required by sub-
19 section (a) shall include an assessment of each of the fol-
20 lowing:

21 (1) The ability of the military of Ukraine to de-
22 fend against Russian aggression if the United States
23 does, or does not, continue to provide military and
24 economic assistance to Ukraine during the period
25 described in such subsection.

1 (2) The likely course of the war during such pe-
2 riod if the United States does, or does not, continue
3 to provide military and economic assistance to
4 Ukraine.

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

11 (4) The effects of a potential defeat of Ukraine
12 by the Russian Federation on the potential for fur-
13 ther aggression from the Russian Federation, the
14 People's Republic of China, the Islamic Republic of
15 Iran, and the Democratic People's Republic of
16 Korea.

17 (c) FORM.—The assessment required by subsection
18 (a) shall be submitted in unclassified form, but may in-
19 clude a classified annex.

Subtitle C—International Terrorism

SEC. 421. INCLUSION OF HAMAS, HEZBOLLAH, AL-QAEDA, AND ISIS OFFICIALS AND MEMBERS AMONG ALIENS ENGAGED IN TERRORIST ACTIVITY.

Section 212(a)(3)(B)(i) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)) is amended, in the undesignated matter following subparagraph (IX), by striking “or spokesman of the Palestine Liberation Organization” and inserting “spokesperson, or member of the Palestine Liberation Organization, Hamas, Hezbollah, Al-Qaeda, ISIS, or any successor or affiliate group, or who endorses or espouses terrorist activities conducted by any of the aforementioned groups,”.

SEC. 422. ASSESSMENT AND REPORT ON THE THREAT OF ISIS-KHORASAN TO THE UNITED STATES.

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

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

1 (2) submit to the congressional intelligence
2 committees a written report on the findings of the
3 assessment.

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

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

9 (2) A description of the ideology and stated in-
10 tentions of ISIS-Khorasan as related to the United
11 States and the interests of the United States, includ-
12 ing the homeland.

13 (3) A list of all terrorist attacks worldwide at-
14 tributable to ISIS-Khorasan or for which ISIS-
15 Khorasan claimed credit, beginning on January 1,
16 2015.

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

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

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

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

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

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

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

12 (8) A description of ISIS-Khorasan's develop-
13 ment of, and relationships with, travel facilitation
14 networks in Europe, Central Asia, Eurasia, and
15 Latin America.

16 (9) An assessment of ISIS-Khorasan's under-
17 standing of the border and immigration policies and
18 enforcement of the United States.

19 (10) An assessment of the known travel of
20 members of ISIS-Khorasan within the Western
21 Hemisphere and specifically across the southern bor-
22 der of the United States.

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

1 **SEC. 423. TERRORIST FINANCING PREVENTION.**

2 (a) DEFINITIONS.—In this section:

3 (1) DIGITAL ASSET.—The term “digital asset”
4 means any digital representation of value that is re-
5 corded on a cryptographically secured distributed
6 ledger or any similar technology, or another imple-
7 mentation which was designed and built as part of
8 a system to leverage or replace blockchain or distrib-
9 uted ledger technology or their derivatives.

10 (2) DIGITAL ASSET PROTOCOL.—The term
11 “digital asset protocol” means any communication
12 protocol, smart contract, or other software—

13 (A) deployed through the use of distributed
14 ledger or similar technology; and

15 (B) that provides a mechanism for users to
16 interact and agree to the terms of a trade for
17 digital assets.

18 (3) FOREIGN DIGITAL ASSET TRANSACTION
19 FACILITATOR.—The term “foreign digital asset
20 transaction facilitator” means any foreign person or
21 group of foreign persons that, as determined by the
22 Secretary, controls, operates, or makes available a
23 digital asset protocol or similar facility, or otherwise
24 materially assists in the purchase, sale, exchange,
25 custody, or other transaction involving an exchange
26 or transfer of value using digital assets.

1 (4) FOREIGN FINANCIAL INSTITUTION.—The
2 term “foreign financial institution” has the meaning
3 given that term under section 561.308 of title 31,
4 Code of Federal Regulations.

5 (5) FOREIGN PERSON.—The term “foreign per-
6 son” means an individual or entity that is not a
7 United States person.

8 (6) FOREIGN TERRORIST ORGANIZATION.—The
9 term “foreign terrorist organization” means an or-
10 ganization that has been designated as a foreign ter-
11 rorist organization by the Secretary of State, pursu-
12 ant to section 219 of the Immigration and Nation-
13 ality Act (8 U.S.C. 1189).

14 (7) GOOD.—The term “good” means any arti-
15 cle, natural or manmade substance, material, supply,
16 or manufactured product, including inspection and
17 test equipment, and excluding technical data.

18 (8) SECRETARY.—The term “Secretary” means
19 the Secretary of the Treasury.

20 (9) SPECIALLY DESIGNATED GLOBAL TER-
21 RODIST ORGANIZATION.—The term “specially des-
22 ignated global terrorist organization” means an or-
23 ganization that has been designated as a specially
24 designated global terrorist by the Secretary of State
25 or the Secretary, pursuant to Executive Order

1 13224 (50 U.S.C. 1701 note; relating to blocking
2 property and prohibiting transactions with persons
3 who commit, threaten to commit, or support ter-
4 rorism).

5 (10) UNITED STATES PERSON.—The term
6 “United States person” means—

7 (A) an individual who is a United States
8 citizen or an alien lawfully admitted for perma-
9 nent residence to the United States;

10 (B) an entity organized under the laws of
11 the United States or any jurisdiction within the
12 United States, including a foreign branch of
13 such an entity; or

14 (C) any person in the United States.

15 (b) SANCTIONS WITH RESPECT TO FOREIGN FINAN-
16 CIAL INSTITUTIONS AND FOREIGN DIGITAL ASSET
17 TRANSACTION FACILITATORS THAT ENGAGE IN CERTAIN
18 TRANSACTIONS.—

19 (1) MANDATORY IDENTIFICATION.—Not later
20 than 60 days after the date of enactment of this
21 Act, and periodically thereafter, the Secretary shall
22 identify and submit to the President a report identi-
23 fying any foreign financial institution or foreign dig-
24 ital asset transaction facilitator that has know-
25 ingly—

1 (A) facilitated a significant financial trans-
2 action with—

3 (i) a Foreign Terrorist Organization;

4 (ii) a specially designated global ter-
5 rorist organization; or

6 (iii) a person identified on the list of
7 specially designated nationals and blocked
8 persons maintained by the Office of For-
9 eign Assets Control of the Department of
10 the Treasury, the property and interests in
11 property of which are blocked pursuant to
12 the International Emergency Economic
13 Powers Act (50 U.S.C. 1701 et seq.) for
14 acting on behalf of or at the direction of,
15 or being owned or controlled by, a foreign
16 terrorist organization or a specially des-
17 ignated global terrorist organization; or

18 (B) engaged in money laundering to carry
19 out an activity described in subparagraph (A).

20 (2) IMPOSITION OF SANCTIONS.—

21 (A) FOREIGN FINANCIAL INSTITUTIONS.—

22 The President shall prohibit, or impose strict
23 conditions on, the opening or maintaining of a
24 correspondent account or a payable-through ac-

count in the United States by a foreign financial institution identified under paragraph (1).

(B) FOREIGN DIGITAL ASSET TRANSACTION FACILITATORS.—The President, pursuant to such regulations as the President may prescribe, shall prohibit any transactions between any person subject to the jurisdiction of the United States and a foreign digital asset transaction facilitator identified under paragraph (1).

(3) IMPLEMENTATION AND PENALTIES.—

(A) IMPLEMENTATION.—The President may exercise all authorities provided under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702, 1704) to the extent necessary to carry out this Act.

(B) PENALTIES.—The penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) shall apply to a person that violates, attempts to violate, conspires to violate, or causes a violation of regulations prescribed under this section to the same extent that such penalties apply to a person that com-

1 mits an unlawful act described in subsection (a)
2 of such section 206.

3 (4) PROCEDURES FOR JUDICIAL REVIEW OF
4 CLASSIFIED INFORMATION.—

5 (A) IN GENERAL.—If a finding under this
6 subsection, or a prohibition, condition, or pen-
7 alty imposed as a result of any such finding, is
8 based on classified information (as defined in
9 section 1(a) of the Classified Information Pro-
10 cedures Act (18 U.S.C. App.)), the Secretary
11 may submit to a court reviewing the finding or
12 the imposition of the prohibition, condition, or
13 penalty such classified information ex parte and
14 in camera.

15 (B) RULE OF CONSTRUCTION.—Nothing in
16 this paragraph shall be construed to confer or
17 imply any right to judicial review of any finding
18 under this subsection or any prohibition, condi-
19 tion, or penalty imposed as a result of any such
20 finding.

21 (5) WAIVER FOR NATIONAL SECURITY.—The
22 Secretary may waive the imposition of sanctions
23 under this subsection with respect to a person if the
24 Secretary—

1 (A) determines that such a waiver is in the
 2 national interests of the United States; and

3 (B) submits to Congress a notification of
 4 the waiver and the reasons for the waiver.

5 (6) EXCEPTION FOR INTELLIGENCE ACTIVITIES.—This subsection shall not apply with respect
 6 to any activity subject to the reporting requirements
 7 under title V of the National Security Act of 1947
 8 (50 U.S.C. 3091 et seq.) or any authorized intel-
 9 ligence activities of the United States.
 10

11 (7) EXCEPTION RELATING TO IMPORTATION OF
 12 GOODS.—The authorities and requirements under
 13 this section shall not include the authority or a re-
 14 quirement to impose sanctions on the importation of
 15 goods.

16 (c) SPECIAL MEASURES FOR MODERN THREATS.—
 17 Section 5318A of title 31, United States Code, is amend-
 18 ed—

19 (1) in subsection (a)(2)(C), by striking “sub-
 20 section (b)(5)” and inserting “paragraphs (5) and
 21 (6) of subsection (b)”;

22 (2) in subsection (b)—

23 (A) in paragraph (5), by striking “for or
 24 on behalf of a foreign banking institution”; and

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

1 “(6) PROHIBITIONS OR CONDITIONS ON CER-
2 TAIN TRANSMITTALS OF FUNDS.—If the Secretary
3 finds a jurisdiction outside of the United States, 1
4 or more financial institutions operating outside of
5 the United States, 1 or more types of accounts with-
6 in, or involving, a jurisdiction outside of the United
7 States, or 1 or more classes of transactions within,
8 or involving, a jurisdiction outside of the United
9 States to be of primary money laundering concern,
10 the Secretary, in consultation with the Secretary of
11 State, the Attorney General, and the Chairman of
12 the Board of Governors of the Federal Reserve Sys-
13 tem, may prohibit, or impose conditions upon, cer-
14 tain transmittals of funds (as such term may be de-
15 fined by the Secretary in a special measure issuance,
16 by regulation, or as otherwise permitted by law), to
17 or from any domestic financial institution or domes-
18 tic financial agency if such transmittal of funds in-
19 volves any such jurisdiction, institution, type of ac-
20 count, class of transaction, or type of account.”.

21 (d) FUNDING.—There is authorized to be appro-
22 priated to the Secretary such funds as are necessary to
23 carry out the purposes of this section.

1 **Subtitle D—Other Foreign Threats**

2 **SEC. 431. ASSESSMENT OF VISA-FREE TRAVEL TO AND** 3 **WITHIN WESTERN HEMISPHERE BY NATION-** 4 **ALS OF COUNTRIES OF CONCERN.**

5 (a) IN GENERAL.—Not later than 90 days after the
 6 date of the enactment of this Act, the Director of National
 7 Intelligence shall submit to the congressional intelligence
 8 committees a written assessment of the impacts to na-
 9 tional security caused by travel without a visa to and with-
 10 in countries in the Western Hemisphere by nationals of
 11 countries of concern.

12 (b) FORM.—The assessment required by subsection
 13 (a) shall be submitted in unclassified form, but may in-
 14 clude a classified annex.

15 (c) COUNTRIES OF CONCERN DEFINED.—In this sec-
 16 tion, the term “countries of concern” means—

- 17 (1) the Russian Federation;
- 18 (2) the People’s Republic of China;
- 19 (3) the Islamic Republic of Iran;
- 20 (4) the Syrian Arab Republic;
- 21 (5) the Democratic People’s Republic of Korea;
- 22 (6) the Bolivarian Republic of Venezuela; and
- 23 (7) the Republic of Cuba.

1 **SEC. 432. STUDY ON THREAT POSED BY FOREIGN INVEST-**
2 **MENT IN UNITED STATES AGRICULTURAL**
3 **LAND.**

4 (a) DEFINITIONS.—In this section:

5 (1) APPROPRIATE COMMITTEES OF CON-
6 GRESS.—The term “appropriate committees of Con-
7 gress” means—

8 (A) the Select Committee on Intelligence,
9 the Committee on Agriculture, Nutrition, and
10 Forestry, the Committee on Foreign Relations,
11 and the Committee on Banking, Housing, and
12 Urban Affairs of the Senate; and

13 (B) the Permanent Select Committee on
14 Intelligence, the Committee on Agriculture, the
15 Committee on Foreign Affairs, and the Com-
16 mittee on Financial Services of the House of
17 Representatives.

18 (2) DIRECTOR.—The term “Director” means
19 the Director of National Intelligence.

20 (3) NONMARKET ECONOMY COUNTRY.—The
21 term “nonmarket economy country” has the mean-
22 ing given that term in section 771(18) of the Tariff
23 Act of 1930 (19 U.S.C. 1677(18)).

24 (b) STUDY AND BRIEFING.—

25 (1) IN GENERAL.—Not later than 1 year after
26 the date of the enactment of this Act, the Director,

1 in coordination with the elements of the intelligence
2 community the Director considers appropriate and
3 with the Secretary of State, the Secretary of Agri-
4 culture, and the Secretary of the Treasury, shall—

5 (A) complete a study on the threat posed
6 to the United States by foreign investment in
7 agricultural land in the United States; and

8 (B) provide to the appropriate committees
9 of Congress a briefing on the results of the
10 study.

11 (2) DATA.—In conducting the study required
12 by paragraph (1), the Director shall process and
13 analyze relevant data collected by the Secretary of
14 State, the Secretary of Agriculture, and the Sec-
15 retary of the Treasury, including the information
16 submitted to the Secretary of Agriculture under sec-
17 tion 2 of the Agricultural Foreign Investment Dis-
18 closure Act of 1978 (7 U.S.C. 3501).

19 (3) ELEMENTS.—The study required by para-
20 graph (1) shall include the following:

21 (A) Data and an analysis of agricultural
22 land holdings, including current and previous
23 uses of the land disaggregated by sector and in-
24 dustry, in each county in the United States held
25 by a foreign person from—

1 (i) a country identified as a country
2 that poses a risk to the national security of
3 the United States in the most recent an-
4 nual report on worldwide threats issued by
5 the Director pursuant to section 108B of
6 the National Security Act of 1947 (50
7 U.S.C. 3043b) (commonly known as the
8 “Annual Threat Assessment”);

9 (ii) a nonmarket economy country; or

10 (iii) any other country that the Direc-
11 tor determines to be appropriate.

12 (B) An analysis of the proximity of the ag-
13 ricultural land holdings to critical infrastructure
14 and military installations.

15 (C) An assessment of the threats posed to
16 the national security of the United States by
17 malign actors that use foreign investment in ag-
18 ricultural land in the United States.

19 (D) An assessment of warning indicators
20 and methods by which to detect potential
21 threats from the use by foreign adversaries of
22 agricultural products for nefarious ends.

23 (E) An assessment of additional resources
24 or authorities necessary to counter threats iden-
25 tified during the study.

1 **SEC. 433. ASSESSMENT OF THREAT POSED BY CITIZENSHIP-**
2 **BY-INVESTMENT PROGRAMS.**

3 (a) DEFINITIONS.—In this section:

4 (1) APPROPRIATE COMMITTEES OF CON-
5 GRESS.—The term “appropriate committees of Con-
6 gress” means—

7 (A) the Committee on Homeland Security
8 and Governmental Affairs, the Committee on
9 Foreign Relations, the Committee on Banking,
10 Housing, and Urban Affairs, the Select Com-
11 mittee on Intelligence, and the Committee on
12 the Judiciary of the Senate; and

13 (B) the Committee on Homeland Security,
14 the Committee on Foreign Affairs, the Com-
15 mittee on Financial Services, the Permanent
16 Select Committee on Intelligence, and the Com-
17 mittee on the Judiciary of the House of Rep-
18 resentatives.

19 (2) ASSISTANT SECRETARY.—The term “Assist-
20 ant Secretary” means the Assistant Secretary for
21 Intelligence and Analysis of the Department of the
22 Treasury.

23 (3) CITIZENSHIP-BY-INVESTMENT PROGRAM.—
24 The term “citizenship-by-investment program”
25 means an immigration, investment, or other pro-
26 gram of a foreign country that, in exchange for a

1 covered contribution, authorizes the individual mak-
2 ing the covered contribution to acquire citizenship in
3 such country, including temporary or permanent res-
4 idence that may serve as the basis for subsequent
5 naturalization.

6 (4) COVERED CONTRIBUTION.—The term “cov-
7 ered contribution” means—

8 (A) an investment in, or a monetary dona-
9 tion or any other form of direct or indirect cap-
10 ital transfer to, including through the purchase
11 or rental of real estate—

12 (i) the government of a foreign coun-
13 try; or

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

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

19 (5) DIRECTOR.—The term “Director” means
20 the Director of National Intelligence.

21 (b) ASSESSMENT OF THREAT POSED BY CITIZEN-
22 SHIP-BY-INVESTMENT PROGRAMS.—

23 (1) ASSESSMENT.—Not later than 1 year after
24 the date of the enactment of this Act, the Director
25 and the Assistant Secretary, in coordination with the

1 heads of the other elements of the intelligence com-
2 munity and the head of any appropriate Federal
3 agency, shall complete an assessment of the threat
4 posed to the United States by citizenship-by-invest-
5 ment programs.

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

8 (A) An identification of each citizenship-
9 by-investment program, including an identifica-
10 tion of the foreign country that operates each
11 such program.

12 (B) With respect to each citizenship-by-in-
13 vestment program identified under subpara-
14 graph (A)—

15 (i) a description of the types of invest-
16 ments required under the program; and

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

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

24 (i) to evade sanctions or taxes;

25 (ii) to facilitate or finance—

1 (I) crimes relating to national se-
2 curity, including terrorism, weapons
3 trafficking or proliferation,
4 cybercrime, drug trafficking, human
5 trafficking, and espionage; or

6 (II) any other activity that fur-
7 thers the interests of a foreign adver-
8 sary or undermines the integrity of
9 the immigration laws or security of
10 the United States; or

11 (iii) to undermine the United States
12 and its interests through any other means
13 identified by the Director and the Assist-
14 ant Secretary.

15 (D) An identification of the foreign coun-
16 tries the citizenship-by-investment programs of
17 which pose the greatest threat to the national
18 security of the United States.

19 (3) REPORT AND BRIEFING.—

20 (A) REPORT.—

21 (i) IN GENERAL.—Not later than 180
22 days after completing the assessment re-
23 quired by paragraph (1), the Director and
24 the Assistant Secretary shall jointly submit
25 to the appropriate committees of Congress

1 a report on the findings of the Director
2 and the Assistant Secretary with respect to
3 the assessment.

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

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

10 (II) Recommendations for addi-
11 tional resources or authorities nec-
12 essary to counter such threats.

13 (III) A description of opportuni-
14 ties to counter such threats.

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

19 (B) BRIEFING.—Not later than 90 days
20 after the date on which the report required by
21 subparagraph (A) is submitted, the Director
22 and Assistant Secretary shall provide the appro-
23 priate committees of Congress with a briefing
24 on the report.

1 **SEC. 434. MITIGATING THE USE OF UNITED STATES COMPO-**
2 **NENTS AND TECHNOLOGY IN HOSTILE AC-**
3 **TIVITIES BY FOREIGN ADVERSARIES.**

4 (a) FINDINGS.—Congress finds the following:

5 (1) Foreign defense material, including ad-
6 vanced military and intelligence capabilities, con-
7 tinues to rely heavily on products and services
8 sourced from the United States.

9 (2) Iran drones operating against Ukraine were
10 found to include several United States components.

11 (3) The components described in paragraph (2)
12 came from 13 different United States companies and
13 are integral to the operation of the drones.

14 (4) The Chinese spy balloon that flew across
15 the United States in 2023 used a United States
16 internet service provider to communicate.

17 (5) The connection allowed the balloon to send
18 burst transmissions, or high-bandwidth collections of
19 data over short periods.

20 (6) Foreign adversaries and affiliated foreign
21 defense companies frequently acquire components
22 and services, sourced from the United States,
23 through violation of United States export control
24 laws.

25 (b) SUPPLY CHAIN RISK MITIGATION.—Not later
26 than 180 days after the date of the enactment of this Act,

1 the Director of National Intelligence shall, in collaboration
2 with such heads of elements of the intelligence community
3 as the Director considers appropriate, develop and com-
4 mence implementation of a strategy to work with United
5 States companies to mitigate or disrupt the acquisition
6 and use of United States components in the conduct of
7 activities harmful to the national security of the United
8 States.

9 (c) GOAL.—The goal of the strategy required by sub-
10 section (b) shall be to inform and provide intelligence sup-
11 port to government and private sector entities in pre-
12 venting United States components and technologies from
13 aiding or supporting hostile or harmful activities con-
14 ducted by foreign adversaries of the United States.

15 (d) CONSULTATION.—In developing and imple-
16 menting the strategy required by subsection (b), the Di-
17 rector of National Intelligence—

18 (1) shall consult with the Secretary of Com-
19 merce, the Secretary of Defense, and the Secretary
20 of Homeland Security; and

21 (2) may consult with such other heads of Fed-
22 eral departments or agencies as the Director of Na-
23 tional Intelligence considers appropriate.

24 (e) ANNUAL REPORTS.—Not later than 1 year after
25 the date of the enactment of this Act and annually there-

1 after until the date that is 3 years after the date of the
 2 enactment of this Act, the Director shall submit to Con-
 3 gress an annual report on the status and effect of the im-
 4 plementation of the strategy required by subsection (b).

5 **SEC. 435. OFFICE OF INTELLIGENCE AND COUNTERINTEL-**
 6 **LIGENCE REVIEW OF VISITORS AND ASSIGN-**
 7 **EES.**

8 (a) DEFINITIONS.—In this section:

9 (1) APPROPRIATE CONGRESSIONAL COMMIT-
 10 TEES.—The term “appropriate congressional com-
 11 mittees” means—

12 (A) the Select Committee on Intelligence
 13 and the Committee on Energy and Natural Re-
 14 sources of the Senate; and

15 (B) the Permanent Select Committee on
 16 Intelligence and the Committee on Energy and
 17 Commerce of the House of Representatives.

18 (2) ASSIGNEE; VISITOR.—The terms “assignee”
 19 and “visitor” mean a foreign national from a coun-
 20 try identified in the report submitted to Congress by
 21 the Director of National Intelligence in 2024 pursu-
 22 ant to section 108B of the National Security Act of
 23 1947 (50 U.S.C. 3043b) (commonly referred to as
 24 the “Annual Threat Assessment”) as “engaging in
 25 competitive behavior that directly threatens U.S. na-

1 tional security”, who is not an employee of a Na-
2 tional Laboratory, and has requested access to the
3 premises, information, or technology of a National
4 Laboratory.

5 (3) DIRECTOR.—The term “Director” means
6 the Director of the Office of Intelligence and Coun-
7 terintelligence of the Department of Energy (or their
8 designee).

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

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

17 (6) NON-TRADITIONAL COLLECTOR.—The term
18 “non-traditional collector” means an individual not
19 employed by a foreign intelligence service, who is
20 seeking access to sensitive information about a capa-
21 bility, research, or organizational dynamics of the
22 United States to inform a foreign adversary or non-
23 state actor.

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

1 (1) The National Laboratories conduct critical,
2 cutting-edge research across a range of scientific dis-
3 ciplines that provide the United States with a tech-
4 nological edge over other countries.

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

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

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

18 (5) Approximately 40,000 citizens of foreign
19 countries, including more than 8,000 citizens from
20 China and Russia, were granted access to the prem-
21 ises, information, or technology of National Labora-
22 tories in fiscal year 2023.

