

Calendar No. 420

119TH CONGRESS
2D SESSION**S. 4615**

To authorize appropriations for fiscal year 2027 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

MAY 20, 2026

Mr. COTTON, 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 2027 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 2027”.

- 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—MATTERS RELATING TO THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Sec. 301. Appointment of Deputy Director of National Intelligence and Assistant Directors of National Intelligence.
 Sec. 302. Repeal of National Intelligence Management Council.
 Sec. 303. Repeal of various positions, units, centers, councils, and offices.
 Sec. 304. Transfer of National Intelligence University.
 Sec. 305. Limitation on domestic activities at the National Counterterrorism Center.
 Sec. 306. Timely provision of security direction to intelligence community whistleblowers.
 Sec. 307. Notification of certain declassifications.
 Sec. 308. No police, subpoena, or law enforcement powers or internal security functions for Director of National Intelligence.

TITLE IV—MATTERS RELATING TO THE CENTRAL INTELLIGENCE AGENCY

Sec. 401. Extension of Central Intelligence Agency authority regarding unmanned aircraft systems.
 Sec. 402. Higher Education Act of 1965 special rule.
 Sec. 403. Modification relating to security personnel at certain installations.

TITLE V—MATTERS RELATING TO OTHER ELEMENTS OF THE INTELLIGENCE COMMUNITY

Sec. 501. Authority of National Security Agency to correlate, evaluate, and disseminate certain intelligence.
 Sec. 502. Prohibition on availability of funds for relocation of Office of Intelligence and Analysis to certain facilities.
 Sec. 503. Funds for foreign intelligence activities conducted with and by the National Reconnaissance Office.
 Sec. 504. Modification of annual report on Federal Bureau of Investigation case data.
 Sec. 505. Establishment of Office of Counterintelligence.
 Sec. 506. Modification of responsibilities of Office of Intelligence and Analysis.

Sec. 507. Role of National Security Agency in collection and analysis of signals intelligence.

TITLE VI—GENERAL INTELLIGENCE COMMUNITY MATTERS

- Sec. 601. Amendments to presidential appointments for intelligence community positions.
- Sec. 602. Procedures regarding dissemination of nonpublicly available information concerning United States persons.
- Sec. 603. Analytic standards for all-source intelligence products.
- Sec. 604. Limitation on use of Intelligence Community Management Account funds for certain entities.
- Sec. 605. Ben Sasse Intelligence Community Technology Fellowship Program