23 (6) The Office of Intelligence and Counterintel-
24 ligence of the Department of Energy is responsible
25 for identifying and mitigating counterintelligence

1 risks to the Department, including the National
2 Laboratories.

3 (c) SENSE OF THE SENATE.—It is the sense of the
4 Senate that, before being granted access to the premises,
5 information, or technology of a National Laboratory, citi-
6 zens of foreign countries identified in the 2024 Annual
7 Threat Assessment of the intelligence community as “en-
8 gaging in competitive behavior that directly threatens U.S.
9 national security” should be appropriately screened by the
10 National Laboratory to which they seek access, and by the
11 Office of Intelligence and Counterintelligence of the De-
12 partment, to identify and mitigate risks associated with
13 granting the requested access to sensitive military, or
14 dual-use technologies.

15 (d) REVIEW OF SENSITIVE COUNTRY VISITOR AND
16 ASSIGNEE ACCESS REQUESTS.—The Director shall pro-
17 mulgate a policy to assess the counterintelligence risk each
18 visitor or assignee poses to the research or activities un-
19 dertaken at a National Laboratory.

20 (e) ADVICE WITH RESPECT TO VISITORS OR ASSIGN-
21 EES.—

22 (1) IN GENERAL.—The Director shall provide
23 advice to a National Laboratory on visitors and as-
24 signees when 1 or more of the following conditions
25 are present:

1 (A) The Director has reason to believe that
2 a visitor or assignee is a non-traditional intel-
3 ligence collector.

4 (B) The Director is in receipt of informa-
5 tion indicating that a visitor or assignee con-
6 stitutes a counterintelligence risk to a National
7 Laboratory.

8 (2) ADVICE DESCRIBED.—Advice provided to a
9 National Laboratory in accordance with paragraph
10 (1) shall include—

11 (A) a description of the assessed risk;

12 (B) recommendations to mitigate the risk;

13 and

14 (C) identification of research or technology
15 that would be at risk if access is granted to the
16 visitor or assignee concerned.

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

21 (1) the number of visitors or assignees per-
22 mitted to access the premises, information, or tech-
23 nology of each National Laboratory;

1 (2) the number of instances in which the Direc-
 2 tor advised a National Laboratory in accordance
 3 with subsection (e); and

4 (3) the number of instances in which a National
 5 Laboratory admitted a visitor or assignee against
 6 the advice of the Director.

7 **SEC. 436. PROHIBITION ON NATIONAL LABORATORIES AD-**
 8 **MITTING CERTAIN FOREIGN NATIONALS.**

9 (a) DEFINITIONS.—In this section:

10 (1) ASSIGNEE.—The term “assignee” means an
 11 individual who is seeking approval from, or has been
 12 approved by, a National Laboratory to access the
 13 premises, information, or technology of the National
 14 Laboratory for a period of more than 30 consecutive
 15 days.

16 (2) COVERED FOREIGN NATIONAL.—

17 (A) IN GENERAL.—The term “covered for-
 18 eign national” means a foreign national of any
 19 of the following countries:

20 (i) The People’s Republic of China.

21 (ii) The Russian Federation.

22 (iii) The Islamic Republic of Iran.

23 (iv) The Democratic People’s Republic
 24 of Korea.

25 (v) The Republic of Cuba.

1 (B) EXCLUSION.—The term “covered for-
 2 eign national” does not include an individual
 3 that is lawfully admitted for permanent resi-
 4 dence (as defined in section 101(a) of the Im-
 5 migration and Nationality Act (8 U.S.C.
 6 1101(a))).

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

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

15 (5) SENIOR COUNTERINTELLIGENCE OFFI-
 16 CIAL.—The term “senior counterintelligence official”
 17 means—

18 (A) the Director of the Federal Bureau of
 19 Investigation;

20 (B) the Deputy Director of the Federal
 21 Bureau of Investigation;

22 (C) the Executive Assistant Director of the
 23 National Security Branch of the Federal Bu-
 24 reau of Investigation; or

1 (D) the Assistant Director of the Counter-
2 intelligence Division of the Federal Bureau of
3 Investigation.

4 (6) VISITOR.—The term “visitor” means an in-
5 dividual who is seeking approval from, or has been
6 approved by, a National Laboratory to access the
7 premises, information, or technology of the National
8 Laboratory for any period shorter than a period de-
9 scribed in paragraph (1).

10 (b) PROHIBITION.—

11 (1) IN GENERAL.—Except as provided in para-
12 graph (2), beginning on the date of enactment of
13 this Act, a National Laboratory—

14 (A) shall not admit as a visitor or assignee
15 any covered foreign national; and

16 (B) shall prohibit access to any visitor or
17 assignee that is a covered foreign national and
18 has sought or obtained approval to access the
19 premises, information, or technology of the Na-
20 tional Laboratory as of that date.

21 (2) WAIVER.—Paragraph (1) shall not apply to
22 a National Laboratory if the Secretary of Energy, in
23 consultation with the Director of the Office of Intel-
24 ligence and Counterintelligence of the Department of
25 Energy and a senior counterintelligence official, cer-

1 tifies and issues a waiver to the National Laboratory
2 requesting to admit a covered foreign national as a
3 visitor or assignee, in writing, that the benefits to
4 the United States of admittance or access by that
5 covered foreign national outweigh the national secu-
6 rity and economic risks to the United States.

7 (3) NOTIFICATION TO CONGRESS.—Not later
8 than 30 days after the date that a waiver is issued
9 pursuant to paragraph (2), the Secretary of Energy
10 shall submit to the Select Committee on Intelligence
11 of the Senate, the Committee on Energy and Nat-
12 ural Resources of the Senate, the Committee on
13 Commerce, Science, and Transportation of the Sen-
14 ate, the Permanent Select Committee on Intelligence
15 of the House of Representatives, the Committee on
16 Energy and Commerce of the House of Representa-
17 tives, and the Committee on Science, Space, and
18 Technology of the House of Representatives a notifi-
19 cation describing each waiver issued pursuant to
20 paragraph (2), including—

21 (A) the country of origin of the covered
22 foreign national who is the subject of the waiv-
23 er;

1 (B) the date of the request by the covered
 2 foreign national for admission or access to a
 3 National Laboratory;

4 (C) the date on which the decision to issue
 5 the waiver was made; and

6 (D) the specific reasons for issuing the
 7 waiver.

8 **SEC. 437. QUARTERLY REPORT ON CERTAIN FOREIGN NA-**
 9 **TIONALS ENCOUNTERED AT THE UNITED**
 10 **STATES BORDER.**

11 (a) DEFINITIONS.—In this section:

12 (1) ENCOUNTERED.—The term “encountered”,
 13 with respect to a special interest alien, means phys-
 14 ically apprehended by U.S. Customs and Border
 15 Protection personnel.

16 (2) SPECIAL INTEREST ALIEN.—The term “spe-
 17 cial interest alien” means an alien (as defined in sec-
 18 tion 101(a)(3) of the Immigration and Nationality
 19 Act (8 U.S.C. 1101(a)(3)) who, based upon an anal-
 20 ysis of travel patterns and other information avail-
 21 able to the United States Government, potentially
 22 poses a threat to the national security of the United
 23 States and its interests due to a known or potential
 24 nexus to terrorism, espionage, organized crime, or
 25 other malign actors.

1 (b) IN GENERAL.—Not later than 60 days after the
 2 date of the enactment of this Act, and quarterly thereafter
 3 for the following 3 years, the Secretary of Homeland Secu-
 4 rity, in coordination with the Director of National Intel-
 5 ligence, shall publish, on a publicly accessible website of
 6 the Department of Homeland Security, a report identi-
 7 fying the aggregate number of special interest aliens who,
 8 during the applicable reporting period—

9 (1) have been encountered at or near an inter-
 10 national border of the United States; and

11 (2)(A) have been released from custody;

12 (B) are under supervision;

13 (C) are being detained by the Department of
 14 Homeland Security; or

15 (D) have been removed from the United States.

16 **SEC. 438. ASSESSMENT OF THE LESSONS LEARNED BY THE**
 17 **INTELLIGENCE COMMUNITY WITH RESPECT**
 18 **TO THE ISRAEL-HAMAS WAR.**

19 (a) IN GENERAL.—Not later than 90 days after the
 20 date of the enactment of this Act, the Director of National
 21 Intelligence, in consultation with such other heads of ele-
 22 ments of the intelligence community as the Director con-
 23 siders appropriate, shall submit to the appropriate com-
 24 mittees of Congress a written assessment of the lessons
 25 learned from the Israel-Hamas war.

1 (b) ELEMENTS.—The assessment required by sub-
2 section (a) shall include the following:

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

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

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

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

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

19 (c) FORM.—The assessment required by subsection
20 (a) shall be submitted in unclassified form, but may in-
21 clude a classified annex.

22 (d) APPROPRIATE COMMITTEES OF CONGRESS DE-
23 FINED.—In this section, the term “appropriate commit-
24 tees of Congress” means—

25 (1) the congressional intelligence committees;

1 (2) the Committee on Armed Services and the
2 Committee on Appropriations of the Senate; and

3 (3) the Committee on Armed Services and the
4 Committee on Appropriations of the House of Rep-
5 resentatives.

6 **SEC. 439. CENTRAL INTELLIGENCE AGENCY INTELLIGENCE**

7 **ASSESSMENT ON TREN DE ARAGUA.**

8 (a) IN GENERAL.—Not later than 90 days after the
9 date of the enactment of this Act, the Director of the Cen-
10 tral Intelligence Agency, in consultation with such other
11 heads of elements of the intelligence community as the Di-
12 rector considers appropriate, shall submit to the appro-
13 priate committees of Congress an intelligence assessment
14 on the gang known as “Tren de Aragua”.

15 (b) ELEMENTS.—The intelligence assessment re-
16 quired by subsection (a) shall include the following:

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

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

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

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

5 (5) A description of the degree to which Tren
6 de Aragua cooperates or competes with other crimi-
7 nal organizations in the Western Hemisphere.

8 (6) An estimate of the annual revenue received
9 by Tren de Aragua from the sale of illicit drugs, kid-
10 napping, and human trafficking, disaggregated by
11 activity.

12 (7) A determination on whether Tren De
13 Aragua meets the definition of “significant
14 transnational criminal organization” in section 3 of
15 Executive Order 13581 (76 Fed. Reg. 44757; relat-
16 ing to blocking property of transnational criminal or-
17 ganizations), as amended by Executive Order 13863
18 (84 Fed. Reg. 10255; relating to taking additional
19 steps to address the national emergency with respect
20 to significant transnational criminal organizations).

21 (8) Any other information the Director of the
22 Central Intelligence Agency considers relevant.

23 (c) FORM.—The intelligence assessment required by
24 subsection (a) may be submitted in classified form.

1 (d) DEFINITION OF APPROPRIATE COMMITTEES OF
2 CONGRESS.—In this section, the term “appropriate com-
3 mittees of Congress” means—

4 (1) the congressional intelligence committees;

5 (2) the Committee on Foreign Relations, the
6 Committee on Homeland Security and Governmental
7 Affairs, the Committee on Banking, Housing, and
8 Urban Affairs, and the Committee on Appropria-
9 tions of the Senate; and

10 (3) the Committee on Foreign Affairs, the
11 Committee on Homeland Security, and the Com-
12 mittee on Appropriations of the House of Represent-
13 atives.

14 **SEC. 440. ASSESSMENT OF MADURO REGIME’S ECONOMIC**
15 **AND SECURITY RELATIONSHIPS WITH STATE**
16 **SPONSORS OF TERRORISM AND FOREIGN**
17 **TERRORIST ORGANIZATIONS.**

18 (a) IN GENERAL.—Not later than 90 days after the
19 date of the enactment of this Act, the Director of National
20 Intelligence shall submit to the congressional intelligence
21 committees a written assessment of the economic and se-
22 curity relationships of the regime of Nicolás Maduro of
23 Venezuela with the countries and organizations described
24 in subsection (b), including formal and informal support
25 to and from such countries and organizations.

1 (b) COUNTRIES AND ORGANIZATIONS DESCRIBED.—

2 The countries and organizations described in this sub-
3 section are the following:

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

6 (A) The Republic of Cuba.

7 (B) The Islamic Republic of Iran.

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

10 (A) The National Liberation Army (ELN).

11 (B) The Revolutionary Armed Forces of
12 Colombia—People’s Army (FARC-EP).

13 (C) The Segunda Marquetalia.

14 (c) FORM.—The assessment required by subsection
15 (a) shall be submitted in unclassified form, but may in-
16 clude a classified annex.

17 **SEC. 441. CONTINUED CONGRESSIONAL OVERSIGHT OF**
18 **IRANIAN EXPENDITURES SUPPORTING FOR-**
19 **EIGN MILITARY AND TERRORIST ACTIVITIES.**

20 (a) UPDATE REQUIRED.—Not later than 90 days
21 after the date of the enactment of this Act, the Director
22 of National Intelligence shall submit to the congressional
23 intelligence committees an update to the report submitted
24 under section 6705 of the Damon Paul Nelson and Mat-
25 thew Young Pollard Intelligence Authorization Act for

1 Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412) to
2 reflect current occurrences, circumstances, and expendi-
3 tures.

4 (b) FORM.—The update submitted pursuant to sub-
5 section (a) shall be submitted in unclassified form, but
6 may include a classified annex.

7 **TITLE V—EMERGING** 8 **TECHNOLOGIES**

9 **SEC. 501. STRATEGY TO COUNTER FOREIGN ADVERSARY** 10 **EFFORTS TO UTILIZE BIOTECHNOLOGIES IN** 11 **WAYS THAT THREATEN UNITED STATES NA-** 12 **TIONAL SECURITY.**

13 (a) SENSE OF CONGRESS.—It is the sense of Con-
14 gress that as biotechnologies become increasingly impor-
15 tant with regard to the national security interests of the
16 United States, and with the addition of biotechnologies to
17 the biosecurity mission of the National Counterprolifera-
18 tion and Biosecurity Center, the intelligence community
19 must articulate and implement a whole-of-government
20 strategy for addressing concerns relating to biotech-
21 nologies.

22 (b) STRATEGY FOR BIOTECHNOLOGIES CRITICAL TO
23 NATIONAL SECURITY.—

24 (1) STRATEGY REQUIRED.—Not later than 90
25 days after the date of the enactment of this Act, the

1 Director of National Intelligence shall, acting
2 through the Director of the National Counterpro-
3 liferation and Biosecurity Center and in coordination
4 with the heads of such other elements of the intel-
5 ligence community as the Director of National Intel-
6 ligence considers appropriate, develop and submit to
7 the congressional intelligence committees a whole-of-
8 government strategy to address concerns relating to
9 biotechnologies.

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

13 (A) Identification and assessment of bio-
14 technologies critical to the national security of
15 the United States, including an assessment of
16 which materials involve a dependency on foreign
17 adversary nations.

18 (B) A determination of how best to
19 counter foreign adversary efforts to utilize bio-
20 technologies that threaten the national security
21 of the United States, including technologies
22 identified pursuant to paragraph (1).

23 (C) A plan to support United States ef-
24 forts and capabilities to secure the United
25 States supply chains of the technologies identi-

1 fied pursuant to paragraph (1), by coordi-
 2 nating—

3 (i) across the intelligence community;

4 (ii) the support provided by the intel-
 5 ligence community to other relevant Fed-
 6 eral agencies and policymakers;

7 (iii) the engagement of the intelligence
 8 community with private sector entities; and

9 (iv) how the intelligence community
 10 can support securing United States supply
 11 chains for and use of biotechnologies.

12 (D) Proposals for such legislative or ad-
 13 ministrative action as the Directors consider
 14 necessary to support the strategy.

15 **SEC. 502. IMPROVEMENTS TO THE ROLES, MISSIONS, AND**
 16 **OBJECTIVES OF THE NATIONAL COUNTER-**
 17 **PROLIFERATION AND BIOSECURITY CENTER.**

18 Section 119A of the National Security Act of 1947
 19 (50 U.S.C. 3057) is amended—

20 (1) in subsection (a)(4), by striking “biosecurity
 21 and” and inserting “counterproliferation, biosecu-
 22 rity, and”; and

23 (2) in subsection (b)—

24 (A) in paragraph (1)—

1 (i) in subparagraph (A), by striking
2 “analyzing and”;

3 (ii) in subparagraph (C), by striking
4 “Establishing” and inserting “Coordi-
5 nating the establishment of”;

6 (iii) in subparagraph (D), by striking
7 “Disseminating” and inserting “Over-
8 seeing the dissemination of”;

9 (iv) in subparagraph (E), by inserting
10 “and coordinating” after “Conducting”;
11 and

12 (v) in subparagraph (G), by striking
13 “Conducting” and inserting “Coordinating
14 and advancing”; and

15 (B) in paragraph (2)—

16 (i) in subparagraph (B), by striking
17 “and analysis”;

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

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

23 “(C) Overseeing and coordinating the anal-
24 ysis of intelligence on biosecurity and foreign
25 biological threats in support of the intelligence

needs of Federal departments and agencies responsible for public health, including by providing analytic priorities to elements of the intelligence community and by conducting and coordinating net assessments.”;

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

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

(vi) by adding at the end the following:

“(G) Coordinating with relevant elements of the intelligence community and other Federal departments and agencies responsible for public health to engage with private sector entities on information relevant to biosecurity, biotechnology, and foreign biological threats.”.

**SEC. 503. ENHANCING CAPABILITIES TO DETECT FOREIGN
ADVERSARY THREATS RELATING TO BIO-
LOGICAL DATA.**

Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence

1 shall, in consultation with the heads of such Federal de-
2 partments and agencies as the Director considers appro-
3 priate, take the following steps to standardize and enhance
4 the capabilities of the intelligence community to detect for-
5 eign adversary threats relating to biological data:

6 (1) Prioritize the collection, analysis, and dis-
7 semination of information relating to foreign adver-
8 sary use of biological data, particularly in ways that
9 threaten or could threaten the national security of
10 the United States.

11 (2) Issue policy guidance within the intelligence
12 community—

13 (A) to standardize the handling and proc-
14 essing of biological data, including with respect
15 to protecting the civil liberties and privacy of
16 United States persons;

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

20 (C) to standardize the creation of
21 metadata relating to biological data.

22 (3) Ensure coordination with such Federal de-
23 partments and agencies and entities in the private
24 sector as the Director considers appropriate to un-
25 derstand how foreign adversaries are accessing and

1 using biological data stored within the United
2 States.

3 **SEC. 504. NATIONAL SECURITY PROCEDURES TO ADDRESS**
4 **CERTAIN RISKS AND THREATS RELATING TO**
5 **ARTIFICIAL INTELLIGENCE.**

6 (a) FINDINGS.—Congress finds the following:

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

12 (2) The growing capabilities of artificial intel-
13 ligence systems in the areas described in paragraph
14 (1), as well as the greater accessibility of large-scale
15 artificial intelligence models and advanced computa-
16 tion capabilities to individuals, businesses, and gov-
17 ernments, have dramatically increased the adoption
18 of artificial intelligence products in the United
19 States and globally.

20 (3) The advanced capabilities of the systems de-
21 scribed in paragraph (1), and their accessibility to a
22 wide-range of users, have increased the likelihood
23 and effect of misuse or malfunction of these systems,
24 such as to generate synthetic media for
25 disinformation campaigns, develop or refine malware

1 for computer network exploitation activity, enhance
2 surveillance capabilities in ways that undermine the
3 privacy of citizens of the United States, and increase
4 the risk of exploitation or malfunction of information
5 technology systems incorporating artificial intel-
6 ligence systems in mission-critical fields such as
7 health care, critical infrastructure, and transpor-
8 tation.

9 (b) PROCEDURES REQUIRED.—Not later than 180
10 days after the date of the enactment of this Act, the Presi-
11 dent shall develop and issue procedures to facilitate and
12 promote mechanisms by which—

13 (1) vendors of advanced computation capabili-
14 ties, vendors and commercial users of artificial intel-
15 ligence systems, as well as independent researchers
16 and other third parties, may effectively notify appro-
17 priate elements of the United States Government
18 of—

19 (A) information security risks emanating
20 from artificial intelligence systems, such as the
21 use of an artificial intelligence system to de-
22 velop or refine malicious software;

23 (B) information security risks such as indi-
24 cations of compromise or other threat informa-
25 tion indicating a compromise to the confiden-

1 tiality, integrity, or availability of an artificial
2 intelligence system, or to the supply chain of an
3 artificial intelligence system, including training
4 or test data, frameworks, computing environ-
5 ments, or other components necessary for the
6 training, management, or maintenance of an ar-
7 tificial intelligence system;

8 (C) biosecurity risks emanating from artifi-
9 cial intelligence systems, such as the use of an
10 artificial intelligence system to design, develop,
11 or acquire dual-use biological entities such as
12 putatively toxic small molecules, proteins, or
13 pathogenic organisms;

14 (D) suspected foreign malign influence (as
15 defined by section 119C of the National Secu-
16 rity Act of 1947 (50 U.S.C. 3059(f))) activity
17 that appears to be facilitated by an artificial in-
18 telligence system; and

19 (E) any other unlawful activity facilitated
20 by, or directed at, an artificial intelligence sys-
21 tem;

22 (2) elements of the Federal Government may
23 provide threat briefings to vendors of advanced com-
24 putation capabilities and vendors of artificial intel-
25 ligence systems, alerting them, as may be appro-

1 piate, to potential or confirmed foreign exploitation
2 of their systems, as well as malign foreign plans and
3 intentions.

4 (c) BRIEFING REQUIRED.—

5 (1) APPROPRIATE COMMITTEES OF CON-
6 GRESS.—In this subsection, the term “appropriate
7 committees of Congress” means—

8 (A) the congressional intelligence commit-
9 tees;

10 (B) the Committee on Homeland Security
11 and Governmental Affairs of the Senate; and

12 (C) the Committee on Homeland Security
13 of the House of Representatives.

14 (2) IN GENERAL.—The President shall provide
15 the appropriate committees of Congress a briefing
16 on procedures developed and issued pursuant to sub-
17 section (b).

18 (3) ELEMENTS.—The briefing provided pursu-
19 ant to paragraph (2) shall include the following:

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

1 (B) An outline of a plan for industry out-
 2 reach and public education regarding risks
 3 posed by, and directed at, artificial intelligence
 4 systems.

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

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

11 (ii) Federal agency guidelines.

12 **SEC. 505. ESTABLISHMENT OF ARTIFICIAL INTELLIGENCE**
 13 **SECURITY CENTER.**

14 (a) ESTABLISHMENT.—Not later than 90 days after
 15 the date of the enactment of this Act, the Director of the
 16 National Security Agency shall establish an Artificial In-
 17 telligence Security Center within the Cybersecurity Col-
 18 laboration Center of the National Security Agency.

19 (b) FUNCTIONS.—The functions of the Artificial In-
 20 telligence Security Center shall be as follows:

21 (1) Making available a research test bed to pri-
 22 vate sector and academic researchers, on a sub-
 23 sidized basis, to engage in artificial intelligence secu-
 24 rity research, including through the secure provision
 25 of access in a secure environment to proprietary

1 third-party models, with the consent of the vendors
2 of the models.

3 (2) Developing guidance to prevent or mitigate
4 counter-artificial intelligence techniques.

5 (3) Promoting secure artificial intelligence
6 adoption practices for managers of national security
7 systems (as defined in section 3552 of title 44,
8 United States Code) and elements of the defense in-
9 dustrial base.

10 (4) Coordinating with the Artificial Intelligence
11 Safety Institute of the National Institute of Stand-
12 ards and Technology.

13 (5) Such other functions as the Director con-
14 siders appropriate.

15 (c) TEST BED REQUIREMENTS.—

16 (1) ACCESS AND TERMS OF USAGE.—

17 (A) RESEARCHER ACCESS.—The Director
18 shall establish terms of usage governing re-
19 searcher access to the test bed made available
20 under subsection (b)(1), with limitations on re-
21 searcher publication only to the extent nec-
22 essary to protect classified information or pro-
23 prietary information concerning third-party
24 models provided through the consent of model
25 vendors.

1 (B) AVAILABILITY TO FEDERAL AGEN-
2 CIES.—The Director shall ensure that the test
3 bed made available under subsection (b)(1) is
4 also made available to other Federal agencies
5 on a cost-recovery basis.

6 (2) USE OF CERTAIN INFRASTRUCTURE AND
7 OTHER RESOURCES.—In carrying out subsection
8 (b)(1), the Director shall leverage, to the greatest
9 extent practicable, infrastructure and other re-
10 sources provided under section 5.2 of the Executive
11 Order dated October 30, 2023 (relating to safe, se-
12 cure, and trustworthy development and use of artifi-
13 cial intelligence).

14 (d) ACCESS TO PROPRIETARY MODELS.—In carrying
15 out this section, the Director shall establish such mecha-
16 nisms as the Director considers appropriate, including po-
17 tential contractual incentives, to ensure the provision of
18 access to proprietary models by qualified independent
19 third-party researchers if commercial model vendors have
20 voluntarily provided models and associated resources for
21 such testing.

22 (e) COUNTER-ARTIFICIAL INTELLIGENCE DE-
23 FINED.—In this section, the term “counter-artificial intel-
24 ligence” means techniques or procedures to extract infor-
25 mation about the behavior or characteristics of an artifi-

1 cial intelligence system, or to learn how to manipulate an
 2 artificial intelligence system, in order to subvert the con-
 3 fidentiality, integrity, or availability of an artificial intel-
 4 ligence system or adjacent system.

5 **SEC. 506. SENSE OF CONGRESS ENCOURAGING INTEL-**
 6 **LIGENCE COMMUNITY TO INCREASE PRIVATE**
 7 **SECTOR CAPITAL PARTNERSHIPS AND PART-**
 8 **NERSHIP WITH OFFICE OF STRATEGIC CAP-**
 9 **ITAL OF DEPARTMENT OF DEFENSE TO SE-**
 10 **CURE ENDURING TECHNOLOGICAL ADVAN-**
 11 **TAGES.**

12 It is the sense of Congress that—

13 (1) acquisition leaders in the intelligence com-
 14 munity should further explore the strategic use of
 15 private capital partnerships to secure enduring tech-
 16 nological advantages for the intelligence community,
 17 including through the identification, development,
 18 and transfer of promising technologies to full-scale
 19 programs capable of meeting intelligence community
 20 requirements; and

21 (2) the intelligence community should under-
 22 take regular consultation with Federal partners,
 23 such as the Office of Strategic Capital of the Office
 24 of the Secretary of Defense, on best practices and
 25 lessons learned from their experiences integrating

1 these resources so as to accelerate attainment of na-
2 tional security objectives.

3 **SEC. 507. INTELLIGENCE COMMUNITY TECHNOLOGY**
4 **BRIDGE FUND.**

5 (a) DEFINITIONS.—In this section:

6 (1) NONPROFIT ORGANIZATION.—The term
7 “nonprofit organization” means an organization that
8 is described in section 501(c)(3) of the Internal Rev-
9 enue Code of 1986 and that is exempt from tax
10 under section 501(a) of such Code.

11 (2) WORK PROGRAM.—The term “work pro-
12 gram” means any agreement between In-Q-Tel and
13 a third-party company, where such third-party com-
14 pany furnishes or is furnishing a product or service
15 for use by any of In-Q-Tel’s government customers
16 to address those customers’ technology needs or re-
17 quirements.

18 (b) ESTABLISHMENT OF FUND.—There is estab-
19 lished in the Treasury of the United States a fund to be
20 known as the “Intelligence Community Technology Bridge
21 Fund” (in this subsection referred to as the “Fund”) to
22 assist in the transitioning of products or services from the
23 research and development phase to the contracting and
24 production phase.

1 (c) CONTENTS OF FUND.—The Fund shall consist of
2 amounts appropriated to the Fund, and amounts in the
3 Fund shall remain available until expended.

4 (d) AVAILABILITY AND USE OF FUND.—

5 (1) IN GENERAL.—Subject to paragraph (3),
6 amounts in the Fund shall be available to the Direc-
7 tor of National Intelligence to provide assistance to
8 a business or nonprofit organization that is
9 transitioning a product or service.

10 (2) TYPES OF ASSISTANCE.—Assistance pro-
11 vided under paragraph (1) may be distributed as
12 funds in the form of a grant, a payment for a prod-
13 uct or service, or a payment for equity.

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

18 (A) the business or nonprofit organiza-
19 tion—

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

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

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

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

(e) ADMINISTRATION OF FUND.—

(1) IN GENERAL.—The Fund shall be administered by the Director of National Intelligence.

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

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

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

5 (f) ANNUAL REPORTS.—

6 (1) IN GENERAL.—Not later than September
7 30, 2025, and each fiscal year thereafter, the Direc-
8 tor shall submit to the congressional intelligence
9 committees a report on the Fund.

10 (2) CONTENTS.—Each report submitted pursu-
11 ant to paragraph (1) shall include, for the period
12 covered by the report, information about the fol-
13 lowing:

14 (A) How much was expended or obligated
15 using amounts from the Fund.

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

18 (C) The effects of such expenditures and
19 obligations.

20 (D) A summary of annual transition activi-
21 ties and outcomes of such activities for the in-
22 telligence community.

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

1 (g) AUTHORIZATION OF APPROPRIATIONS.—

2 (1) IN GENERAL.—Subject to paragraph (2),
 3 there is authorized to be appropriated to the Fund
 4 \$75,000,000 for fiscal year 2025 and for each fiscal
 5 year thereafter.

6 (2) LIMITATION.—The amount in the Fund
 7 shall not exceed \$75,000,000 at any time.

8 **SEC. 508. ENHANCEMENT OF AUTHORITY FOR INTEL-**
 9 **LIGENCE COMMUNITY PUBLIC-PRIVATE TAL-**
 10 **ENT EXCHANGES.**

11 (a) FOCUS AREAS.—Subsection (a) of section 5306
 12 of the Damon Paul Nelson and Matthew Young Pollard
 13 Intelligence Authorization Act for Fiscal Years 2018,
 14 2019, and 2020 (50 U.S.C. 3334) is amended—

15 (1) by striking “Not later than” and inserting
 16 the following:

17 “(1) IN GENERAL.—Not later than”; and

18 (2) by adding at the end the following:

19 “(2) FOCUS AREAS.—The Director shall ensure
 20 that the policies, processes, and procedures devel-
 21 oped pursuant to paragraph (1) include a focus on
 22 rotations described in such paragraph with private-
 23 sector organizations in the following fields:

24 “(A) Finance.

25 “(B) Acquisition.

1 “(C) Biotechnology.

2 “(D) Computing.

3 “(E) Artificial intelligence.

4 “(F) Business process innovation and en-
5 trepreneurship.

6 “(G) Cybersecurity.

7 “(H) Materials and manufacturing.

8 “(I) Any other technology or research field
9 the Director determines relevant to meet evolv-
10 ing national security threats in technology sec-
11 tors.”.

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

17 (1) in paragraph (1), by striking “3 years” and
18 inserting “5 years”; and

19 (2) in paragraph (2), by striking “3 years” and
20 inserting “5 years”.

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

23 (1) in paragraph (5), by striking “; and” and
24 inserting a semicolon;

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

3 (3) by adding at the end the following:

4 “(7) shall not be considered to have a conflict
5 of interest with an element of the intelligence com-
6 munity solely because of being detailed to an ele-
7 ment of the intelligence community under this sec-
8 tion.”.

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

10 (1) by redesignating subsection (j) as sub-
11 section (k); and

12 (2) by inserting after subsection (i) the fol-
13 lowing:

14 “(j) **HIRING AUTHORITY.**—

15 “(1) **IN GENERAL.**—The Director may hire,
16 under section 213.3102(r) of title 5, Code of Federal
17 Regulations, or successor regulations, an individual
18 who is an employee of a private-sector organization
19 who is detailed to an element of the intelligence com-
20 munity under this section.

21 “(2) **NO PERSONNEL BILLET REQUIRED.**—Hir-
22 ing an individual under paragraph (1) shall not re-
23 quire a personnel billet.”.

24 (e) **ANNUAL REPORTS.**—Not later than 1 year after
25 the date of the enactment of this Act and annually there-

1 after for 2 more years, the Director of National Intel-
2 ligence shall submit to the congressional intelligence com-
3 mittees an annual report on—

4 (1) the implementation of the policies, proc-
5 esses, and procedures developed pursuant to sub-
6 section (a) of such section 5306 (50 U.S.C. 3334)
7 and the administration of such section;

8 (2) how the heads of the elements of the intel-
9 ligence community are using or plan to use the au-
10 thorities provided under such section; and

11 (3) recommendations for legislative or adminis-
12 trative action to increase use of the authorities pro-
13 vided under such section.

14 **SEC. 509. ENHANCING INTELLIGENCE COMMUNITY ABILITY**
15 **TO ACQUIRE EMERGING TECHNOLOGY THAT**
16 **FULFILLS INTELLIGENCE COMMUNITY**
17 **NEEDS.**

18 (a) DEFINITION OF WORK PROGRAM.—The term
19 “work program” means any agreement between In-Q-Tel
20 and a third-party company, where such third-party com-
21 pany furnishes or is furnishing a property, product, or
22 service for use by any of In-Q-Tel’s government customers
23 to address those customers’ technology needs or require-
24 ments.

1 (b) IN GENERAL.—In addition to the exceptions list-
 2 ed under section 3304(a) of title 41, United States Code,
 3 and under section 3204(a) of title 10, United States Code,
 4 for the use of competitive procedures, the Director of Na-
 5 tional Intelligence or the head of an element of the intel-
 6 ligence community may use procedures other than com-
 7 petitive procedures to acquire a property, product, or serv-
 8 ice if—

9 (1) the source of the property, product, or serv-
 10 ice is a company that completed a work program in
 11 which the company furnished the property, product,
 12 or service; and

13 (2) the Director of National Intelligence or the
 14 head of an element of the intelligence community
 15 certifies that such property, product, or service has
 16 been shown to meet an identified need of the intel-
 17 ligence community.

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

20 (1) IN GENERAL.—A property, product, or serv-
 21 ice may not be acquired by the Director or the head
 22 of an element of the intelligence community under
 23 subsection (b) using procedures other than competi-
 24 tive procedures unless the acquiring officer for the

1 acquisition justifies the use of such procedures in
2 writing.

3 (2) CONTENTS.—A justification in writing de-
4 scribed in paragraph (1) for an acquisition using
5 procedures other than competitive procedures shall
6 include the following:

7 (A) A description of the need of the ele-
8 ment of the intelligence community that the
9 property, product, or service satisfies.

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

12 (C) A description of the market survey
13 conducted or a statement of the reasons a mar-
14 ket survey was not conducted.

15 (D) Such other matters as the Director or
16 the head, as the case may be, determines appro-
17 priate.

18 **SEC. 510. MANAGEMENT OF ARTIFICIAL INTELLIGENCE SE-**
19 **CURITY RISKS.**

20 (a) DEFINITIONS.—In this section:

21 (1) ARTIFICIAL INTELLIGENCE SAFETY INCI-
22 DENT.—The term “artificial intelligence safety inci-
23 dent” means an event that increases the risk that
24 operation of an artificial intelligence system will—

1 (A) result in physical or psychological
2 harm; or

3 (B) lead to a state in which human life,
4 health, property, or the environment is endan-
5 gered.

6 (2) ARTIFICIAL INTELLIGENCE SECURITY INCI-
7 DENT.—The term “artificial intelligence security in-
8 cident” means an event that increases—

9 (A) the risk that operation of an artificial
10 intelligence system occurs in a way that enables
11 the extraction of information about the behavior
12 or characteristics of an artificial intelligence
13 system by a third party; or

14 (B) the ability of a third party to manipu-
15 late an artificial intelligence system to subvert
16 the confidentiality, integrity, or availability of
17 an artificial intelligence system or adjacent sys-
18 tem.

19 (3) ARTIFICIAL INTELLIGENCE SECURITY VUL-
20 NERABILITY.—The term “artificial intelligence secu-
21 rity vulnerability” means a weakness in an artificial
22 intelligence system that could be exploited by a third
23 party to, without authorization, subvert the con-
24 fidentiality, integrity, or availability of an artificial

1 intelligence system, including through techniques
 2 such as—

- 3 (A) data poisoning;
- 4 (B) evasion attacks;
- 5 (C) privacy-based attacks; and
- 6 (D) abuse attacks.

7 (4) COUNTER-ARTIFICIAL INTELLIGENCE.—The
 8 term “counter-artificial intelligence” means tech-
 9 niques or procedures to extract information about
 10 the behavior or characteristics of an artificial intel-
 11 ligence system, or to learn how to manipulate an ar-
 12 tificial intelligence system, so as to subvert the con-
 13 fidentiality, integrity, or availability of an artificial
 14 intelligence system or adjacent system.

15 (b) VOLUNTARY TRACKING AND PROCESSING OF SE-
 16 CURITY AND SAFETY INCIDENTS AND RISKS ASSOCIATED
 17 WITH ARTIFICIAL INTELLIGENCE.—

18 (1) PROCESSES AND PROCEDURES FOR VUL-
 19 NERABILITY MANAGEMENT.—Not later than 180
 20 days after the date of the enactment of this Act, the
 21 Director of the National Institute of Standards and
 22 Technology shall—

- 23 (A) initiate a process to update processes
- 24 and procedures associated with the National
- 25 Vulnerability Database of the Institute to en-

1 sure that the database and associated vulner-
 2 ability management processes incorporate artifi-
 3 cial intelligence security vulnerabilities to the
 4 greatest extent practicable; and

5 (B) identify any characteristics of artificial
 6 intelligence security vulnerabilities that make
 7 utilization of the National Vulnerability Data-
 8 base inappropriate for their management and
 9 develop processes and procedures for vulner-
 10 ability management of those vulnerabilities.

11 (2) VOLUNTARY TRACKING OF ARTIFICIAL IN-
 12 TELLIGENCE SECURITY AND ARTIFICIAL INTEL-
 13 LIGENCE SAFETY INCIDENTS.—

14 (A) VOLUNTARY DATABASE REQUIRED.—

15 Not later than 1 year after the date of the en-
 16 actment of this Act, the Director of the Insti-
 17 tute, in coordination with the Director of the
 18 Cybersecurity and Infrastructure Security
 19 Agency, shall—

20 (i) develop and establish a comprehen-
 21 sive database to publicly track artificial in-
 22 telligence security and artificial intelligence
 23 safety incidents through voluntary input;
 24 and

1 (ii) in establishing the database under
2 clause (i)—

3 (I) establish mechanisms by
4 which private sector entities, public
5 sector organizations, civil society
6 groups, and academic researchers may
7 voluntarily share information with the
8 Institute on confirmed or suspected
9 artificial intelligence security or artifi-
10 cial intelligence safety incidents, in a
11 manner that preserves the confiden-
12 tiality of any affected party;

13 (II) leverage, to the greatest ex-
14 tent possible, standardized disclosure
15 and incident description formats;

16 (III) develop processes to asso-
17 ciate reports pertaining to the same
18 incident with a single incident identi-
19 fier;

20 (IV) establish classification, in-
21 formation retrieval, and reporting
22 mechanisms that sufficiently differen-
23 tiate between artificial intelligence se-
24 curity incidents and artificial intel-
25 ligence safety incidents; and

1 (V) create appropriate
2 taxonomies to classify incidents based
3 on relevant characteristics, impact, or
4 other relevant criteria.

5 (B) IDENTIFICATION AND TREATMENT OF
6 MATERIAL ARTIFICIAL INTELLIGENCE SECURITY
7 OR ARTIFICIAL INTELLIGENCE SAFETY RISKS.—

8 (i) IN GENERAL.—Upon receipt of rel-
9 evant information on an artificial intel-
10 ligence security or artificial intelligence
11 safety incident, the Director of the Insti-
12 tute shall determine whether the described
13 incident presents a material artificial intel-
14 ligence security or artificial intelligence
15 safety risk sufficient for inclusion in the
16 database developed and established under
17 subparagraph (A).

18 (ii) PRIORITIES.—In evaluating a re-
19 ported incident pursuant to subparagraph
20 (A), the Director shall prioritize inclusion
21 in the database cases in which a described
22 incident—

23 (I) describes an artificial intel-
24 ligence system used in critical infra-
25 structure or safety-critical systems;

1 (II) would result in a high-sever-
 2 ity or catastrophic impact to the peo-
 3 ple or economy of the United States;
 4 or

5 (III) includes an artificial intel-
 6 ligence system widely used in commer-
 7 cial or public sector contexts.

8 (C) REPORTS AND ANONYMITY.—The Di-
 9 rector shall populate the database developed
 10 and established under subparagraph (A) with
 11 incidents based on public reports and informa-
 12 tion shared using the mechanism established
 13 pursuant to clause (ii)(I) of such subparagraph,
 14 ensuring that any incident description suffi-
 15 ciently anonymizes those affected, unless those
 16 who are affected have consented to their names
 17 being included in the database.

18 (c) UPDATING PROCESSES AND PROCEDURES RE-
 19 LATING TO COMMON VULNERABILITIES AND EXPOSURES
 20 PROGRAM AND EVALUATION OF CONSENSUS STANDARDS
 21 RELATING TO ARTIFICIAL INTELLIGENCE SECURITY VUL-
 22 NERABILITY REPORTING.—

23 (1) DEFINITIONS.—In this subsection:

24 (A) COMMON VULNERABILITIES AND EX-
 25 POSURES PROGRAM.—The term “Common

1 Vulnerabilities and Exposures Program” means
2 the reference guide and classification system for
3 publicly known information security
4 vulnerabilities sponsored by the Cybersecurity
5 and Infrastructure Security Agency.

6 (B) DIRECTOR.—The term “Director”
7 means the Director of the Cybersecurity and
8 Infrastructure Security Agency.

9 (C) RELEVANT CONGRESSIONAL COMMIT-
10 TEES.—The term “relevant congressional com-
11 mittees” means—

12 (i) the Committee on Homeland Secu-
13 rity and Governmental Affairs of the Sen-
14 ate;

15 (ii) the Committee on Commerce,
16 Science, and Transportation of the Senate;

17 (iii) the Select Committee on Intel-
18 ligence of the Senate;

19 (iv) the Committee on the Judiciary of
20 the Senate;

21 (v) the Committee on Oversight and
22 Accountability of the House of Representa-
23 tives;

1 (vi) the Committee on Energy and
2 Commerce of the House of Representa-
3 tives;

4 (vii) the Permanent Select Committee
5 on Intelligence of the House of Represent-
6 atives; and

7 (viii) the Committee on the Judiciary
8 of the House of Representatives.

9 (2) IN GENERAL.—Not later than 180 days
10 after the date of enactment of this Act, the Director
11 shall—

12 (A) initiate a process to update processes
13 and procedures associated with the Common
14 Vulnerabilities and Exposures Program to en-
15 sure that the program and associated processes
16 identify and enumerate artificial intelligence se-
17 curity vulnerabilities to the greatest extent
18 practicable; and

19 (B) identify any characteristic of artificial
20 intelligence security vulnerabilities that makes
21 utilization of the Common Vulnerabilities and
22 Exposures Program inappropriate for their
23 management and develop processes and proce-
24 dures for vulnerability identification and enu-

meration of those artificial intelligence security vulnerabilities.

(3) EVALUATION OF CONSENSUS STANDARDS.—

(A) IN GENERAL.—Not later than 30 days after the date of enactment of this Act, the Director of the National Institute of Standards and Technology shall initiate a multi-stakeholder process to evaluate whether existing voluntary consensus standards for vulnerability reporting effectively accommodate artificial intelligence security vulnerabilities.

(B) REPORT.—

(i) SUBMISSION.—Not later than 180 days after the date on which the evaluation under subparagraph (A) is carried out, the Director shall submit a report to the relevant congressional committees on the sufficiency of existing vulnerability reporting processes and standards to accommodate artificial intelligence security vulnerabilities.

(ii) POST-REPORT ACTION.—If the Director concludes in the report submitted under clause (i) that existing processes do not sufficiently accommodate reporting of

1 artificial intelligence security
2 vulnerabilities, the Director shall initiate a
3 process, in consultation with the Director
4 of the National Institute of Standards and
5 Technology and the Director of the Office
6 of Management and Budget, to update rel-
7 evant vulnerability reporting processes, in-
8 cluding the Department of Homeland Se-
9 curity Binding Operational Directive 20–
10 01, or any subsequent directive.

11 (4) BEST PRACTICES.—Not later than 90 days
12 after the date of enactment of this Act, the Director
13 shall, in collaboration with the Director of the Na-
14 tional Security Agency and the Director of the Na-
15 tional Institute of Standards and Technology and
16 leveraging efforts of the Information Communica-
17 tions Technology Supply Chain Risk Management
18 Task Force to the greatest extent practicable, con-
19 vene a multi-stakeholder process to encourage the
20 development and adoption of best practices relating
21 to addressing supply chain risks associated with
22 training and maintaining artificial intelligence mod-
23 els, which shall ensure consideration of supply chain
24 risks associated with—

(A) data collection, cleaning, and labeling, particularly the supply chain risks of reliance on remote workforce and foreign labor for such tasks;

(B) inadequate documentation of training data and test data storage, as well as limited provenance of training data;

(C) human feedback systems used to refine artificial intelligence systems, particularly the supply chain risks of reliance on remote workforce and foreign labor for such tasks;

(D) the use of large-scale, open-source datasets, particularly the supply chain risks to repositories that host such datasets for use by public and private sector developers in the United States; and

(E) the use of proprietary datasets containing sensitive or personally identifiable information.

SEC. 511. PROTECTION OF TECHNOLOGICAL MEASURES DESIGNED TO VERIFY AUTHENTICITY OR PROVENANCE OF MACHINE-MANIPULATED MEDIA.

(a) DEFINITIONS.—In this section:

(1) MACHINE-MANIPULATED MEDIA.—The term “machine-manipulated media” has the meaning

1 given such term in section 5724 of the Damon Paul
2 Nelson and Matthew Young Pollard Intelligence Au-
3 thorization Act for Fiscal Years 2018, 2019, and
4 2020 (Public Law 116–92; 50 U.S.C. 3024 note).

5 (2) STATE.—The term “State” means each of
6 the several States of the United States, the District
7 of Columbia, the Commonwealth of Puerto Rico, the
8 Virgin Islands, Guam, American Samoa, and the
9 Commonwealth of the Northern Mariana Islands.

10 (b) PROHIBITIONS.—

11 (1) PROHIBITION ON CONCEALING SUBVER-
12 SION.—No person shall knowingly and with the in-
13 tent or substantial likelihood of deceiving a third
14 party, enable, facilitate, or conceal the subversion of
15 a technological measure designed to verify the au-
16 thenticity, modifications, or conveyance of machine-
17 manipulated media, or characteristics of the prove-
18 nance of the machine-manipulated media, by gener-
19 ating information about the authenticity of a piece
20 of content that is knowingly false.

21 (2) PROHIBITION ON FRAUDULENT DISTRIBU-
22 TION.—No person shall knowingly and for financial
23 benefit, enable, facilitate, or conceal the subversion
24 of a technological measure described in paragraph
25 (1) by distributing machine-manipulated media with

1 knowingly false information about the authenticity
2 of a piece of machine-manipulated media.

3 (3) PROHIBITION ON PRODUCTS AND SERVICES
4 FOR CIRCUMVENTION.—No person shall deliberately
5 manufacture, import, or offer to the public a tech-
6 nology, product, service, device, component, or part
7 thereof that—

8 (A) is primarily designed or produced and
9 promoted for the purpose of circumventing, re-
10 moving, or otherwise disabling a technological
11 measure described in paragraph (1) with the in-
12 tent or substantial likelihood of deceiving a
13 third party about the authenticity of a piece of
14 machine-manipulated media;

15 (B) has only limited commercially signifi-
16 cant or expressive purpose or use other than to
17 circumvent, remove, or otherwise disable a tech-
18 nological measure designed to verify the authen-
19 ticity of machine-manipulated media and is pro-
20 moted for such purposes; or

21 (C) is marketed by that person or another
22 acting in concert with that person with that
23 person's knowledge for use in circumventing, re-
24 moving, or otherwise disabling a technological
25 measure described in paragraph (1) with an in-

1 tent to deceive a third party about the authen-
2 ticity of a piece of machine-manipulated media.

3 (c) EXEMPTIONS.—

4 (1) IN GENERAL.—Nothing in subsection (b)
5 shall inhibit the ability of any individual to access,
6 read, or review a technological measure described in
7 paragraph (1) of such subsection or to access, read,
8 or review the provenance, modification, or convey-
9 ance information contained therein.

10 (2) EXEMPTION FOR NONPROFIT LIBRARIES,
11 ARCHIVES, AND EDUCATIONAL INSTITUTIONS.—

12 (A) IN GENERAL.—Except as otherwise
13 provided in this subsection, subsection (b) shall
14 not apply to a nonprofit library, archives, or
15 educational institution which generates, distrib-
16 utes, or otherwise handles machine-manipulated
17 media.

18 (B) COMMERCIAL ADVANTAGE, FINANCIAL
19 GAIN, OR TORTIOUS CONDUCT.—The exception
20 in subparagraph (A) shall not apply to a non-
21 profit library, archive, or educational institution
22 that willfully for the purpose of commercial ad-
23 vantage, financial gain, or in furtherance of
24 tortious conduct violates a provision of sub-
25 section (b), except that a nonprofit library, ar-

chive, or educational institution that willfully
for the purpose of commercial advantage, finan-
cial gain, or in furtherance of tortious conduct
violates a provision of subsection (b) shall—

(i) for the first offense, be subject to
the civil remedies under subsection (d);
and

(ii) for repeated or subsequent of-
fenses, in addition to the civil remedies
under subsection (d), forfeit the exemption
provided under subparagraph (A).

(C) CIRCUMVENTING TECHNOLOGIES.—

This paragraph may not be used as a defense
to a claim under paragraph (3) of subsection
(b), nor may this subsection permit a nonprofit
library, archive, or educational institution to
manufacture, import, offer to the public, pro-
vide, or otherwise traffic in any technology,
product, service, component, or part thereof,
that circumvents a technological measure de-
scribed in paragraph (1) of such subsection.

(D) QUALIFICATIONS OF LIBRARIES AND

ARCHIVES.—In order for a library or archive to
qualify for the exemption under subparagraph

1 (A), the collections of that library or archive
2 shall be—

3 (i) open to the public; or

4 (ii) available not only to researchers
5 affiliated with the library or archive or
6 with the institution of which it is a part,
7 but also to other persons doing research in
8 a specialized field.

9 (3) REVERSE ENGINEERING.—

10 (A) DEFINITIONS.—In this paragraph:

11 (i) CIRCUMVENTION.—The term “cir-
12 cumvention” means to remove, deactivate,
13 disable, or impair a technological measure
14 designed to verify the authenticity of ma-
15 chine-manipulated media or characteristics
16 of its provenance, modifications, or convey-
17 ance.

18 (ii) INTEROPERABILITY.—The term
19 “interoperability” means the ability of—

20 (I) computer programs to ex-
21 change information; and

22 (II) such programs mutually to
23 use the information which has been
24 exchanged.

1 (B) IN GENERAL.—An authorized user of
2 a technological measure described in subsection
3 (b)(1) may circumvent such technological meas-
4 ure for the sole purpose of identifying and ana-
5 lyzing those elements of the technological meas-
6 ure that are necessary to achieve interoper-
7 ability with that authorized user’s own techno-
8 logical measures intended for similar purposes
9 of verifying the authenticity of machine-manip-
10 ulated media or characteristics of its prove-
11 nance, modifications, or conveyance.

12 (C) LAW ENFORCEMENT, INTELLIGENCE,
13 AND OTHER GOVERNMENT ACTIVITIES.—Sub-
14 section (b) does not prohibit any lawfully au-
15 thorized investigative, protective, information
16 security, or intelligence activity of an officer,
17 agent, or employee of the United States, a
18 State, or a political subdivision of a State, or a
19 person acting pursuant to a contract with the
20 United States, a State, or a political subdivision
21 of a State.

22 (d) ENFORCEMENT BY ATTORNEY GENERAL.—

23 (1) CIVIL ACTIONS.—The Attorney General
24 may bring a civil action in an appropriate United

1 States district court against any person who violates
2 subsection (b).

3 (2) POWERS OF THE COURT.—In an action
4 brought under paragraph (1), the court—

5 (A) may grant temporary and permanent
6 injunctions on such terms as it deems reason-
7 able to prevent or restrain a violation, but in no
8 event shall impose a prior restraint on free
9 speech or the press protected under the First
10 Amendment to the Constitution of the United
11 States;

12 (B) at any time while an action is pending,
13 may order the impounding, on such terms as it
14 deems reasonable, of any device or product that
15 is in the custody or control of the alleged viola-
16 tor and that the court has reasonable cause to
17 believe was involved in a violation;

18 (C) may award damages under paragraph
19 (3);

20 (D) in its discretion may allow the recovery
21 of costs against any party other than the
22 United States or an officer thereof; and

23 (E) may, as part of a final judgment or
24 decree finding a violation, order the remedial
25 modification or the destruction of any device or

1 product involved in the violation that is in the
2 custody or control of the violator or has been
3 impounded under subparagraph (B).

4 (3) AWARD OF DAMAGES.—

5 (A) IN GENERAL.—Except as otherwise
6 provided in this section, a person committing a
7 violation of subsection (b) is liable for statutory
8 damages as provided in subparagraph (C).

9 (B) STATUTORY DAMAGES.—

10 (i) ELECTION OF AMOUNT BASED ON
11 NUMBER OF ACTS OF CIRCUMVENTION.—

12 At any time before final judgment is en-
13 tered, the Attorney General may elect to
14 recover an award of statutory damages for
15 each violation of subsection (b) in the sum
16 of not less than \$200 or more than \$2,500
17 per act of circumvention, device, product,
18 component, offer, or performance of serv-
19 ice, as the court considers just.

20 (ii) ELECTION OF AMOUNT; TOTAL
21 AMOUNT.—At any time before final judg-
22 ment is entered, the Attorney General may
23 elect to recover an award of statutory dam-
24 ages for each violation of subsection (b) in

1 the sum of not less than \$2,500 or more
2 than \$25,000.

3 (C) REPEATED VIOLATIONS.—In any case
4 in which the Attorney General sustains the bur-
5 den of proving, and the court finds, that a per-
6 son has violated subsection (b) within 3 years
7 after a final judgment was entered against the
8 person for another such violation, the court
9 may increase the award of damages up to triple
10 the amount that would otherwise be awarded,
11 as the court considers just.

12 (D) INNOCENT VIOLATIONS.—

13 (i) IN GENERAL.—The court in its
14 discretion may reduce or remit the total
15 award of damages in any case in which the
16 violator sustains the burden of proving,
17 and the court finds, that the violator was
18 not aware and had no reason to believe
19 that its acts constituted a violation.

20 (ii) NONPROFIT LIBRARY, ARCHIVE,
21 EDUCATIONAL INSTITUTIONS, OR PUBLIC
22 BROADCASTING ENTITIES.—In the case of
23 a nonprofit library, archive, educational in-
24 stitution, or public broadcasting entity, the
25 court shall remit damages in any case in

1 which the library, archive, educational in-
 2 stitution, or public broadcasting entity sus-
 3 tains the burden of proving, and the court
 4 finds, that the library, archive, educational
 5 institution, or public broadcasting entity
 6 was not aware and had no reason to be-
 7 lieve that its acts constituted a violation.

8 **SEC. 512. SENSE OF CONGRESS ON HOSTILE FOREIGN**
 9 **CYBER ACTORS.**

10 It is the sense of Congress that foreign ransomware
 11 organizations, and foreign affiliates associated with them,
 12 constitute hostile foreign cyber actors, that covered na-
 13 tions abet and benefit from the activities of these actors,
 14 and that such actors should be treated as hostile foreign
 15 cyber actors by the United States. Such actors include the
 16 following:

- 17 (1) DarkSide.
- 18 (2) Conti.
- 19 (3) REvil.
- 20 (4) BlackCat, also known as “ALPHV”.
- 21 (5) LockBit.
- 22 (6) Rhysida, also known as “Vice Society”.
- 23 (7) Royal.
- 24 (8) Phobos, also known as “Eight” and also
 25 known as “Joanta”.

1 (9) C10p.

2 (10) Hackers associated with the SamSam
3 ransomware campaigns.

4 (11) Play.

5 (12) BianLian.

6 (13) Killnet.

7 (14) Akira.

8 (15) Ragnar Locker, also known as “Dark An-
9 gels”.

10 (16) Blacksuit.

11 (17) INC.

12 (18) Black Basta.

13 **SEC. 513. DESIGNATION OF STATE SPONSORS OF**
14 **RANSOMWARE AND REPORTING REQUIRE-**
15 **MENTS.**

16 (a) DESIGNATION OF STATE SPONSORS OF
17 RANSOMWARE.—

18 (1) IN GENERAL.—Not later than 180 days
19 after the date of the enactment of this Act, and an-
20 nually thereafter, the Secretary of State, in consulta-
21 tion with the Director of National Intelligence,
22 shall—

23 (A) designate as a state sponsor of
24 ransomware any country the government of
25 which the Secretary has determined has pro-

1 vided support for ransomware demand schemes
2 (including by providing safe haven for individ-
3 uals engaged in such schemes);

4 (B) submit to Congress a report listing the
5 countries designated under subparagraph (A);
6 and

7 (C) in making designations under subpara-
8 graph (A), take into consideration the report
9 submitted to Congress under section 514(c)(1).

10 (2) SANCTIONS AND PENALTIES.—The Presi-
11 dent shall impose with respect to each state sponsor
12 of ransomware designated under paragraph (1)(A)
13 the sanctions and penalties imposed with respect to
14 a state sponsor of terrorism.

15 (3) STATE SPONSOR OF TERRORISM DE-
16 FINED.—In this subsection, the term “state sponsor
17 of terrorism” means a country the government of
18 which the Secretary of State has determined has re-
19 peatedly provided support for acts of international
20 terrorism, for purposes of—

21 (A) section 1754(c)(1)(A)(i) of the Export
22 Control Reform Act of 2018 (50 U.S.C.
23 4813(c)(1)(A)(i));

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

1 (C) section 40(d) of the Arms Export Con-
2 trol Act (22 U.S.C. 2780(d)); or

3 (D) any other provision of law.

4 (b) REPORTING REQUIREMENTS.—

5 (1) SANCTIONS RELATING TO RANSOMWARE RE-
6 PORT.—Not later than 180 days after the date of
7 the enactment of this Act, the Secretary of the
8 Treasury shall submit a report to Congress that de-
9 scribes, for each of the 5 fiscal years immediately
10 preceding the date of such report, the number and
11 geographic locations of individuals, groups, and enti-
12 ties subject to sanctions imposed by the Office of
13 Foreign Assets Control who were subsequently deter-
14 mined to have been involved in a ransomware de-
15 mand scheme.

16 (2) COUNTRY OF ORIGIN REPORT.—The Sec-
17 retary of State, in consultation with the Director of
18 National Intelligence and the Director of the Federal
19 Bureau of Investigation, shall—

20 (A) submit a report, with a classified
21 annex, to the Committee on Foreign Relations
22 of the Senate, the Select Committee on Intel-
23 ligence of the Senate, the Committee on For-
24 eign Affairs of the House of Representatives,
25 and the Permanent Select Committee on Intel-

1 ligence of the House of Representatives that
 2 identifies the country of origin of foreign-based
 3 ransomware attacks; and

4 (B) make the report described in subpara-
 5 graph (A) (excluding the classified annex) avail-
 6 able to the public.

7 (3) INVESTIGATIVE AUTHORITIES REPORT.—

8 Not later than 180 days after the date of the enact-
 9 ment of this Act, the Comptroller General of the
 10 United States shall issue a report that outlines the
 11 authorities available to the Federal Bureau of Inves-
 12 tigation, the United States Secret Service, the Cy-
 13 bersecurity and Infrastructure Security Agency,
 14 Homeland Security Investigations, and the Office of
 15 Foreign Assets Control to respond to foreign-based
 16 ransomware attacks.

17 **SEC. 514. DEEMING RANSOMWARE THREATS TO CRITICAL**
 18 **INFRASTRUCTURE A NATIONAL INTEL-**
 19 **LIGENCE PRIORITY.**

20 (a) CRITICAL INFRASTRUCTURE DEFINED.—In this
 21 section, the term “critical infrastructure” has the meaning
 22 given such term in subsection (e) of the Critical Infra-
 23 structures Protection Act of 2001 (42 U.S.C. 5195c(e)).

24 (b) RANSOMWARE THREATS TO CRITICAL INFRA-
 25 STRUCTURE AS NATIONAL INTELLIGENCE PRIORITY.—

1 The Director of National Intelligence, pursuant to the pro-
2 visions of the National Security Act of 1947 (50 U.S.C.
3 3001 et seq.), the Intelligence Reform and Terrorism Pre-
4 vention Act of 2004 (Public Law 108–458), section
5 1.3(b)(17) of Executive Order 12333 (50 U.S.C. 3001
6 note; relating to United States intelligence activities), as
7 in effect on the day before the date of the enactment of
8 this Act, and National Security Presidential Directive–26
9 (February 24, 2003; relating to intelligence priorities), as
10 in effect on the day before the date of the enactment of
11 this Act, shall deem ransomware threats to critical infra-
12 structure a national intelligence priority component to the
13 National Intelligence Priorities Framework.

14 (c) REPORT.—

15 (1) IN GENERAL.—Not later than 180 days
16 after the date of the enactment of this Act, the Di-
17 rector of National Intelligence shall, in consultation
18 with the Director of the Federal Bureau of Inves-
19 tigation, submit to the Select Committee on Intel-
20 ligence of the Senate and the Permanent Select
21 Committee on Intelligence of the House of Rep-
22 resentatives a report on the implications of the
23 ransomware threat to United States national secu-
24 rity.

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

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

7 (B) Locations from which individuals,
8 groups, and entities conduct ransomware at-
9 tacks.

10 (C) The infrastructure, tactics, and tech-
11 niques ransomware actors commonly use.

12 (D) Any relationships between the individ-
13 uals, groups, and entities that conduct
14 ransomware attacks and their governments or
15 countries of origin that could impede the ability
16 to counter ransomware threats.

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

20 (3) FORM.—The report submitted under para-
21 graph (1) shall be submitted in unclassified form,
22 but may include a classified annex.

TITLE VI—CLASSIFICATION REFORM

SEC. 601. GOVERNANCE OF CLASSIFICATION AND DECLASSIFICATION SYSTEM.

(a) DEFINITIONS.—In this section:

(1) CONTROLLED UNCLASSIFIED INFORMATION.—The term “controlled unclassified information” means information described as “Controlled Unclassified Information” or “CUI” in Executive Order 13556 (75 Fed. Reg. 68675; relating to controlled unclassified information), or any successor order.

(2) EXECUTIVE AGENT.—The term “Executive Agent” means the Executive Agent for Classification and Declassification designated under subsection (b)(1)(A).

(3) EXECUTIVE COMMITTEE.—The term “Executive Committee” means the Executive Committee on Classification and Declassification Programs and Technology established under subsection (b)(1)(C).

(b) ESTABLISHMENT OF CLASSIFICATION AND DECLASSIFICATION GOVERNANCE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the President shall—

1 (A) designate a Federal official as Execu-
2 tive Agent for Classification and Declassifica-
3 tion to identify and promote technological solu-
4 tions to support efficient and effective systems
5 for classification and declassification to be im-
6 plemented on an interoperable and federated
7 basis across the Federal Government;

8 (B) designate a Federal official—

9 (i) to establish policies and guidance
10 relating to classification and declassifica-
11 tion and controlled unclassified information
12 across the Federal Government;

13 (ii) to conduct oversight of the imple-
14 mentation of such policies and guidance;
15 and

16 (iii) who may, at the discretion of the
17 President, also serve as Executive Agent;
18 and

19 (C) establish an Executive Committee on
20 Classification and Declassification Programs
21 and Technology to provide direction, advice,
22 and guidance to the Executive Agent.

23 (2) EXECUTIVE COMMITTEE.—

1 (A) COMPOSITION.—The Executive Com-
2 mittee shall be composed of the following or
3 their designees:

4 (i) The Director of National Intel-
5 ligence.

6 (ii) The Under Secretary of Defense
7 for Intelligence and Security.

8 (iii) The Secretary of Energy.

9 (iv) The Secretary of State.

10 (v) The Director of the Office of Man-
11 agement and Budget.

12 (vi) The Archivist of the United
13 States.

14 (vii) The Federal official designated
15 under subsection (b)(1)(B) if such official
16 is not also the Executive Agent.

17 (viii) Such other members as the Ex-
18 ecutive Agent considers appropriate.

19 (B) CHAIRPERSON.—The Executive Agent
20 shall be the chairperson of the Executive Com-
21 mittee.

22 (c) REPORT TO CONGRESS.—

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

1 President shall submit to Congress a report on the
2 administration of this section.

3 (2) CONTENTS.—The report submitted pursu-
4 ant to paragraph (1) shall include the following:

5 (A) Funding, personnel, expertise, and re-
6 sources required for the Executive Agent and a
7 description of how such funding, personnel, ex-
8 pertise, and resources will be provided.

9 (B) Authorities needed by the Executive
10 Agent, a description of how such authorities
11 will be granted, and a description of any addi-
12 tional statutory authorities required.

13 (C) Funding, personnel, expertise, and re-
14 sources required by the Federal official des-
15 ignated under subsection (b)(1)(B) and a de-
16 scription of how such funding, personnel, exper-
17 tise, and resources will be provided.

18 (D) Authorities needed by the Federal offi-
19 cial designated under subsection (b)(1)(B), a
20 description of how such authorities will be pro-
21 vided, and a description of any additional statu-
22 tory authorities required.

23 (E) Funding and resources required by the
24 Public Interest Declassification Board.

25 (d) PUBLIC REPORTING.—

1 (1) IN GENERAL.—The report required by sub-
2 section (c) shall be made available to the public to
3 the greatest extent possible consistent with the pro-
4 tection of sources and methods.

5 (2) PUBLICATION IN FEDERAL REGISTER.—The
6 President shall publish in the Federal Register the
7 roles and responsibilities of the Federal officials des-
8 ignated under subsection (b), the Executive Com-
9 mittee, and any subordinate individuals or entities.

10 **SEC. 602. CLASSIFICATION AND DECLASSIFICATION OF IN-**
11 **FORMATION.**

12 (a) IN GENERAL.—Title VIII of the National Secu-
13 rity Act of 1947 (50 U.S.C. 3161 et seq.) is amended by
14 inserting after section 801 the following:

15 **“SEC. 801A. CLASSIFICATION AND DECLASSIFICATION OF**
16 **INFORMATION.**

17 “(a) IN GENERAL.—The President may, in accord-
18 ance with this section, protect from unauthorized dislo-
19 sure any information owned by, produced by or for, or
20 under the control of the executive branch of the Federal
21 Government when there is a demonstrable need to do so
22 to protect the national security of the United States.

23 “(b) ESTABLISHMENT OF STANDARDS, CATEGORIES,
24 AND PROCEDURES FOR CLASSIFICATION AND DECLAS-
25 SIFICATION.—

1 “(1) GOVERNMENTWIDE PROCEDURES.—

2 “(A) CLASSIFICATION.—The President
3 shall, to the extent necessary, establish cat-
4 egories of information that may be classified
5 and procedures for classifying information
6 under subsection (a).

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

12 “(C) MINIMUM REQUIREMENTS.—The pro-
13 cedures established pursuant to subparagraphs
14 (A) and (B) shall—

15 “(i) be the exclusive means for
16 classifying information on or after the ef-
17 fective date established by subsection (c),
18 except with respect to information classi-
19 fied pursuant to the Atomic Energy Act of
20 1954 (42 U.S.C. 2011 et seq.);

21 “(ii) ensure that no information is
22 classified unless there is a demonstrable
23 need to do so to protect the national secu-
24 rity and there is a reasonable basis to be-

1 lieve that means other than classification
2 will not provide sufficient protection;

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

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

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

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

13 “(III) to restrain competition; or

14 “(IV) to prevent or delay the re-
15 lease of information that does not re-
16 quire protection in the interest of the
17 national security;

18 “(v) ensure that basic scientific re-
19 search information not clearly related to
20 the national security shall not be classified;

21 “(vi) ensure that information may not
22 be reclassified after being declassified and
23 released to the public under proper author-
24 ity unless personally approved by the
25 President based on a determination that

1 such reclassification is required to prevent
2 significant and demonstrable damage to
3 the national security;

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

6 “(viii) establish standards, criteria,
7 and timelines for the declassification of in-
8 formation classified under this section;

9 “(ix) provide for the automatic declas-
10 sification of classified records with perma-
11 nent historical value not more than 50
12 years after the date of origin of such
13 records, unless the head of each agency
14 that classified information contained in
15 such records makes a written determina-
16 tion to delay automatic declassification and
17 such determination is reviewed not less fre-
18 quently than every 10 years;

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

21 “(xi) ensure that due regard is given
22 for the public interest in disclosure of in-
23 formation;

24 “(xii) ensure that due regard is given
25 for the interests of departments and agen-

1 cies in sharing information at the lowest
2 possible level of classification;

3 “(D) SUBMITTAL TO CONGRESS.—The
4 President shall submit to Congress the cat-
5 egories and procedures established under sub-
6 section (b)(1)(A) and the procedures established
7 under subsection (b)(1)(B) at least 60 days
8 prior to their effective date.

9 “(2) AGENCY STANDARDS AND PROCEDURES.—

10 “(A) IN GENERAL.—The head of each
11 agency shall establish a single set of consoli-
12 dated standards and procedures to permit such
13 agency to classify and declassify information
14 created by such agency in accordance with the
15 categories and procedures established by the
16 President under this section and otherwise to
17 carry out this section.

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

22 “(c) EFFECTIVE DATE.—

23 “(1) IN GENERAL.—Subsections (a) and (b)
24 shall take effect on the date that is 180 days after

1 the date of the enactment of the Intelligence Author-
 2 ization Act for Fiscal Year 2025.

3 “(2) RELATION TO PRESIDENTIAL DIREC-
 4 TIVES.—Presidential directives regarding classifying,
 5 safeguarding, and declassifying national security in-
 6 formation, including Executive Order 13526 (50
 7 U.S.C. 3161 note; relating to classified national se-
 8 curity information), in effect on the day before the
 9 date of the enactment of this Act, as well as proce-
 10 dures issued pursuant to such Presidential direc-
 11 tives, shall remain in effect until superseded by proce-
 12 dures issued pursuant to subsection (b).”.

13 (b) CONFORMING AMENDMENT.—Section 805(2) of
 14 such Act (50 U.S.C. 3164(2)) is amended by inserting
 15 “section 801A,” before “Executive Order”.

16 (c) CLERICAL AMENDMENT.—The table of contents
 17 preceding section 2 of such Act is amended by inserting
 18 after the item relating to section 801 the following new
 19 item:

“Sec. 801A. Classification and declassification of information.”.

20 **SEC. 603. MINIMUM STANDARDS FOR EXECUTIVE AGENCY**
 21 **INSIDER THREAT PROGRAMS.**

22 (a) DEFINITIONS.—In this section:

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) CLASSIFIED INFORMATION.—The term
6 “classified information” means information that has
7 been determined to require protection from unau-
8 thorized disclosure pursuant to Executive Order
9 13526 (50 U.S.C. 3161 note; relating to classified
10 national security information), or predecessor or suc-
11 cessor order, to protect the national security of the
12 United States.

13 (b) ESTABLISHMENT OF INSIDER THREAT PRO-
14 GRAMS.—Each head of an agency with access to classified
15 information shall establish an insider threat program to
16 protect classified information from unauthorized disclo-
17 sure.

18 (c) MINIMUM STANDARDS.—In carrying out an in-
19 sider threat program established by the head of an agency
20 pursuant to subsection (b), the head of the agency shall—

- 21 (1) designate a senior official of the agency who
22 shall be responsible for management of the program;
23 (2) monitor user activity on all classified net-
24 works to detect activity indicative of insider threat
25 behavior;

1 (3) build and maintain an insider threat ana-
 2 lytic and response capability to review, assess, and
 3 respond to information obtained pursuant to para-
 4 graph (2); and

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

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

16 **TITLE VII—SECURITY CLEAR-** 17 **ANCES AND INTELLIGENCE** 18 **COMMUNITY WORKFORCE IM-** 19 **PROVEMENTS**

20 **SEC. 701. SECURITY CLEARANCES HELD BY CERTAIN** 21 **FORMER EMPLOYEES OF INTELLIGENCE** 22 **COMMUNITY.**

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

1 (1) in paragraph (3), by striking “; and” and
2 inserting a semicolon;

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

5 (3) by adding at the end the following:

6 “(5) issue guidelines and instructions to the
7 heads of Federal agencies to ensure that any indi-
8 vidual who was appointed by the President to a posi-
9 tion in an element of the intelligence community but
10 is no longer employed by the Federal Government
11 shall maintain a security clearance only in accord-
12 ance with Executive Order 12968 (50 U.S.C. 3161
13 note; relating to access to classified information), or
14 successor order.”.

15 (b) SUBMITTAL OF GUIDELINES AND INSTRUCTIONS
16 TO CONGRESS REQUIRED.—Not later than 180 days after
17 the date of the enactment of this Act, the Director of Na-
18 tional Intelligence shall, in the Director’s capacity as the
19 Security Executive Agent pursuant to subsection (a) of
20 section 803 of the National Security Act of 1947 (50
21 U.S.C. 3162a), submit to the congressional intelligence
22 committees and the congressional defense committees (as
23 defined in section 101(a) of title 10, United States Code)
24 the guidelines and instructions required by subsection

1 (c)(5) of such Act, as added by subsection (a) of this sec-
2 tion.

3 (c) ANNUAL REPORT REQUIRED.—

4 (1) IN GENERAL.—Not later than 1 year after
5 the date of the enactment of this Act, and not less
6 frequently than once each year thereafter, the Direc-
7 tor of National Intelligence shall, in the Director's
8 capacity as the Security Executive Agent pursuant
9 to section 803(a) of the National Security Act of
10 1947 (50 U.S.C. 3162a(a)), submit to the congres-
11 sional intelligence committees and the congressional
12 defense committees (as defined in section 101(a) of
13 title 10, United States Code) an annual report on
14 the eligibility status of former senior employees of
15 the intelligence community to access classified infor-
16 mation.

17 (2) CONTENTS.—Each report submitted pursu-
18 ant to paragraph (1) shall include, for the period
19 covered by the report, the following:

20 (A) A list of individuals who were ap-
21 pointed by the President to a position in an ele-
22 ment of the intelligence community who cur-
23 rently hold security clearances.

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

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

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

5 (ii) the years of service in such posi-
6 tion; and

7 (iii) the individual's current employ-
8 ment position and employer.

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

12 **SEC. 702. POLICY FOR AUTHORIZING INTELLIGENCE COM-**
13 **MUNITY PROGRAM OF CONTRACTOR-OWNED**
14 **AND CONTRACTOR-OPERATED SENSITIVE**
15 **COMPARTMENTED INFORMATION FACILI-**
16 **TIES.**

17 (a) **POLICY.**—The Director of National Intelligence
18 shall establish a standardized policy for the intelligence
19 community that authorizes a program of contractor-owned
20 and contractor-operated sensitive compartmented informa-
21 tion facilities as a service to the national security and in-
22 telligence enterprises.

23 (b) **REQUIREMENTS.**—The policy established pursu-
24 ant to subsection (a) shall—

1 (1) authorize the head of an element of the in-
2 telligence community to approve and accredit con-
3 tractor-owned and contractor-operated sensitive com-
4 partmented information facilities; and

5 (2) designate an element of the intelligence
6 community as a service of common concern (as de-
7 fined in Intelligence Community Directive 122, or
8 successor directive) to serve as an accrediting au-
9 thority on behalf of other elements of the intelligence
10 community for contractor-owned and contractor-op-
11 erated sensitive compartmented information facili-
12 ties.

13 (c) COST CONSIDERATIONS.—In establishing the pol-
14 icy required by subsection (a), the Director shall consider
15 existing demonstrated models where a contractor acquires,
16 outfits, and manages a facility pursuant to an agreement
17 with the Federal Government such that no funding from
18 the Federal Government is required to carry out the agree-
19 ment.

20 (d) BRIEFING REQUIRED.—Not later than 1 year
21 after the date on which the Director establishes the policy
22 pursuant to subsection (a), the Director shall brief the
23 congressional intelligence committees on—

24 (1) additional opportunities to leverage con-
25 tractor-provided secure facility space; and

1 (2) recommendations to address barriers, in-
2 cluding resources or authorities needed.

3 **SEC. 703. ENABLING INTELLIGENCE COMMUNITY INTEGRA-**
4 **TION.**

5 (a) IN GENERAL.—The National Security Act of
6 1947 (50 U.S.C. 3001 et seq.) is amended by inserting
7 after section 113B the following new section:

8 **“SEC. 113C. ENABLING INTELLIGENCE COMMUNITY INTE-**
9 **GRATION.**

10 “(a) PROVISION OF GOODS OR SERVICES.—Subject
11 to and in accordance with any guidance and requirements
12 developed by the Director of National Intelligence, the
13 head of an element of the intelligence community may pro-
14 vide goods or services to another element of the intel-
15 ligence community without reimbursement or transfer of
16 funds for hoteling initiatives for intelligence community
17 employees and affiliates defined in any such guidance and
18 requirements issued by the Director of National Intel-
19 ligence.

20 “(b) APPROVAL.—Prior to the provision of goods or
21 services pursuant to subsection (a), the head of the ele-
22 ment of the intelligence community providing such goods
23 or services and the head of the element of the intelligence
24 community receiving such goods or services shall approve
25 such provision.”.

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

“Sec. 113C. Enabling intelligence community integration.”.

4 **SEC. 704. APPOINTMENT OF SPOUSES OF CERTAIN FED-**
 5 **ERAL EMPLOYEES.**

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

8 (1) in the section heading, by striking “**mili-**
 9 **tary and Department of Defense civilian**
 10 **spouses**” and inserting “**military and Depart-**
 11 **ment of Defense, Department of State,**
 12 **and intelligence community spouses**”;

13 (2) in subsection (a)—

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

17 (B) by striking paragraph (5);

18 (C) by redesignating paragraph (4) (relat-
 19 ing to the spouse of a disabled or deceased
 20 member of the Armed Forces) as paragraph
 21 (6);

22 (D) by striking paragraph (3) and insert-
 23 ing the following:

24 “(3) The term ‘covered spouse’ means an indi-
 25 vidual who is married to an individual who—

1 “(A)(i) is an employee of the Department
2 of State or an element of the intelligence com-
3 munity; or

4 “(ii) is a member of the Armed Forces who
5 is assigned to an element of the intelligence
6 community; and

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

12 “(4) The term ‘intelligence community’ has the
13 meaning given the term in section 3 of the National
14 Security Act of 1947 (50 U.S.C. 3003).

15 “(5) The term ‘remote work’ refers to a work
16 flexibility arrangement under which an employee—

17 “(A) is not expected to physically report to
18 the location from which the employee would
19 otherwise work, considering the position of the
20 employee; and

21 “(B) performs the duties and responsibil-
22 ities of such employee’s position, and other au-
23 thorized activities, from an approved worksite—

24 “(i) other than the location from
25 which the employee would otherwise work;

1 “(ii) that may be inside or outside the
2 local commuting area of the location from
3 which the employee would otherwise work;
4 and

5 “(iii) that is typically the residence of
6 the employee.”; and

7 (E) by adding at the end the following:

8 “(8) The term ‘telework’ has the meaning given
9 the term in section 6501.”; and
10 (3) in subsection (b)—

11 (A) in paragraph (2), by striking “or” at
12 the end;

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

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

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

21 (i) by inserting “, including to a posi-
22 tion in which the spouse will engage in re-
23 mote work” after “Department of De-
24 fense”; and

1 (ii) by striking the period at the end
 2 and inserting “; or”; and

3 (E) by adding at the end the following:

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

6 (b) TECHNICAL AND CONFORMING AMENDMENT.—

7 The table of sections for subchapter I of chapter 33 of
 8 title 5, United States Code, is amended by striking the
 9 item relating to section 3330d and inserting the following:

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

10 **SEC. 705. PLAN FOR STAFFING THE INTELLIGENCE COL-**
 11 **LECTION POSITIONS OF THE CENTRAL IN-**
 12 **TELLIGENCE AGENCY.**

13 (a) IN GENERAL.—Not later than 90 days after the
 14 date of the enactment of this Act, the Director of the Cen-
 15 tral Intelligence Agency shall submit to the congressional
 16 intelligence committees a plan for ensuring that the Direc-
 17 torate of Operations of the Agency has staffed every civil-
 18 ian full-time equivalent position authorized for that Direc-
 19 torate under the Intelligence Authorization Act for Fiscal
 20 Year 2024 (division G of Public Law 118–31).

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

1 (1) Specific benchmarks and timelines for ac-
 2 complishing the goal described in such subsection by
 3 September 30, 2025.

4 (2) An assessment of the appropriate balance of
 5 staffing between the Directorate of Operations and
 6 the Directorate of Analysis consistent with the re-
 7 sponsibilities of the Director of the Central Intel-
 8 ligence Agency under section 104A(d) of the Na-
 9 tional Security Act of 1947 (50 U.S.C. 3036(d)).

10 **SEC. 706. INTELLIGENCE COMMUNITY WORKPLACE PRO-**
 11 **TECTIONS.**

12 (a) EMPLOYMENT STATUS.—

13 (1) CONVERSION OF POSITIONS BY DIRECTOR
 14 OF NATIONAL INTELLIGENCE TO EXCEPTED SERV-
 15 ICE.—Section 102A(v) of the National Security Act
 16 of 1947 (50 U.S.C. 3024(v)) is amended—

17 (A) by redesignating paragraphs (2)
 18 through (4) as paragraphs (3) through (5), re-
 19 spectively;

20 (B) by inserting after paragraph (1) the
 21 following:

22 “(2) The Director shall promptly notify the congres-
 23 sional intelligence committees of any action taken pursu-
 24 ant to paragraph (1).”; and

1 (C) in paragraph (3), as redesignated by
 2 subparagraph (A), by striking “occupying a po-
 3 sition on the date of the enactment of the Intel-
 4 ligence Authorization Act for Fiscal Year
 5 2012”.

6 (2) CONVERSION OF DEFENSE INTELLIGENCE
 7 POSITIONS TO EXCEPTED SERVICE.—Section
 8 1601(a) of title 10, United States Code, is amend-
 9 ed—

10 (A) by redesignating subsection (b) as sub-
 11 section (d); and

12 (B) by inserting after subsection (a) the
 13 following:

14 “(b) CONGRESSIONAL NOTIFICATION.—The Sec-
 15 retary shall promptly notify the congressional defense
 16 committees and the congressional intelligence committees
 17 (as defined in section 3 of the National Security Act of
 18 1947 (50 U.S.C. 3003)) of any action taken pursuant to
 19 subsection (a).

20 “(c) RETENTION OF ACCRUED RIGHTS UPON CON-
 21 VERSION.—An incumbent whose position is selected to be
 22 converted, without regard to the wishes of the incumbent,
 23 to the excepted service under subsection (a) shall remain
 24 in the competitive service for the purposes of status and
 25 any accrued adverse action protections while the individual

1 occupies that position or any other position to which the
2 employee is moved involuntarily. Once such individual no
3 longer occupies the converted position, the position may
4 be treated as a regularly excepted service position.”.

5 (3) CONVERSION WITHIN THE EXCEPTED SERV-
6 ICE.—An intelligence community incumbent em-
7 ployee whose position is selected to be converted
8 from one excepted service schedule to another sched-
9 ule within the excepted service without regard to the
10 wishes of the incumbent shall remain in the current
11 schedule for the purpose of status and any accrued
12 adverse action protections while the individual occu-
13 pies that position or any other position to which the
14 employee is moved without regard to the wishes of
15 the employee.

16 (b) CONGRESSIONAL NOTIFICATION OF GUIDE-
17 LINES.—

18 (1) SUBMITTAL TO CONGRESS.—Not later than
19 30 days after the date of the enactment of this Act,
20 each head of an element of the intelligence commu-
21 nity shall submit to the congressional intelligence
22 committees the guidelines and regulations of the ele-
23 ment relating to employment status and protections
24 relating to that status.

1 (2) NOTICE OF CHANGES.—In any case in
2 which a guideline or regulation of an element of the
3 intelligence community submitted pursuant to para-
4 graph (1) is modified or replaced, the head of the
5 element shall promptly notify the congressional intel-
6 ligence committees of the change and submit the
7 new or modified guideline or regulation.

8 (c) TERMINATION AUTHORITIES OF THE DIRECTOR
9 OF THE CIA.—

10 (1) PROCESS AND NOTIFICATION.—Section
11 104A(e) of the National Security Act of 1947 (50
12 U.S.C. 3036(e)) is amended—

13 (A) by redesignating paragraph (2) as
14 paragraph (3); and

15 (B) by inserting after paragraph (1) the
16 following:

17 “(2)(A) Subject to subparagraph (B), the Director
18 shall not take an action under paragraph (1) to terminate
19 the employment of an officer or employee, except in ac-
20 cordance with guidelines and regulations submitted to the
21 congressional intelligence committees.

22 “(B) The Director may take an action under para-
23 graph (1) without or in contravention of the guidelines
24 and regulations specified in subparagraph (A) of this
25 paragraph if the Director determines that complying with

1 such guidelines and regulations poses a threat to the na-
2 tional security of the United States. If the Director makes
3 such a determination, the Director shall provide prompt
4 notification to the congressional intelligence committees
5 that includes—

6 “(i) an explanation for the basis for the termi-
7 nation and the factual support for such determina-
8 tion; and

9 “(ii) an explanation for the determination that
10 the process described in subparagraph (A) poses a
11 threat to the national security of the United
12 States.”.

13 (d) IMPROVEMENT OF CONGRESSIONAL NOTICE RE-
14 QUIREMENT RELATING TO TERMINATION OF DEFENSE
15 INTELLIGENCE EMPLOYEES.—Section 1609(c) of title 10,
16 United States Code, is amended by adding at the end the
17 following: “Such notification shall include the following:

18 “(1) An explanation for the determination that
19 the termination was in the interests of the United
20 States.

21 “(2) An explanation for the determination that
22 the procedures prescribed in other provisions of law
23 that authorize the termination of the employment of
24 such employee cannot be invoked in a manner con-

1 sistent with the national security of the United
2 States.”.

3 (e) CONGRESSIONAL NOTIFICATION OF OTHER SUS-
4 PENSION AND REMOVAL AUTHORITIES.—Section 7532 of
5 title 5, United States Code, is amended by adding at the
6 end the following:

7 “(d)(1) The head of an element of the intelligence
8 community who takes an action under this section shall
9 promptly notify the congressional intelligence committees
10 of such action.

11 “(2) Each notification under paragraph (1) regarding
12 an action shall include the following:

13 “(A) An explanation for the determination that
14 the action is necessary or advisable in the interests
15 of national security.

16 “(B) If the head of an element of the intel-
17 ligence community determines, pursuant to sub-
18 section (a), that the interests of national security do
19 not permit notification to the employee of the rea-
20 sons for the action under that subsection, an expla-
21 nation for such determination.

22 “(3) In this subsection, the terms ‘congressional in-
23 telligence committees’ and ‘intelligence community’ have
24 the meanings given such terms in section 3 of the National
25 Security Act of 1947 (50 U.S.C. 3003).”.

1 (f) SAVINGS CLAUSE.—Nothing in this section shall
2 be construed to diminish the rights conferred by chapter
3 75 of title 5, United States Code, or other applicable agen-
4 cy adverse action or disciplinary procedures.

5 **SEC. 707. SENSE OF CONGRESS ON GOVERNMENT PER-**
6 **SONNEL SUPPORT FOR FOREIGN TERRORIST**
7 **ORGANIZATIONS.**

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

15 (1) Espousing the actions of an organization
16 designated as a foreign terrorist organization under
17 section 219 of the Immigration and Nationality Act
18 (8 U.S.C. 1189).

19 (2) Advocating for continued attacks by an or-
20 ganization described in paragraph (1).

21 (3) Soliciting funds for an organization de-
22 scribed in paragraph (1).

1 **TITLE VIII—WHISTLEBLOWERS**

2 **SEC. 801. IMPROVEMENTS REGARDING URGENT CONCERNS**

3 **SUBMITTED TO INSPECTORS GENERAL OF**

4 **THE INTELLIGENCE COMMUNITY.**

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

8 (1) in subparagraph (A)—

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

11 (B) by inserting “in writing” before “to
12 the Inspector General”; and

13 (C) by adding at the end the following:

14 “(ii) The Inspector General shall provide any support
15 necessary to ensure that an employee can submit a com-
16 plaint or information under this subparagraph in writing
17 and, if such submission is not feasible, shall create a writ-
18 ten record of the employee’s verbal complaint or informa-
19 tion and treat such written record as a written submis-
20 sion.”;

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

23 “(B)(i)(I) Not later than the end of the period speci-
24 fied in subclause (II), the Inspector General shall deter-
25 mine whether the written complaint or information sub-

mitted under subparagraph (A) appears credible. Upon making such a determination, the Inspector General shall transmit to the Director notice of that determination, together with the complaint or information.

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

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

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

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

1 (3) in subparagraph (D)—

2 (A) in clause (i), by striking “or does not
3 transmit the complaint or information to the
4 Director in accurate form under subparagraph
5 (B),” and inserting “does not transmit the
6 complaint or information to the Director in ac-
7 curate form under subparagraph (B)(i)(I), or
8 makes a determination pursuant to subpara-
9 graph (B)(ii)(I) but does not transmit the com-
10 plaint or information to the congressional intel-
11 ligence committees within 21 calendar days of
12 receipt,”; and

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

15 “(ii) An employee may contact the congres-
16 sional intelligence committees directly as described
17 in clause (i) only if—

18 “(I) the employee, before making such a
19 contact—

20 “(aa) transmits to the Director,
21 through the Inspector General, a statement
22 of the employee’s complaint or information
23 and notice of the employee’s intent to con-
24 tact the congressional intelligence commit-
25 tees directly; and

1 “(bb) obtains and follows from the Di-
 2 rector, through the Inspector General, di-
 3 rection on how to contact the congressional
 4 intelligence committees in accordance with
 5 appropriate security practices; or

6 “(II) the Inspector General—

7 “(aa) determines that—

8 “(AA) a transmittal under sub-
 9 clause (I) could compromise the ano-
 10 nymity of the employee or result in
 11 the complaint or information being
 12 transmitted to a subject of the com-
 13 plaint or information; or

14 “(BB) the Director has failed to
 15 provide adequate direction pursuant
 16 to item (bb) of subclause (I) within 7
 17 calendar days of a transmittal under
 18 such subclause; and

19 “(bb) provides the employee direction
 20 on how to contact the congressional intel-
 21 ligence committees in accordance with ap-
 22 propriate security practices.”; and

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

24 “(J) In this paragraph, the term ‘employee’, with re-
 25 spect to an employee of an element of the intelligence com-

1 munity, an employee assigned or detailed to an element
 2 of the intelligence community, or an employee of a con-
 3 tractor to the intelligence community who may submit a
 4 complaint or information to the Inspector General under
 5 subparagraph (A), means—

6 “(i) a current employee at the time of such sub-
 7 mission; or

8 “(ii) a former employee at the time of such sub-
 9 mission, if such complaint or information arises
 10 from and relates to the period of employment as
 11 such an employee.”.

12 (b) INSPECTOR GENERAL OF THE CENTRAL INTEL-
 13 LIGENCE AGENCY.—Section 17(d)(5) of the Central Intel-
 14 ligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)) is
 15 amended—

16 (1) in subparagraph (A)—

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

18 (B) by inserting “in writing” before “to
 19 the Inspector General”; and

20 (C) by adding at the end the following:

21 “(ii) The Inspector General shall provide any support
 22 necessary to ensure that an employee can submit a com-
 23 plaint or information under this subparagraph in writing
 24 and, if such submission is not feasible, shall create a writ-
 25 ten record of the employee’s verbal complaint or informa-

1 tion and treat such written record as a written submis-
2 sion.”;

3 (2) in subparagraph (B)—

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

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

13 “(II) The period specified in this subclause is the 14-
14 calendar-day period beginning on the date on which an
15 employee who has submitted an initial written complaint
16 or information under subparagraph (A) confirms that the
17 employee has submitted to the Inspector General the ma-
18 terial the employee intends to submit to Congress under
19 such subparagraph.”; and

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

21 “(iii) The Inspector General may transmit a com-
22 plaint or information submitted under subparagraph (A)
23 directly to the congressional intelligence committees—

24 “(I) without transmittal to the Director if the
25 Inspector General determines that transmittal to the

1 Director could compromise the anonymity of the em-
2 ployee or result in the complaint or information
3 being transmitted to a subject of the complaint or
4 information;

5 “(II) following transmittal to the Director if the
6 Director does not transmit the complaint or infor-
7 mation to the congressional intelligence committees
8 within the time period specified in subparagraph (C)
9 and has not made a determination regarding a con-
10 flict of interest pursuant to clause (ii); or

11 “(III) following transmittal to the Director and
12 a determination by the Director that a conflict of in-
13 terest exists pursuant to clause (ii) if the Inspector
14 General determines that—

15 “(aa) transmittal to the Director of Na-
16 tional Intelligence could compromise the ano-
17 nymity of the employee or result in the com-
18 plaint or information being transmitted to a
19 subject of the complaint or information; or

20 “(bb) the Director of National Intelligence
21 has not transmitted the complaint or informa-
22 tion to the congressional intelligence committees
23 within the time period specified in subpara-
24 graph (C).”;

25 (3) in subparagraph (D)—

1 (A) in clause (i), by striking “or does not
2 transmit the complaint or information to the
3 Director in accurate form under subparagraph
4 (B),” and inserting “does not transmit the
5 complaint or information to the Director in ac-
6 curate form under subparagraph (B)(i)(I), or
7 makes a determination pursuant to subpara-
8 graph (B)(iii)(I) but does not transmit the com-
9 plaint or information to the congressional intel-
10 ligence committees within 21 calendar days of
11 receipt,”; and

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

14 “(ii) An employee may contact the congressional in-
15 telligence committees directly as described in clause (i)
16 only if—

17 “(I) the employee, before making such a con-
18 tact—

19 “(aa) transmits to the Director, through
20 the Inspector General, a statement of the em-
21 ployee’s complaint or information and notice of
22 the employee’s intent to contact the congres-
23 sional intelligence committees directly; and

24 “(bb) obtains and follows from the Direc-
25 tor, through the Inspector General, direction on

1 how to contact the congressional intelligence
 2 committees in accordance with appropriate se-
 3 curity practices; or

4 “(II) the Inspector General—

5 “(aa) determines that—

6 “(AA) the transmittal under sub-
 7 clause (I) could compromise the anonymity
 8 of the employee or result in the complaint
 9 or information being transmitted to a sub-
 10 ject of the complaint or information; or

11 “(BB) the Director has failed to pro-
 12 vide adequate direction pursuant to item
 13 (bb) of subclause (I) within 7 calendar
 14 days of a transmittal under such sub-
 15 clause; and

16 “(bb) provides the employee direction on
 17 how to contact the congressional intelligence
 18 committees in accordance with appropriate se-
 19 curity practices.”; and

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

21 “(I) In this paragraph, the term ‘employee’, with re-
 22 spect to an employee of the Agency, or of a contractor
 23 to the Agency, who may submit a complaint or information
 24 to the Inspector General under subparagraph (A),
 25 means—

1 “(i) a current employee at the time of such sub-
2 mission; or

3 “(ii) a former employee at the time of such sub-
4 mission, if such complaint or information arises
5 from and relates to the period of employment as
6 such an employee.”.

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

10 (1) in subsection (a)—

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

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

15 “(1) EMPLOYEE.—The term ‘employee’, with
16 respect to an employee of an element of the Federal
17 Government covered by subsection (b), or of a con-
18 tractor to such an element, who may submit a com-
19 plaint or information to an Inspector General under
20 such subsection, means—

21 “(A) a current employee at the time of
22 such submission; or

23 “(B) a former employee at the time of
24 such submission, if such complaint or informa-

tion arises from and relates to the period of employment as such an employee.”;

(2) in subsection (b)—

(A) in paragraph (1)—

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

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

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

(B) by adding at the end the following:

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

(3) in subsection (c)—

1 (A) by striking paragraph (1) and insert-
2 ing the following:

3 “(1) CREDIBILITY.—

4 “(A) DETERMINATION.—Not later than
5 the end of the period specified in subparagraph
6 (B), the Inspector General shall determine
7 whether the written complaint or information
8 submitted under subsection (b) appears cred-
9 ible. Upon making such a determination, the
10 Inspector General shall transmit to the head of
11 the establishment notice of that determination,
12 together with the complaint or information.

13 “(B) PERIOD SPECIFIED.—The period
14 specified in this subparagraph is the 14-cal-
15 endar-day period beginning on the date on
16 which an employee who has submitted an initial
17 written complaint or information under sub-
18 section (b) confirms that the employee has sub-
19 mitted to the Inspector General the material
20 the employee intends to submit to Congress
21 under such subsection.”; and

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

23 “(3) TRANSMITTAL DIRECTLY TO INTEL-
24 LIGENCE COMMITTEES.—The Inspector General may

1 transmit the complaint or information directly to the
2 intelligence committees—

3 “(A) without transmittal to the head of the
4 establishment if the Inspector General deter-
5 mines that transmittal to the head of the estab-
6 lishment could compromise the anonymity of
7 the employee or result in the complaint or infor-
8 mation being transmitted to a subject of the
9 complaint or information;

10 “(B) following transmittal to the head of
11 the establishment if the head of the establish-
12 ment does not transmit the complaint or infor-
13 mation to the intelligence committees within the
14 time period specified in subsection (d) and has
15 not made a determination regarding a conflict
16 of interest pursuant to paragraph (2); or

17 “(C) following transmittal to the head of
18 the establishment and a determination by the
19 head of the establishment that a conflict of in-
20 terest exists pursuant to paragraph (2) if the
21 Inspector General determines that—

22 “(i) transmittal to the Director of Na-
23 tional Intelligence or the Secretary of De-
24 fense could compromise the anonymity of
25 the employee or result in the complaint or

1 information being transmitted to a subject
2 of the complaint or information; or

3 “(ii) the Director of National Intel-
4 ligence or the Secretary of Defense has not
5 transmitted the complaint or information
6 to the intelligence committees within the
7 time period specified in subsection (d).”;

8 (4) in subsection (e)(1), by striking “or does
9 not transmit the complaint or information to the
10 head of the establishment in accurate form under
11 subsection (c),” and inserting “does not transmit the
12 complaint or information to the head of the estab-
13 lishment in accurate form under subsection
14 (c)(1)(A), or makes a determination pursuant to
15 subsection (c)(3)(A) but does not transmit the com-
16 plaint or information to the intelligence committees
17 within 21 calendar days of receipt,”; and

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

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

23 “(A) the employee, before making such a
24 contact—

1 “(i) transmits to the head of the es-
2 tablishment, through the Inspector Gen-
3 eral, a statement of the employee’s com-
4 plaint or information and notice of the em-
5 ployee’s intent to contact the intelligence
6 committees directly; and

7 “(ii) obtains and follows from the
8 head of the establishment, through the In-
9 specter General, direction on how to con-
10 tact the intelligence committees in accord-
11 ance with appropriate security practices; or
12 “(B) the Inspector General—

13 “(i) determines that the transmittal
14 under subparagraph (A) could compromise
15 the anonymity of the employee or result in
16 the complaint or information being trans-
17 mitted to a subject of the complaint or in-
18 formation; or

19 “(ii) determines that the head of the
20 establishment has failed to provide ade-
21 quate direction pursuant to clause (ii) of
22 subparagraph (A) within 7 calendar days
23 of a transmittal under such subparagraph;
24 and

1 “(iii) provides the employee direction
 2 on how to contact the intelligence commit-
 3 tees in accordance with appropriate secu-
 4 rity practices.”.

5 **SEC. 802. PROHIBITION AGAINST DISCLOSURE OF WHIS-**
 6 **TLEBLOWER IDENTITY AS ACT OF REPRISAL.**

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

9 (1) in paragraph (3)—

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

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

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

16 “(J) an unauthorized whistleblower iden-
 17 tity disclosure;”; and

18 (2) by adding at the end the following:

19 “(5) UNAUTHORIZED WHISTLEBLOWER IDEN-
 20 TITY DISCLOSURE.—The term ‘unauthorized whistle-
 21 blower identity disclosure’ means, with respect to an
 22 employee or a contractor employee described in
 23 paragraph (3), a knowing and willful disclosure re-
 24 vealing the identity or other personally identifiable
 25 information of the employee or contractor employee

1 so as to identify the employee or contractor em-
2 ployee as an employee or contractor employee who
3 has made a lawful disclosure described in subsection
4 (b) or (c), but does not include such a knowing and
5 willful disclosure that meets any of the following cri-
6 teria:

7 “(A) Such disclosure was made with the
8 express consent of the employee or contractor
9 employee.

10 “(B) Such disclosure was made during the
11 course of reporting or remedying the subject of
12 the lawful disclosure of the whistleblower
13 through management, legal, or oversight proc-
14 esses, including such processes relating to
15 human resources, equal opportunity, security,
16 or an Inspector General.

17 “(C) An Inspector General with oversight
18 responsibility for the relevant covered intel-
19 ligence community element determines that
20 such disclosure—

21 “(i) was unavoidable under section
22 103H of this Act (50 U.S.C. 3033), sec-
23 tion 17 of the Central Intelligence Agency
24 Act of 1949 (50 U.S.C. 3517), section 407

1 of title 5, United States Code, or section
 2 420(b)(2)(B) of such title;

3 “(ii) was made to an official of the
 4 Department of Justice responsible for de-
 5 termining whether a prosecution should be
 6 undertaken; or

7 “(iii) was required by statute or an
 8 order from a court of competent jurisdic-
 9 tion.”.

10 (b) PRIVATE RIGHT OF ACTION FOR UNLAWFUL DIS-
 11 CLOSURE OF WHISTLEBLOWER IDENTITY.—Subsection
 12 (f) of such section is amended to read as follows:

13 “(f) ENFORCEMENT.—

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

17 “(2) HARMONIZATION WITH OTHER ENFORCE-
 18 MENT.—To the fullest extent possible, the President
 19 shall provide for enforcement of this section in a
 20 manner that is consistent with the enforcement of
 21 section 2302(b)(8) of title 5, United States Code, es-
 22 pecially with respect to policies and procedures used
 23 to adjudicate alleged violations of such section.

24 “(3) PRIVATE RIGHT OF ACTION FOR DISCLO-
 25 SURES OF WHISTLEBLOWER IDENTITY IN VIOLATION

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

20 “(4) REQUIREMENTS.—

21 “(A) REVIEW BY INSPECTOR GENERAL
22 AND BY EXTERNAL REVIEW PANEL.—Before
23 the employee or contractor employee may bring
24 a private action under paragraph (3), the em-

1 employee or contractor employee shall exhaust ad-
 2 ministrative remedies by—

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

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

12 “(B) PERIOD TO BRING ACTION.—The em-
 13 ployee or contractor employee may bring a pri-
 14 vate right of action under paragraph (3) during
 15 the 180-day period beginning on the date on
 16 which the employee or contractor employee is
 17 notified of the final disposition of their claim
 18 under section 1106.”.

19 **SEC. 803. PROTECTION FOR INDIVIDUALS MAKING AU-**
 20 **THORIZED DISCLOSURES TO INSPECTORS**
 21 **GENERAL OF ELEMENTS OF THE INTEL-**
 22 **LIGENCE COMMUNITY.**

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

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

3 (2) by adding at the end the following new sub-
4 paragraph:

5 “(B) An individual may disclose classified infor-
6 mation to the Inspector General in accordance with
7 the applicable security standards and procedures es-
8 tablished under Executive Order 13526 (50 U.S.C.
9 3161 note; relating to classified national security in-
10 formation), section 102A or section 803, chapter 12
11 of the Atomic Energy Act of 1954 (42 U.S.C. 2161
12 et seq.), or any applicable provision of law. Such a
13 disclosure of classified information that is made by
14 an individual who at the time of the disclosure does
15 not hold the appropriate clearance or authority to
16 access such classified information, but that is other-
17 wise made in accordance with such security stand-
18 ards and procedures, shall be treated as an author-
19 ized disclosure and does not violate—

20 “(i) any otherwise applicable nondisclosure
21 agreement;

22 “(ii) any otherwise applicable regulation or
23 order issued under the authority of Executive
24 Order 13526 (50 U.S.C. 3161 note; relating to
25 classified national security information) or

1 chapter 18 of the Atomic Energy Act of 1954
2 (42 U.S.C. 2271 et seq.); or

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

7 (3) in the paragraph enumerator, by striking
8 “(3) ” and inserting “(3)(A)”.

9 (b) INSPECTOR GENERAL OF THE CENTRAL INTEL-
10 LIGENCE AGENCY.—Section 17(e)(3) of the Central Intel-
11 ligence Agency Act of 1949 (50 U.S.C. 3517(e)(3)) is
12 amended—

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

15 (2) by adding at the end the following new sub-
16 paragraph:

17 “(B) An individual may disclose classified infor-
18 mation to the Inspector General in accordance with
19 the applicable security standards and procedures es-
20 tablished under Executive Order 13526 (50 U.S.C.
21 3161 note; relating to classified national security in-
22 formation), section 102A or 803 of the National Se-
23 curity Act of 1947 (50 U.S.C. 3024; 3162a), or
24 chapter 12 of the Atomic Energy Act of 1954 (42
25 U.S.C. 2161 et seq.). Such a disclosure of classified

1 information that is made by an individual who at the
 2 time of the disclosure does not hold the appropriate
 3 clearance or authority to access such classified infor-
 4 mation, but that is otherwise made in accordance
 5 with such security standards and procedures, shall
 6 be treated as an authorized disclosure and does not
 7 violate—

8 “(i) any otherwise applicable nondisclosure
 9 agreement;

10 “(ii) any otherwise applicable regulation or
 11 order issued under the authority of Executive
 12 Order 13526 or chapter 18 of the Atomic En-
 13 ergy Act of 1954 (42 U.S.C. 2271 et seq.); or

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

18 (3) in the paragraph enumerator, by striking
 19 “(3) ” and inserting “(3)(A)”.

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

24 “(i) PROTECTION FOR INDIVIDUALS MAKING AU-
 25 THORIZED DISCLOSURES.—An individual may disclose

1 classified information to an Inspector General of an ele-
2 ment of the intelligence community in accordance with the
3 applicable security standards and procedures established
4 under Executive Order 13526 (50 U.S.C. 3161 note; relat-
5 ing to classified national security information), section
6 102A or 803 of the National Security Act of 1947 (50
7 U.S.C. 3024; 3162a), or chapter 12 of the Atomic Energy
8 Act of 1954 (42 U.S.C. 2161 et seq.). Such a disclosure
9 of classified information that is made by an individual who
10 at the time of the disclosure does not hold the appropriate
11 clearance or authority to access such classified informa-
12 tion, but that is otherwise made in accordance with such
13 security standards and procedures, shall be treated as an
14 authorized disclosure and does not violate—

15 “(1) any otherwise applicable nondisclosure
16 agreement;

17 “(2) any otherwise applicable regulation or
18 order issued under the authority of Executive Order
19 13526 or chapter 18 of the Atomic Energy Act of
20 1954 (42 U.S.C. 2271 et seq.); or

21 “(3) section 798 of title 18, or any other provi-
22 sion of law relating to the unauthorized disclosure of
23 national security information.”.

1 **SEC. 804. CLARIFICATION OF AUTHORITY OF CERTAIN IN-**
2 **SPECTORS GENERAL TO RECEIVE PRO-**
3 **TECTED DISCLOSURES.**

4 Section 1104 of the National Security Act of 1947
5 (50 U.S.C. 3234) is amended—

6 (1) in subsection (b)(1), by inserting “or cov-
7 ered intelligence community element” after “the ap-
8 propriate inspector general of the employing agen-
9 cy”; and

10 (2) in subsection (c)(1)(A), by inserting “or
11 covered intelligence community element” after “the
12 appropriate inspector general of the employing or
13 contracting agency”.

14 **SEC. 805. WHISTLEBLOWER PROTECTIONS RELATING TO**
15 **PSYCHIATRIC TESTING OR EXAMINATION.**

16 (a) **PROHIBITED PERSONNEL PRACTICES.**—Section
17 1104(a)(3) of the National Security Act of 1947 (50
18 U.S.C. 3234(a)(3)) is amended—

19 (1) in subparagraph (I), by striking “; or” and
20 inserting a semicolon;

21 (2) by redesignating subparagraph (J) as sub-
22 paragraph (K); and

23 (3) by inserting after subparagraph (I) the fol-
24 lowing new subparagraph:

25 “(J) a decision to order psychiatric testing
26 or examination; or”.

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

6 **SEC. 806. ESTABLISHING PROCESS PARITY FOR ADVERSE**
 7 **SECURITY CLEARANCE AND ACCESS DETER-**
 8 **MINATIONS.**

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

12 “(C) CONTRIBUTING FACTOR.—

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

23 “(ii) CIRCUMSTANTIAL EVIDENCE.—
 24 An individual under clause (i) may dem-
 25 onstrate that the disclosure was a contrib-

1 uting factor in the adverse security clear-
2 ance or access determination taken against
3 the individual through circumstantial evi-
4 dence, such as evidence that—

5 “(I) the official making the de-
6 termination knew of the disclosure;
7 and

8 “(II) the determination occurred
9 within a period such that a reasonable
10 person could conclude that the disclo-
11 sure was a contributing factor in the
12 determination.

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

1 **SEC. 807. ELIMINATION OF CAP ON COMPENSATORY DAM-**
 2 **AGES FOR RETALIATORY REVOCATION OF SE-**
 3 **CURITY CLEARANCES AND ACCESS DETER-**
 4 **MINATIONS.**

5 Section 3001(j)(4)(B) of the Intelligence Reform and
 6 Terrorism Prevention Act of 2004 (50 U.S.C.
 7 3341(j)(4)(B)) is amended, in the second sentence, by
 8 striking “not to exceed \$300,000”.

9 **TITLE IX—ANOMALOUS HEALTH**
 10 **INCIDENTS**

11 **SEC. 901. ADDITIONAL DISCRETION FOR DIRECTOR OF**
 12 **CENTRAL INTELLIGENCE AGENCY IN PAYING**
 13 **COSTS OF TREATING QUALIFYING INJURIES**
 14 **AND MAKING PAYMENTS FOR QUALIFYING**
 15 **INJURIES TO THE BRAIN.**

16 (a) ADDITIONAL AUTHORITY FOR COVERING COSTS
 17 FOR TREATING QUALIFYING INJURIES UNDER EXTRAOR-
 18 DINARY CIRCUMSTANCES.—Subsection (c) of section 19A
 19 of the Central Intelligence Agency Act of 1949 (50 U.S.C.
 20 3519b) is amended—

21 (1) by striking “The Director may” and insert-
 22 ing the following:

23 “(1) IN GENERAL.—The Director may”; and

24 (2) by adding at the end the following:

25 “(2) EXTRAORDINARY CIRCUMSTANCES.—

26 Under such circumstances as the Director deter-

1 mines extraordinary, the Director may pay the costs
2 of treating a qualifying injury of a covered employee,
3 a covered individual, or a covered dependent or may
4 reimburse a covered employee, a covered individual,
5 or a covered dependent for such costs, that are not
6 otherwise covered by a provision of Federal law, re-
7 gardless of the date of the injury and the location
8 of the employee, individual, or dependent when the
9 injury occurred.”.

10 (b) ADDITIONAL AUTHORITY FOR MAKING PAY-
11 MENTS FOR QUALIFYING INJURIES TO THE BRAIN UNDER
12 EXTRAORDINARY CIRCUMSTANCES.—Subsection (d)(2) of
13 such section is amended—

14 (1) by striking “Notwithstanding” and insert-
15 ing the following:

16 “(A) IN GENERAL.—Notwithstanding”;
17 and

18 (2) by adding at the end the following:

19 “(B) EXTRAORDINARY CIRCUMSTANCES.—
20 Under such circumstances as the Director de-
21 termines extraordinary, the Director may pro-
22 vide payment to a covered employee, a covered
23 individual, or a covered dependent for any
24 qualifying injury to the brain, regardless of the
25 date of the injury and the location of the em-

1 employee, individual, or dependent when the injury
2 occurred.”.

3 (c) CONGRESSIONAL NOTIFICATION.—Such section is
4 amended by adding at the end the following new sub-
5 section:

6 “(e) CONGRESSIONAL NOTIFICATION.—Whenever the
7 Director makes a payment or reimbursement made under
8 subsection (c) or (d)(2), the Director shall, not later than
9 30 days after the date on which the payment or reimburse-
10 ment is made, submit to the congressional intelligence
11 committees (as defined in section 3 of the National Secu-
12 rity Act of 1947 (50 U.S.C. 3003)) a notification of such
13 payment or reimbursement.”.

14 **SEC. 902. ADDITIONAL DISCRETION FOR SECRETARY OF**
15 **STATE AND HEADS OF OTHER FEDERAL**
16 **AGENCIES IN PAYING COSTS OF TREATING**
17 **QUALIFYING INJURIES AND MAKING PAY-**
18 **MENTS FOR QUALIFYING INJURIES TO THE**
19 **BRAIN.**

20 (a) ADDITIONAL AUTHORITY FOR COVERING COSTS
21 FOR TREATING QUALIFYING INJURIES UNDER EXTRAOR-
22 DINARY CIRCUMSTANCES.—Subsection (b) of section 901
23 of division J of the Further Consolidated Appropriations
24 Act, 2020 (22 U.S.C. 2680b) is amended to read as fol-
25 lows:

1 “(b) COSTS FOR TREATING QUALIFYING INJU-
2 RIES.—

3 “(1) IN GENERAL.—The Secretary of State or
4 the head of any other Federal agency may pay or re-
5 imburse the costs relating to diagnosing and treat-
6 ing—

7 “(A) a qualifying injury of a covered em-
8 ployee for such costs, that are not otherwise
9 covered by chapter 81 of title 5, United States
10 Code, or other provision of Federal law; or

11 “(B) a qualifying injury of a covered indi-
12 vidual, or a covered dependent, for such costs
13 that are not otherwise covered by Federal law.

14 “(2) EXTRAORDINARY CIRCUMSTANCES.—
15 Under such circumstances as the Secretary of State
16 or other agency head determines extraordinary, the
17 Secretary or other agency head may pay the costs of
18 treating a qualifying injury of a covered employee, a
19 covered individual, or a covered dependent or may
20 reimburse a covered employee, a covered individual,
21 or a covered dependent for such costs, that are not
22 otherwise covered by a provision of Federal law, re-
23 gardless of the date on which the injury occurred.”.

24 (b) ADDITIONAL AUTHORITY FOR MAKING PAY-
25 MENTS FOR QUALIFYING INJURIES TO THE BRAIN UNDER

1 EXTRAORDINARY CIRCUMSTANCES.—Subsection (i)(2) of
2 such section is amended—

3 (1) by striking “Notwithstanding” and insert-
4 ing the following:

5 “(A) IN GENERAL.—Notwithstanding”;
6 and

7 (2) by adding at the end the following:

8 “(B) EXTRAORDINARY CIRCUMSTANCES.—
9 Under such circumstances as the Secretary of
10 State or other agency head with an employee
11 determines extraordinary, the Secretary or
12 other agency head may provide payment to a
13 covered dependent, a dependent of a former em-
14 ployee, a covered employee, a former employee,
15 and a covered individual for any qualifying in-
16 jury to the brain, regardless of the date on
17 which the injury occurred.”.

18 (c) CHANGES TO DEFINITIONS.—Subsection (e) of
19 such section is amended—

20 (1) in paragraph (1)—

21 (A) in the matter before subparagraph (A),
22 by striking “a employee who, on or after Janu-
23 ary 1, 2016” and inserting “an employee who,
24 on or after September 11, 2001”; and

1 (B) in subparagraph (A), by inserting “, or
2 duty station in the United States” before the
3 semicolon;

4 (2) in paragraph (2)—

5 (A) by striking “January 1, 2016” and in-
6 serting “September 11, 2001”; and

7 (B) by inserting “, or duty station in the
8 United States,” after “pursuant to subsection
9 (f)”;

10 (3) in paragraph (3)—

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

14 (B) in subparagraph (A), by inserting “, or
15 duty station in the United States” before the
16 semicolon; and

17 (4) in paragraph (4)—

18 (A) in subparagraph (A)(i), by inserting “,
19 or duty station in the United States” before the
20 semicolon; and

21 (B) in subparagraph (B)(i), by inserting “,
22 or duty station in the United States” before the
23 semicolon.

24 (d) CLARIFICATION RELATING TO AUTHORITIES OF
25 DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY.—

1 Such section is further amended by adding at the end the
 2 following:

3 “(k) RELATION TO DIRECTOR OF CENTRAL INTEL-
 4 LIGENCE AGENCY.—The authorities and requirements of
 5 this section shall not apply to the Director of the Central
 6 Intelligence Agency.”.

7 **SEC. 903. IMPROVED FUNDING FLEXIBILITY FOR PAY-**
 8 **MENTS MADE BY DEPARTMENT OF STATE**
 9 **FOR QUALIFYING INJURIES TO THE BRAIN.**

10 Section 901(i) of division J of the Further Consoli-
 11 dated Appropriations Act, 2020 (22 U.S.C. 2680b) is
 12 amended by striking paragraph (3) and inserting the fol-
 13 lowing:

14 “(3) FUNDING.—

15 “(A) IN GENERAL.—Payment under para-
 16 graph (2) in a fiscal year may be made using
 17 any funds—

18 “(i) appropriated specifically for pay-
 19 ments under such paragraph; or

20 “(ii) reprogrammed in accordance
 21 with an applicable provision of law.

22 “(B) BUDGET.—For each fiscal year, the
 23 Secretary of State shall include with the budget
 24 justification materials submitted to Congress in
 25 support of the budget of the President for that

1 fiscal year pursuant to section 1105(a) of title
2 31, United States Code, an estimate of the
3 funds required in that fiscal year to make pay-
4 ments under paragraph (2).”.

5 **TITLE X—UNIDENTIFIED**
6 **ANOMALOUS PHENOMENA**

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

10 (a) DEFINITIONS.—In this section, the terms “con-
11 gressional defense committees”, “congressional leader-
12 ship”, and “unidentified anomalous phenomena” have the
13 meanings given such terms in section 1683(n) of the Na-
14 tional Defense Authorization Act for Fiscal Year 2022 (50
15 U.S.C. 3373(n)).

16 (b) REVIEW REQUIRED.—The Comptroller General
17 of the United States shall conduct a review of the All-
18 domain Anomaly Resolution Office (in this section re-
19 ferred to as the “Office”).

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

22 (1) A review of the implementation by the Of-
23 fice of the duties and requirements of the Office
24 under section 1683 of the National Defense Author-
25 ization Act for Fiscal Year 2022 (50 U.S.C. 3373),

1 such as the process for operational unidentified
 2 anomalous phenomena reporting and coordination
 3 with the Department of Defense, the intelligence
 4 community, and other departments and agencies of
 5 the Federal Government and non-Government enti-
 6 ties.

7 (2) A review of such other matters relating to
 8 the activities of the Office that pertain to unidenti-
 9 fied anomalous phenomena as the Comptroller Gen-
 10 eral considers appropriate.

11 (d) REPORT.—Following the review required by sub-
 12 section (b), in a timeframe mutually agreed upon by the
 13 congressional intelligence committees, the congressional
 14 defense committees, congressional leadership, and the
 15 Comptroller General, the Comptroller General shall submit
 16 to such committees and congressional leadership a report
 17 on the findings of the Comptroller General with respect
 18 to the review conducted under subsection (b).

19 **SEC. 1002. SUNSET OF REQUIREMENTS RELATING TO AU-**
 20 **DITS OF UNIDENTIFIED ANOMALOUS PHE-**
 21 **NOMENA HISTORICAL RECORD REPORT.**

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

24 (1) in subsection (b)(2), by inserting “until
 25 April 1, 2025” after “quarterly basis”; and

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

3 **SEC. 1003. FUNDING LIMITATIONS RELATING TO UNIDENTI-**
4 **FIED ANOMALOUS PHENOMENA.**

5 (a) DEFINITIONS.—In this section:

6 (1) APPROPRIATE COMMITTEES OF CON-
7 GRESS.—The term “appropriate committees of Con-
8 gress” means—

9 (A) the Select Committee on Intelligence,
10 the Committee on Armed Services, and the
11 Committee on Appropriations of the Senate;
12 and

13 (B) the Permanent Select Committee on
14 Intelligence, the Committee on Armed Services,
15 and the Committee on Appropriations of the
16 House of Representatives.

17 (2) CONGRESSIONAL LEADERSHIP.—The term
18 “congressional leadership” means—

19 (A) the majority leader of the Senate;

20 (B) the minority leader of the Senate;

21 (C) the Speaker of the House of Rep-
22 resentatives; and

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

1 (3) UNIDENTIFIED ANOMALOUS PHENOMENA.—

2 The term “unidentified anomalous phenomena” has
3 the meaning given such term in section 1683(n) of
4 the National Defense Authorization Act for Fiscal
5 Year 2022 (50 U.S.C. 3373(n)).

6 (b) LIMITATIONS.—None of the funds authorized to
7 be appropriated or otherwise made available by this Act
8 may be obligated or expended in support of any activity
9 involving unidentified anomalous phenomena protected
10 under any form of special access or restricted access limi-
11 tation unless the Director of National Intelligence has pro-
12 vided the details of the activity to the appropriate commit-
13 tees of Congress and congressional leadership, including
14 for any activities described in a report released by the All-
15 domain Anomaly Resolution Office in fiscal year 2024.

16 (c) LIMITATION REGARDING INDEPENDENT RE-
17 SEARCH AND DEVELOPMENT.—Independent research and
18 development funding relating to unidentified anomalous
19 phenomena shall not be allowable as indirect expenses for
20 purposes of contracts covered by such instruction, unless
21 such material and information is made available to the ap-
22 propriate congressional committees and leadership.

1 **TITLE XI—AIR AMERICA**

2 **SEC. 1101. SHORT TITLE.**

3 This title may be cited as the “Air America Act of
4 2024”.

5 **SEC. 1102. FINDINGS.**

6 Congress finds the following:

7 (1) Air America and its affiliated companies, in
8 coordination with the Central Intelligence Agency,
9 provided direct and indirect support to the United
10 States Government from 1950 to 1976.

11 (2) The service and sacrifice of employees of
12 Air America included—

13 (A) suffering a high rate of casualties in
14 the course of service;

15 (B) saving thousands of lives in search and
16 rescue missions for downed United States air-
17 men and in allied refugee evacuations; and

18 (C) serving lengthy periods under chal-
19 lenging circumstances abroad.

20 **SEC. 1103. DEFINITIONS.**

21 In this title:

22 (1) **AFFILIATED COMPANY.**—The term “affili-
23 ated company”, with respect to Air America, in-
24 cludes Air Asia Company Limited, CAT Incor-

1 porated, Civil Air Transport Company Limited, and
2 the Pacific Division of Southern Air Transport.

3 (2) AIR AMERICA.—The term “Air America”
4 means Air America, Incorporated.

5 (3) APPROPRIATE CONGRESSIONAL COMMIT-
6 TEES.—The term “appropriate congressional com-
7 mittees” means—

8 (A) the Committee on Homeland Security
9 and Governmental Affairs, the Select Com-
10 mittee on Intelligence, and the Committee on
11 Appropriations of the Senate; and

12 (B) the Committee on Oversight and Ac-
13 countability, the Permanent Select Committee
14 on Intelligence, and the Committee on Appro-
15 priations of the House of Representatives.

16 (4) CHILD; DEPENDENT; WIDOW; WIDOWER.—
17 The terms “child”, “dependent”, “widow”, and
18 “widower” have the meanings given those terms in
19 section 8341(a) of title 5, United States Code, ex-
20 cept that such section shall be applied by sub-
21 stituting “individual who performed qualifying serv-
22 ice” for “employee or Member”.

23 (5) COVERED DECEDENT.—The term “covered
24 decedent” means an individual who was killed in
25 Southeast Asia while supporting operations of the

1 Central Intelligence Agency during the period begin-
2 ning on January 1, 1950, and ending on December
3 31, 1976, as a United States citizen employee of Air
4 America or an affiliated company.

5 (6) DIRECTOR.—The term “Director” means
6 the Director of the Central Intelligence Agency.

7 (7) QUALIFYING SERVICE.— The term “quali-
8 fying service” means service that—

9 (A) was performed by a United States cit-
10 izen as an employee of Air America or an affili-
11 ated company during the period beginning on
12 January 1, 1950, and ending on December 31,
13 1976; and

14 (B) is documented in—

15 (i) the corporate records of Air Amer-
16 ica or an affiliated company;

17 (ii) records possessed by the United
18 States Government; or

19 (iii) the personal records of a former
20 employee of Air America or an affiliated
21 company that are verified by the United
22 States Government.

23 (8) SURVIVOR.—The term “survivor” means—

24 (A) the widow or widower of—

1 (i) an individual who performed quali-
2 fying service; or

3 (ii) a covered decedent; or

4 (B) an individual who, at any time during
5 or since the period of qualifying service, or on
6 the date of death of a covered decedent, was a
7 dependent or child of—

8 (i) the individual who performed such
9 qualifying service; or

10 (ii) the covered decedent.

11 **SEC. 1104. AWARD AUTHORIZED TO ELIGIBLE PERSONS.**

12 (a) IN GENERAL.—Subject to the limitation in sub-
13 section (d), the Director shall provide an award payment
14 of \$40,000 under this section—

15 (1) to an individual who performed qualifying
16 service for a period greater than or equal to 5 years
17 or to a survivor of such individual; or

18 (2) to the survivor of a covered decedent.

19 (b) REQUIREMENTS.—

20 (1) IN GENERAL.—To be eligible for a payment
21 under this subsection, an individual who performed
22 qualifying service or survivor (as the case may be)
23 must demonstrate to the satisfaction of the Director
24 that the individual whose qualifying service upon

1 which the payment is based meets the criteria of
2 paragraph (1) or (2) of subsection (a).

3 (2) RELIANCE ON RECORDS.—In carrying out
4 this subsection, in addition to any evidence provided
5 by such an individual or survivor, the Director may
6 rely on records possessed by the United States Gov-
7 ernment.

8 (c) ADDITIONAL PAYMENT.—If an individual, or in
9 the case of a survivor, the individual whose qualifying
10 service upon which the payment is based, can demonstrate
11 to the Director that the qualifying service of the individual
12 exceeded 5 years, the Director shall pay to such individual
13 or survivor an additional \$8,000 for each full year in ex-
14 cess of 5 years (and a proportionate amount for a partial
15 year).

16 (d) SURVIVORS.—In the case of an award granted to
17 a survivor under this section, the payment shall be made—

18 (1) to the surviving widow or widower; or

19 (2) if there is no surviving widow or widower,
20 to the surviving dependents or children, in equal
21 shares.

22 **SEC. 1105. FUNDING LIMITATION.**

23 (a) IN GENERAL.—The total amount of awards
24 granted under this title may not exceed \$60,000,000.

1 (b) REQUESTS FOR ADDITIONAL FUNDS.—If, at the
2 determination of the Director, the amount of funds re-
3 quired to satisfy all valid applications for payment under
4 this title exceeds the limitation set forth in subsection (a),
5 the Director shall submit to Congress a request for suffi-
6 cient funds to fulfill all remaining payments.

7 (c) AWARDS TO EMPLOYEES OF INTERMOUNTAIN
8 AVIATION.—The Director may determine, on a case-by-
9 case basis, to award amounts to individuals who performed
10 service consistent with the definition of qualifying service
11 as employees of Intermountain Aviation.

12 **SEC. 1106. TIME LIMITATION.**

13 (a) IN GENERAL.—To be eligible for an award pay-
14 ment under this title, a claimant must file a claim for such
15 payment with the Director not later than 2 years after
16 the effective date of the regulations prescribed by the Di-
17 rector in accordance with section 1107.

18 (b) DETERMINATION.—Not later than 90 days after
19 receiving a claim for an award payment under this section,
20 the Director shall determine the eligibility of the claimant
21 for payment.

22 (c) PAYMENT.—

23 (1) IN GENERAL.—If the Director determines
24 that the claimant is eligible for the award payment,

1 the Director shall pay the award payment not later
2 than 60 days after the date of such determination.

3 (2) LUMP-SUM PAYMENT.—The Director shall
4 issue each payment as a one-time lump sum pay-
5 ment contingent upon the timely filing of the claim-
6 ant under this section.

7 (3) NOTICE AND DELAYS.—The Director shall
8 notify the appropriate congressional committees of
9 any delays in making an award payment not later
10 than 30 days after the date such payment is due.

11 **SEC. 1107. APPLICATION PROCEDURES.**

12 (a) IN GENERAL.—The Director shall prescribe pro-
13 cedures to carry out this title, which shall include proc-
14 esses under which—

15 (1) claimants may submit claims for payment
16 under this title;

17 (2) the Director will award the amounts under
18 section 1104; and

19 (3) claimants can obtain redress and appeal de-
20 terminations under section 1106.

21 (b) OTHER MATTERS.—Such procedures—

22 (1) shall be—

23 (A) prescribed not later than 60 days after
24 the date of the enactment of this Act; and

1 (B) published in the Code of Federal Reg-
2 ulations; and

3 (2) shall not be subject to chapter 5 of title 5,
4 United States Code.

5 **SEC. 1108. RULE OF CONSTRUCTION.**

6 Nothing in this title shall be construed to—

7 (1) entitle any person to Federal benefits, in-
8 cluding retirement benefits under chapter 83 or 84
9 of title 5, United States Code, and disability or
10 death benefits under chapter 81 of such title;

11 (2) change the legal status of the former Air
12 America corporation or any affiliated company; or

13 (3) create any legal rights, benefits, or entitle-
14 ments beyond the one-time award authorized by this
15 title.

16 **SEC. 1109. ATTORNEYS' AND AGENTS' FEES.**

17 (a) IN GENERAL.—It shall be unlawful for more than
18 25 percent of an award paid pursuant to this title to be
19 paid to, or received by, any agent or attorney for any serv-
20 ice rendered to a person who receives an award under sec-
21 tion 1104, in connection with the award under this title.

22 (b) VIOLATION.—Any agent or attorney who violates
23 subsection (a) shall be fined under title 18, United States
24 Code.

1 **SEC. 1110. NO JUDICIAL REVIEW.**

2 A determination by the Director pursuant to this title
3 is final and conclusive and shall not be subject to judicial
4 review.

5 **SEC. 1111. REPORTS TO CONGRESS.**

6 Until the date that all funds available for awards
7 under this title are expended, the Director shall submit
8 to the appropriate congressional committees a semiannual
9 report describing the number of award payments made
10 and denied during the 180 days preceding the submission
11 of the report, including the rationales for any denials, and
12 if, at the determination of the Director, the amount of
13 funds provided to carry out this title is insufficient to sat-
14 isfy any remaining or anticipated claims.

15 **TITLE XII—OTHER MATTERS**

16 **SEC. 1201. ENHANCED AUTHORITIES FOR AMICUS CURIAE**

17 **UNDER THE FOREIGN INTELLIGENCE SUR-**
18 **VEILLANCE ACT OF 1978.**

19 (a) EXPANSION OF APPOINTMENT AUTHORITY.—

20 (1) IN GENERAL.—Section 103(i)(2)(A) of the
21 Foreign Intelligence Surveillance Act of 1978 (50
22 U.S.C. 1803(i)(2)(A)) is amended by striking clause
23 (i) and inserting the following:

24 “(i) shall appoint one or more individ-
25 uals who have been designated under para-
26 graph (1), not less than one of whom pos-

1 sesses privacy and civil liberties expertise,
2 unless the court finds that such a quali-
3 fication is inappropriate, to serve as ami-
4 cus curiae to assist the court in the consid-
5 eration of any application or motion for an
6 order or review that, in the opinion of the
7 court—

8 “(I) presents a novel or signifi-
9 cant interpretation of the law, unless
10 the court issues a finding that such
11 appointment is not appropriate;

12 “(II) presents exceptional con-
13 cerns with respect to the activities of
14 a United States person that are pro-
15 tected by the first amendment to the
16 Constitution of the United States, un-
17 less the court issues a finding that
18 such appointment is not appropriate;

19 “(III) targets a United States
20 person and presents or involves a sen-
21 sitive investigative matter, unless—

22 “(aa) the matter represents
23 an immediate danger to human
24 life; or

1 “(bb) the court issues a
2 finding that such appointment is
3 not appropriate;

4 “(IV) targets a United States
5 person and presents a request for ap-
6 proval of programmatic surveillance or
7 reauthorization of programmatic sur-
8 veillance, unless the court issues a
9 finding that such appointment is not
10 appropriate; or

11 “(V) targets a United States per-
12 son and otherwise presents novel or
13 exceptional civil liberties issues, unless
14 the court issues a finding that such
15 appointment is not appropriate;”.

16 (2) DEFINITION OF SENSITIVE INVESTIGATIVE
17 MATTER.—Subsection (i) of section 103 of such Act
18 (50 U.S.C. 1803) is amended by adding at the end
19 the following:

20 “(12) DEFINITION OF SENSITIVE INVESTIGA-
21 TIVE MATTER.—In this subsection, the term ‘sen-
22 sitive investigative matter’ means—

23 “(A) an investigative matter that targets a
24 United States person who is—

25 “(i) a United States elected official;

1 “(ii) an appointee of—

2 “(I) the President; or

3 “(II) a State Governor;

4 “(iii) a United States political can-
5 didate;

6 “(iv) a United States political organi-
7 zation or an individual prominent in such
8 an organization;

9 “(v) a United States news media or-
10 ganization or a member of a United States
11 news media organization; or

12 “(vi) a United States religious organi-
13 zation or an individual prominent in such
14 an organization; or

15 “(B) any other investigative matter involv-
16 ing a domestic entity or a known or presumed
17 United States person that, in the judgment of
18 the applicable court established under sub-
19 section (a) or (b), is as sensitive as an inves-
20 tigative matter described in subparagraph
21 (A).”.

22 (b) AUTHORITY TO SEEK REVIEW.—Subsection (i)
23 of such section (50 U.S.C. 1803), as amended by sub-
24 section (a) of this section, is further amended—

25 (1) in paragraph (4)—

1 (A) in the paragraph heading, by inserting
2 “; AUTHORITY” after “DUTIES”;

3 (B) by striking “the amicus curiae shall”
4 and all that follows through “provide” and in-
5 sert the following: “the amicus curiae—

6 “(A) shall provide”;

7 (C) in subparagraph (A), as so des-
8 ignated—

9 (i) in clause (i), by inserting before
10 the semicolon at the end the following: “,
11 including legal arguments regarding any
12 privacy or civil liberties interest of any
13 United States person that would be signifi-
14 cantly impacted by the application or mo-
15 tion”; and

16 (ii) in clause (iii), by striking the pe-
17 riod at the end and inserting “; and”; and

18 (D) by adding at the end the following:

19 “(B) may seek leave to raise any novel or
20 significant privacy or civil liberties issue rel-
21 evant to the application or motion or other
22 issue directly impacting the legality of the pro-
23 posed electronic surveillance with the court, re-
24 gardless of whether the court has requested as-
25 sistance on that issue.”;

1 (2) by redesignating paragraphs (7) through
2 (12) as paragraphs (8) through (13), respectively;
3 and

4 (3) by inserting after paragraph (6) the fol-
5 lowing:

6 “(7) AUTHORITY TO SEEK REVIEW OF DECI-
7 SIONS.—

8 “(A) FISA COURT DECISIONS.—Following
9 issuance of a final order under this Act by the
10 Foreign Intelligence Surveillance Court in a
11 matter in which an amicus curiae was ap-
12 pointed under paragraph (2), that amicus cu-
13 riae may petition the Foreign Intelligence Sur-
14 veillance Court to certify for review to the For-
15 eign Intelligence Surveillance Court of Review a
16 question of law pursuant to subsection (j). If
17 the court denies such petition, the court shall
18 provide for the record a written statement of
19 the reasons for such denial. Upon certification
20 of any question of law pursuant to this sub-
21 paragraph, the Court of Review shall appoint
22 the amicus curiae to assist the Court of Review
23 in its consideration of the certified question, un-
24 less the Court of Review issues a finding that
25 such appointment is not appropriate.

“(B) FISA COURT OF REVIEW DECISIONS.—An amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court of Review to certify for review to the Supreme Court of the United States any question of law pursuant to section 1254(2) of title 28, United States Code, in the matter in which that amicus curiae was appointed.

“(C) DECLASSIFICATION OF REFERRALS.—For purposes of section 602, if the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review denies a petition filed under subparagraph (A) or (B) of this paragraph, that petition and all of its content shall be considered a decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review described in section 602(a).”.

(c) ACCESS TO INFORMATION.—

(1) APPLICATION AND MATERIALS.—Subparagraph (A) of section 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)) is amended to read as follows:

“(A) IN GENERAL.—

1 “(i) RIGHTS OF AMICUS.—If a court
2 established under subsection (a) or (b) ap-
3 points an amicus curiae under paragraph
4 (2), the amicus curiae—

5 “(I) shall have access to, to the
6 extent such information is available to
7 the Government and the court estab-
8 lished under subsection (a) or (b) de-
9 termines it is necessary to fulfill the
10 duties of the amicus curiae—

11 “(aa) the application, certifi-
12 cation, petition, motion, and
13 other information and supporting
14 materials submitted to the For-
15 eign Intelligence Surveillance
16 Court in connection with the
17 matter in which the amicus cu-
18 riae has been appointed, includ-
19 ing access to any relevant legal
20 precedent (including any such
21 precedent that is cited by the
22 Government, including in such an
23 application);

24 “(bb) a copy of each rel-
25 evant decision made by the For-

1 eign Intelligence Surveillance
2 Court or the Foreign Intelligence
3 Surveillance Court of Review in
4 which the court decides a ques-
5 tion of law, without regard to
6 whether the decision is classified;
7 and

8 “(cc) any other information
9 or materials that the court deter-
10 mines are relevant to the duties
11 of the amicus curiae; and

12 “(II) may make a submission to
13 the court requesting access to any
14 other particular materials or informa-
15 tion (or category of materials or infor-
16 mation) that the amicus curiae be-
17 lieves to be relevant to the duties of
18 the amicus curiae.

19 “(ii) SUPPORTING DOCUMENTATION
20 REGARDING ACCURACY.—The Foreign In-
21 telligence Surveillance Court, upon the mo-
22 tion of an amicus curiae appointed under
23 paragraph (2) or upon its own motion,
24 may require the Government to make
25 available the supporting documentation re-

1 garding the accuracy of any material sub-
2 mitted to the Foreign Intelligence Surveil-
3 lance Court in connection with the matter
4 in which the amicus curiae has been ap-
5 pointed if the court determines the infor-
6 mation is relevant to the duties of the ami-
7 cus curiae.”.

8 (2) CLARIFICATION OF ACCESS TO CERTAIN IN-
9 FORMATION.—Such section is further amended by
10 striking subparagraph (C) and inserting the fol-
11 lowing:

12 “(C) CLASSIFIED INFORMATION.—An ami-
13 cus curiae appointed by the court shall have ac-
14 cess, to the extent such information is available
15 to the Government and the court determines
16 such information is relevant to the duties of the
17 amicus curiae in the matter in which the ami-
18 cus curiae was appointed, to copies of each
19 opinion, order, transcript, pleading, or other
20 document of the Foreign Intelligence Surveil-
21 lance Court and the Foreign Intelligence Sur-
22 veillance Court of Review, including, if the indi-
23 vidual is eligible for access to classified informa-
24 tion, any classified documents, information, and
25 other materials or proceedings, but only to the

1 extent consistent with the national security of
 2 the United States.”.

3 (3) CONSULTATION AMONG AMICI CURIAE.—

4 Such section is further amended—

5 (A) by redesignating subparagraphs (B),
 6 (C), and (D) as subparagraphs (C), (D), and
 7 (E), respectively; and

8 (B) by inserting after subparagraph (A)
 9 the following:

10 “(B) CONSULTATION.—If the Foreign In-
 11 telligence Surveillance Court or the Foreign In-
 12 telligence Surveillance Court of Review deter-
 13 mines that it is relevant to the duties of an
 14 amicus curiae appointed by the court under
 15 paragraph (2), the amicus curiae may consult
 16 with one or more of the other individuals des-
 17 ignated to serve as amicus curiae pursuant to
 18 paragraph (1) regarding any of the information
 19 relevant to any assigned proceeding.”.

20 (d) TERM LIMITS.—

21 (1) REQUIREMENT.—Paragraph (1) of section
 22 103(i) of such Act (50 U.S.C. 1803(i)) is amended
 23 by adding at the end the following new sentence:
 24 “An individual may serve as an amicus curiae for a
 25 5-year term, and the presiding judges may, for good

1 cause, jointly reappoint the individual to a single ad-
 2 ditional 5-year term.”.

3 (2) APPLICATION.—The amendment made by
 4 paragraph (1) shall apply with respect to the service
 5 of an amicus curiae appointed under section 103(i)
 6 of such Act (50 U.S.C. 1803(i)) that occurs on or
 7 after the date of the enactment of this Act, regard-
 8 less of the date on which the amicus curiae is ap-
 9 pointed.

10 **SEC. 1202. LIMITATION ON DIRECTIVES UNDER FOREIGN**
 11 **INTELLIGENCE SURVEILLANCE ACT OF 1978**
 12 **RELATING TO CERTAIN ELECTRONIC COM-**
 13 **MUNICATION SERVICE PROVIDERS.**

14 Section 702(i) of the Foreign Intelligence Surveil-
 15 lance Act of 1978 (50 U.S.C. 1881a(i)) is amended by
 16 adding at the end the following:

17 “(7) LIMITATION RELATING TO CERTAIN ELEC-
 18 TRONIC COMMUNICATION SERVICE PROVIDERS.—

19 “(A) DEFINITIONS.—In this paragraph:

20 “(i) APPROPRIATE COMMITTEES OF
 21 CONGRESS.—The term ‘appropriate com-
 22 mittees of Congress’ means—

23 “(I) the congressional intelligence
 24 committees;

1 “(II) the Committee on the Judi-
2 ciary of the Senate; and

3 “(III) the Committee on the Ju-
4 diciary of the House of Representa-
5 tives.

6 “(ii) COVERED ELECTRONIC COMMU-
7 NICATION SERVICE PROVIDER.—The term
8 ‘covered electronic communication service
9 provider’ means—

10 “(I) a service provider described
11 in section 701(b)(4)(E); or

12 “(II) a custodian of an entity as
13 defined in section 701(b)(4)(F).

14 “(iii) COVERED OPINIONS.—The term
15 ‘covered opinions’ means the opinions of
16 the Foreign Intelligence Surveillance Court
17 and the Foreign Intelligence Surveillance
18 Court of Review authorized for public re-
19 lease on August 23, 2023 (Opinion and
20 Order, In re Petition to Set Aside or Mod-
21 ify Directive Issued to [REDACTED], No.
22 [REDACTED], (FISA Ct. [REDACTED]
23 2022) (Contreras J.); Opinion, In re Peti-
24 tion to Set Aside or Modify Directive
25 Issued to [REDACTED], No. [RE-

1 DACTED], (FISA Ct. Rev. [RE-
2 DACTED] 2023) (Sentelle, J.; Higginson,
3 J.; Miller J.)).

4 “(B) LIMITATION.—A directive may not be
5 issued under paragraph (1) to a covered elec-
6 tronic communication service provider unless
7 the covered electronic communication service
8 provider is a provider of the type of service at
9 issue in the covered opinions.

10 “(C) REQUIREMENTS FOR DIRECTIVES TO
11 COVERED ELECTRONIC COMMUNICATION SERV-
12 ICE PROVIDERS.—

13 “(i) IN GENERAL.—Subject to clause
14 (ii), any directive issued under paragraph
15 (1) on or after the date of the enactment
16 of the Intelligence Authorization Act for
17 Fiscal Year 2025 to a covered electronic
18 communication service provider that is not
19 prohibited by subparagraph (B) of this
20 paragraph shall include a summary de-
21 scription of the services at issue in the cov-
22 ered opinions.

23 “(ii) DUPLICATE SUMMARIES NOT RE-
24 QUIRED.—A directive need not include a
25 summary description of the services at

1 issue in the covered opinions if such sum-
2 mary was included in a prior directive
3 issued to the covered electronic commu-
4 nication service provider and the summary
5 has not materially changed.

6 “(D) FOREIGN INTELLIGENCE SURVEIL-
7 LANCE COURT NOTIFICATION AND REVIEW.—

8 “(i) NOTIFICATION.—

9 “(I) IN GENERAL.—Subject to
10 subclause (II), each time the Attorney
11 General and the Director of National
12 Intelligence issue a directive under
13 paragraph (1) to a covered electronic
14 communication service provider that is
15 not prohibited by subparagraph (B)
16 and each time the Attorney General
17 and the Director materially change a
18 directive under paragraph (1) issued
19 to a covered electronic communication
20 service provider that is not prohibited
21 by subparagraph (B), the Attorney
22 General and the Director shall provide
23 the directive to the Foreign Intel-
24 ligence Surveillance Court on or be-
25 fore the date that is 7 days after the

1 date on which the Attorney General
2 and the Director issue the directive,
3 along with a description of the covered
4 electronic communication service pro-
5 vider to whom the directive is issued
6 and the services at issue.

7 “(II) DUPLICATION NOT RE-
8 QUIRED.—The Attorney General and
9 the Director do not need to provide a
10 directive or description to the Foreign
11 Intelligence Surveillance Court under
12 subclause (I) if a directive and de-
13 scription concerning the covered elec-
14 tronic communication service provider
15 was previously provided to the Court
16 and the directive or description has
17 not materially changed.

18 “(ii) ADDITIONAL INFORMATION.—As
19 soon as feasible and not later than the ini-
20 tiation of collection, the Attorney General
21 and the Director shall, for each directive
22 described in subparagraph (i), provide the
23 Foreign Intelligence Surveillance Court a
24 description of the type of equipment to be
25 accessed, the nature of the access, and the

1 form of assistance required pursuant to the
2 directive.

3 “(iii) REVIEW.—

4 “(I) IN GENERAL.—The Foreign
5 Intelligence Surveillance Act Court
6 may review a directive received by the
7 Court under clause (i) to determine
8 whether the directive is consistent
9 with subparagraph (B) and affirm,
10 modify, or set aside the directive.

11 “(II) NOTICE OF INTENT TO RE-
12 VIEW.—Not later than 10 days after
13 the date on which the Court receives
14 information under clause (ii) with re-
15 spect to a directive, the Court shall
16 provide notice to the Attorney Gen-
17 eral, the Director, and the covered
18 electronic communication service pro-
19 vider, indicating whether the Court in-
20 tends to undertake a review under
21 subclause (I) of this clause.

22 “(III) COMPLETION OF RE-
23 VIEWS.—In a case in which the Court
24 provides notice under subclause (II)
25 indicating that the Court intends to

1 review a directive under subclause (I),
2 the Court shall, not later than 30
3 days after the date on which the
4 Court provides notice under subclause
5 (II) with respect to the directive, com-
6 plete the review.

7 “(E) CONGRESSIONAL OVERSIGHT.—

8 “(i) NOTIFICATION.—

9 “(I) IN GENERAL.—Subject to
10 subclause (II), each time the Attorney
11 General and the Director of National
12 Intelligence issue a directive under
13 paragraph (1) to a covered electronic
14 communication service provider that is
15 not prohibited by subparagraph (B)
16 and each time the Attorney General
17 and the Director materially change a
18 directive under paragraph (1) issued
19 to a covered electronic communication
20 service provider that is not prohibited
21 by subparagraph (B), the Attorney
22 General and the Director shall submit
23 to the appropriate committees of Con-
24 gress the directive on or before the
25 date that is 7 days after the date on

1 which the Attorney General and the
2 Director issue the directive, along
3 with description of the covered elec-
4 tronic communication service provider
5 to whom the directive is issued and
6 the services at issue.

7 “(II) DUPLICATION NOT RE-
8 QUIRED.—The Attorney General and
9 the Director do not need to submit a
10 directive or description to the appro-
11 priate committees of Congress under
12 subclause (I) if a directive and de-
13 scription concerning the covered elec-
14 tronic communication service provider
15 was previously submitted to the ap-
16 propriate committees of Congress and
17 the directive or description has not
18 materially changed.

19 “(ii) ADDITIONAL INFORMATION.—As
20 soon as feasible and not later than the ini-
21 tiation of collection, the Attorney General
22 and the Director shall, for each directive
23 described in subparagraph (i), provide the
24 appropriate committees of Congress a de-
25 scription of the type of equipment to be

1 accessed, the nature of the access, and the
2 form of assistance required pursuant to the
3 directive.

4 “(iii) REPORTING.—

5 “(I) QUARTERLY REPORTS.—Not
6 later than 90 days after the date of
7 the enactment of the Intelligence Au-
8 thorization Act for Fiscal Year 2025
9 and not less frequently than once each
10 quarter thereafter, the Attorney Gen-
11 eral and the Director shall submit to
12 the appropriate committees of Con-
13 gress a report on the number of direc-
14 tives issued, during the period covered
15 by the report, under paragraph (1) to
16 a covered electronic communication
17 service provider and the number of di-
18 rectives provided during the same pe-
19 riod to the Foreign Intelligence Sur-
20 veillance Court under subparagraph
21 (D)(i).

22 “(II) FORM OF REPORTS.—Each
23 report submitted pursuant to sub-
24 clause (I) shall be submitted in un-

classified form, but may include a
classified annex.

“(III) SUBMITTAL OF COURT
OPINIONS.—Not later than 45 days
after the date on which the Foreign
Intelligence Surveillance Court or the
Foreign Intelligence Surveillance
Court of Review issues an opinion re-
lating to a directive issued to a cov-
ered electronic communication service
provider under paragraph (1), the At-
torney General shall submit to the ap-
propriate committees of Congress a
copy of the opinion.”.

**SEC. 1203. STRENGTHENING ELECTION CYBERSECURITY
TO UPHOLD RESPECT FOR ELECTIONS
THROUGH INDEPENDENT TESTING ACT OF
2024.**

(a) SHORT TITLE.—This section may be cited as the
“Strengthening Election Cybersecurity to Uphold Respect
for Elections through Independent Testing Act of 2024”
or the “SECURE IT Act of 2024”.

(b) REQUIRING PENETRATION TESTING AS PART OF
THE TESTING AND CERTIFICATION OF VOTING SYS-
TEMS.—Section 231 of the Help America Vote Act of

1 2002 (52 U.S.C. 20971) is amended by adding at the end
2 the following new subsection:

3 “(e) REQUIRED PENETRATION TESTING.—

4 “(1) IN GENERAL.—Not later than 180 days
5 after the date of the enactment of this subsection,
6 the Commission shall provide for the conduct of pen-
7 etration testing as part of the testing, certification,
8 decertification, and recertification of voting system
9 hardware and software by the Commission based on
10 accredited laboratories under this section.

11 “(2) ACCREDITATION.—The Commission shall
12 develop a program for the acceptance of the results
13 of penetration testing on election systems. The pene-
14 tration testing required by this subsection shall be
15 required for Commission certification. The Commis-
16 sion shall vote on the selection of any entity identi-
17 fied. The requirements for such selection shall be
18 based on consideration of an entity’s competence to
19 conduct penetration testing under this subsection.
20 The Commission may consult with the National In-
21 stitute of Standards and Technology or any other
22 appropriate Federal agency on lab selection criteria
23 and other aspects of this program.”.

1 (c) INDEPENDENT SECURITY TESTING AND COORDI-
 2 NATED CYBERSECURITY VULNERABILITY DISCLOSURE
 3 PROGRAM FOR ELECTION SYSTEMS.—

4 (1) IN GENERAL.—Subtitle D of title II of the
 5 Help America Vote Act of 2002 (42 U.S.C. 15401
 6 et seq.) is amended by adding at the end the fol-
 7 lowing new part:

8 **“PART 7—INDEPENDENT SECURITY TESTING AND**
 9 **COORDINATED CYBERSECURITY VULNER-**
 10 **ABILITY DISCLOSURE PILOT PROGRAM FOR**
 11 **ELECTION SYSTEMS**

12 **“SEC. 297. INDEPENDENT SECURITY TESTING AND COORDI-**
 13 **NATED CYBERSECURITY VULNERABILITY**
 14 **DISCLOSURE PILOT PROGRAM FOR ELEC-**
 15 **TION SYSTEMS.**

16 “(a) IN GENERAL.—

17 “(1) ESTABLISHMENT.—The Commission, in
 18 consultation with the Secretary, shall establish an
 19 Independent Security Testing and Coordinated Vul-
 20 nerability Disclosure Pilot Program for Election Sys-
 21 tems (VDP–E) (in this section referred to as the
 22 ‘program’) to test for and disclose cybersecurity
 23 vulnerabilities in election systems.

24 “(2) DURATION.—The program shall be con-
 25 ducted for a period of 5 years.

1 “(3) REQUIREMENTS.—In carrying out the pro-
2 gram, the Commission, in consultation with the Sec-
3 retary, shall—

4 “(A) establish a mechanism by which an
5 election systems vendor may make their election
6 system (including voting machines and source
7 code) available to cybersecurity researchers par-
8 ticipating in the program;

9 “(B) provide for the vetting of cybersecu-
10 rity researchers prior to their participation in
11 the program, including the conduct of back-
12 ground checks;

13 “(C) establish terms of participation
14 that—

15 “(i) describe the scope of testing per-
16 mitted under the program;

17 “(ii) require researchers to—

18 “(I) notify the vendor, the Com-
19 mission, and the Secretary of any cy-
20 bersecurity vulnerability they identify
21 with respect to an election system;
22 and

23 “(II) otherwise keep such vulner-
24 ability confidential for 180 days after
25 such notification;

1 “(iii) require the good faith participa-
2 tion of all participants in the program;

3 “(iv) require an election system ven-
4 dor, within 180 days after validating noti-
5 fication of a critical or high vulnerability
6 (as defined by the National Institute of
7 Standards and Technology) in an election
8 system of the vendor, to—

9 “(I) send a patch or propound
10 some other fix or mitigation for such
11 vulnerability to the appropriate State
12 and local election officials, in con-
13 sultation with the researcher who dis-
14 covered it; and

15 “(II) notify the Commission and
16 the Secretary that such patch has
17 been sent to such officials;

18 “(D) in the case where a patch or fix to
19 address a vulnerability disclosed under subpara-
20 graph (C)(ii)(I) is intended to be applied to a
21 system certified by the Commission, provide—

22 “(i) for the expedited review of such
23 patch or fix within 90 days after receipt by
24 the Commission; and

1 “(ii) if such review is not completed
 2 by the last day of such 90-day period, that
 3 such patch or fix shall be deemed to be
 4 certified by the Commission, subject to any
 5 subsequent review of such determination
 6 by the Commission; and

7 “(E) 180 days after the disclosure of a
 8 vulnerability under subparagraph (C)(ii)(I), no-
 9 tify the Director of the Cybersecurity and In-
 10 frastructure Security Agency of the vulner-
 11 ability for inclusion in the database of Common
 12 Vulnerabilities and Exposures.

13 “(4) VOLUNTARY PARTICIPATION; SAFE HAR-
 14 BOR.—

15 “(A) VOLUNTARY PARTICIPATION.—Par-
 16 ticipation in the program shall be voluntary for
 17 election systems vendors and researchers.

18 “(B) SAFE HARBOR.—When conducting
 19 research under this program, such research and
 20 subsequent publication shall be—

21 “(i) authorized in accordance with
 22 section 1030 of title 18, United States
 23 Code (commonly known as the ‘Computer
 24 Fraud and Abuse Act’), (and similar State
 25 laws), and the election system vendor will

not initiate or support legal action against the researcher for accidental, good faith violations of the program; and

“(ii) exempt from the anti-circumvention rule of section 1201 of title 17, United States Code (commonly known as the ‘Digital Millennium Copyright Act’), and the election system vendor will not bring a claim against a researcher for circumvention of technology controls.

“(C) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to limit or otherwise affect any exception to the general prohibition against the circumvention of technological measures under subparagraph (A) of section 1201(a)(1) of title 17, United States Code, including with respect to any use that is excepted from that general prohibition by the Librarian of Congress under subparagraphs (B) through (D) of such section 1201(a)(1).

“(5) DEFINITIONS.—In this subsection:

“(A) CYBERSECURITY VULNERABILITY.—The term ‘cybersecurity vulnerability’ means, with respect to an election system, any security vulnerability that affects the election system.

1 “(B) ELECTION INFRASTRUCTURE.—The
2 term ‘election infrastructure’ means—

3 “(i) storage facilities, polling places,
4 and centralized vote tabulation locations
5 used to support the administration of elec-
6 tions for public office; and

7 “(ii) related information and commu-
8 nications technology, including—

9 “(I) voter registration databases;

10 “(II) election management sys-
11 tems;

12 “(III) voting machines;

13 “(IV) electronic mail and other
14 communications systems (including
15 electronic mail and other systems of
16 vendors who have entered into con-
17 tracts with election agencies to sup-
18 port the administration of elections,
19 manage the election process, and re-
20 port and display election results); and

21 “(V) other systems used to man-
22 age the election process and to report
23 and display election results on behalf
24 of an election agency.

1 “(C) ELECTION SYSTEM.—The term ‘elec-
2 tion system’ means any information system that
3 is part of an election infrastructure, including
4 any related information and communications
5 technology described in subparagraph (B)(ii).

6 “(D) ELECTION SYSTEM VENDOR.—The
7 term ‘election system vendor’ means any person
8 providing, supporting, or maintaining an elec-
9 tion system on behalf of a State or local elec-
10 tion official.

11 “(E) INFORMATION SYSTEM.—The term
12 ‘information system’ has the meaning given the
13 term in section 3502 of title 44, United States
14 Code.

15 “(F) SECRETARY.—The term ‘Secretary’
16 means the Secretary of Homeland Security.

17 “(G) SECURITY VULNERABILITY.—The
18 term ‘security vulnerability’ has the meaning
19 given the term in section 102 of the Cybersecu-
20 rity Information Sharing Act of 2015 (6 U.S.C.
21 1501).”.

22 (2) CLERICAL AMENDMENT.—The table of con-
23 tents of such Act is amended by adding at the end

1 of the items relating to subtitle D of title II the fol-
 2 lowing:

“PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS

“Sec. 297. Independent security testing and coordinated cybersecurity vulnerability disclosure program for election systems.”.

3 **SEC. 1204. PRIVACY AND CIVIL LIBERTIES OVERSIGHT**
 4 **BOARD QUALIFICATIONS.**

5 Section 1061(h)(2) of the Intelligence Reform and
 6 Terrorism Prevention Act of 2004 (42 U.S.C.
 7 2000ee(h)(2)) is amended by striking “and relevant experience” and inserting “or experience in positions requiring
 8 a security clearance, and relevant national security experience”.

11 **SEC. 1205. PARITY IN PAY FOR STAFF OF THE PRIVACY AND**
 12 **CIVIL LIBERTIES OVERSIGHT BOARD AND**
 13 **THE INTELLIGENCE COMMUNITY.**

14 Section 1061(j)(1) of the Intelligence Reform and
 15 Terrorism Prevention Act of 2004 (42 U.S.C.
 16 2000ee(j)(1)) is amended by striking “except that” and
 17 all that follows through the period at the end and inserting
 18 “except that no rate of pay fixed under this subsection
 19 may exceed the highest amount paid by any element of
 20 the intelligence community for a comparable position,
 21 based on salary information provided to the chairman of
 22 the Board by the Director of National Intelligence.”.

1 **SEC. 1206. MODIFICATION AND REPEAL OF REPORTING RE-**
2 **QUIREMENTS.**

3 (a) BRIEFING ON IRANIAN EXPENDITURES SUP-
4 PORTING FOREIGN MILITARY AND TERRORIST ACTIVI-
5 TIES.—Section 6705(a)(1) of the Damon Paul Nelson and
6 Matthew Young Pollard Intelligence Authorization Act for
7 Fiscal Years 2018, 2019, and 2020 (22 U.S.C.
8 9412(a)(1)) is amended by striking “, and not less fre-
9 quently than once each year thereafter provide a briefing
10 to Congress,”.

11 (b) REPORTS AND BRIEFINGS ON NATIONAL SECU-
12 RITY EFFECTS OF GLOBAL WATER INSECURITY AND
13 EMERGING INFECTIOUS DISEASES AND PANDEMICS.—
14 Section 6722(b) of the Damon Paul Nelson and Matthew
15 Young Pollard Intelligence Authorization Act for Fiscal
16 Years 2018, 2019, and 2020 (50 U.S.C. 3024 note; divi-
17 sion E of Public Law 116–92) is amended by—

18 (1) striking paragraph (2); and

19 (2) redesignating paragraphs (3) and (4) as
20 paragraphs (2) and (3), respectively.

21 (c) REPEAL OF REPORT ON REMOVAL OF SAT-
22 ELLITES AND RELATED ITEMS FROM THE UNITED
23 STATES MUNITIONS LIST.—Section 1261(e) of the Na-
24 tional Defense Authorization Act for Fiscal Year 2013 (22
25 U.S.C. 2778 note; Public Law 112–239) is repealed.

1 (d) BRIEFING ON REVIEW OF INTELLIGENCE COM-
2 MUNITY ANALYTIC PRODUCTION.—Section 1019(c) of the
3 Intelligence Reform and Terrorism Prevention Act of
4 2004 (50 U.S.C. 3364(c)) is amended by striking “Decem-
5 ber 1” and inserting “February 1”.

6 (e) REPEAL OF REPORT ON OVERSIGHT OF FOREIGN
7 INFLUENCE IN ACADEMIA.—Section 5713 of the Damon
8 Paul Nelson and Matthew Young Pollard Intelligence Au-
9 thorization Act for Fiscal Years 2018, 2019, and 2020
10 (50 U.S.C. 3369b) is repealed.

11 (f) REPEAL OF BRIEFING ON IRANIAN EXPENDI-
12 TURES SUPPORTING FOREIGN MILITARY AND TERRORIST
13 ACTIVITIES.—Section 6705 of the Damon Paul Nelson
14 and Matthew Young Pollard Intelligence Authorization
15 Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C.
16 9412) is amended—

17 (1) by striking subsection (b);

18 (2) by striking the enumerator and heading for
19 subsection (a);

20 (3) by redesignating paragraphs (1) and (2) as
21 subsections (a) and (b), respectively, and moving
22 such subsections, as so redesignated, 2 ems to the
23 left;

24 (4) in subsection (a), as so redesignated, by re-
25 designating subparagraphs (A) and (B) as para-

1 graphs (1) and (2), respectively, and moving such
 2 paragraphs, as so redesignated, 2 ems to the left;
 3 and

4 (5) in paragraph (1), as so redesignated, by re-
 5 designating clauses (i) through (v) as subparagraphs
 6 (A) through (E), respectively, and moving such sub-
 7 paragraphs, as so redesignated, 2 ems to the left.

8 (g) REPEAL OF REPORT ON FOREIGN INVESTMENT
 9 RISKS.—Section 6716 of the Damon Paul Nelson and
 10 Matthew Young Pollard Intelligence Authorization Act for
 11 Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3370a)
 12 is repealed.

13 (h) REPEAL OF REPORT ON INTELLIGENCE COMMU-
 14 NITY LOAN REPAYMENT PROGRAMS.—Section 6725(c) of
 15 the Damon Paul Nelson and Matthew Young Pollard In-
 16 telligence Authorization Act for Fiscal Years 2018, 2019,
 17 and 2020 (50 U.S.C. 3334g(c)) is repealed.

18 (i) REPEAL OF REPORT ON DATA COLLECTION ON
 19 ATTRITION IN INTELLIGENCE COMMUNITY.—Section
 20 306(c) of the Intelligence Authorization Act for Fiscal
 21 Year 2021 (50 U.S.C. 3334h(c)) is repealed.

22 **SEC. 1207. TECHNICAL AMENDMENTS.**

23 (a) REQUIREMENTS RELATING TO CONSTRUCTION
 24 OF FACILITIES TO BE USED PRIMARILY BY INTEL-
 25 LIGENCE COMMUNITY.—Section 602(a) of the Intelligence

1 Authorization Act for Fiscal Year 1995 (50 U.S.C.
2 3304(a)) is amended—

3 (1) in paragraph (1), by striking “\$6,000,000”
4 and inserting “\$9,000,000”; and

5 (2) in paragraph (2)—

6 (A) by striking “\$2,000,000” each place it
7 appears and inserting “\$4,000,000”; and

8 (B) by striking “\$6,000,000” and insert-
9 ing “\$9,000,000”.

10 (b) COPYRIGHT PROTECTION FOR CIVILIAN FACULTY
11 OF CERTAIN ACCREDITED INSTITUTIONS.—Section 105
12 of title 17, United States Code, is amended to read as
13 follows:

14 **“§ 105. Subject matter of copyright: United States**
15 **Government works**

16 “(a) IN GENERAL.—Copyright protection under this
17 title is not available for any work of the United States
18 Government, but the United States Government is not
19 precluded from receiving and holding copyrights trans-
20 ferred to it by assignment, bequest, or otherwise.

21 “(b) COPYRIGHT PROTECTION OF CERTAIN
22 WORKS.—Subject to subsection (c), the covered author of
23 a covered work owns the copyright to that covered work.

24 “(c) USE BY FEDERAL GOVERNMENT.—

1 “(1) SECRETARY OF DEFENSE AUTHORITY.—

2 With respect to a covered author who produces a
3 covered work in the course of employment at a cov-
4 ered institution described in subparagraphs (A)
5 through (K) of subsection (d)(2), the Secretary of
6 Defense may direct the covered author to provide
7 the Federal Government with an irrevocable, royalty-
8 free, worldwide, nonexclusive license to reproduce,
9 distribute, perform, or display such covered work for
10 purposes of the United States Government.

11 “(2) SECRETARY OF HOMELAND SECURITY AU-

12 THORITY.—With respect to a covered author who
13 produces a covered work in the course of employ-
14 ment at the covered institution described in sub-
15 section (d)(2)(L), the Secretary of Homeland Secu-
16 rity may direct the covered author to provide the
17 Federal Government with an irrevocable, royalty-
18 free, worldwide, nonexclusive license to reproduce,
19 distribute, perform, or display such covered work for
20 purposes of the United States Government.

21 “(3) DIRECTOR OF NATIONAL INTELLIGENCE

22 AUTHORITY.—With respect to a covered author who
23 produces a covered work in the course of employ-
24 ment at the covered institution described in sub-
25 section (d)(2)(M), the Director of National Intel-

1 ligence may direct the covered author to provide the
 2 Federal Government with an irrevocable, royalty-
 3 free, worldwide, nonexclusive license to reproduce,
 4 distribute, perform, or display such covered work for
 5 purposes of the United States Government.

6 “(4) SECRETARY OF TRANSPORTATION AU-
 7 THORITY.—With respect to a covered author who
 8 produces a covered work in the course of employ-
 9 ment at the covered institution described in sub-
 10 section (d)(2)(N), the Secretary of Transportation
 11 may direct the covered author to provide the Federal
 12 Government with an irrevocable, royalty-free, world-
 13 wide, nonexclusive license to reproduce, distribute,
 14 perform, or display such covered work for purposes
 15 of the United States Government.

16 “(d) DEFINITIONS.—In this section:

17 “(1) COVERED AUTHOR.—The term ‘covered
 18 author’ means a civilian member of the faculty of a
 19 covered institution.

20 “(2) COVERED INSTITUTION.—The term ‘cov-
 21 ered institution’ means the following:

22 “(A) National Defense University.

23 “(B) United States Military Academy.

24 “(C) Army War College.

1 “(D) United States Army Command and
2 General Staff College.

3 “(E) United States Naval Academy.

4 “(F) Naval War College.

5 “(G) Naval Postgraduate School.

6 “(H) Marine Corps University.

7 “(I) United States Air Force Academy.

8 “(J) Air University.

9 “(K) Defense Language Institute.

10 “(L) United States Coast Guard Academy.

11 “(M) National Intelligence University.

12 “(N) United States Merchant Marine
13 Academy.

14 “(3) COVERED WORK.—The term ‘covered
15 work’ means a literary work produced by a covered
16 author in the course of employment at a covered in-
17 stitution for publication by a scholarly press or jour-
18 nal.”.

Calendar No. 412

118TH CONGRESS
2D Session
S. 4443

A BILL

To authorize appropriations for fiscal year 2025 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 3, 2024

Reported the following original bill: which was read twice
and placed on the calendar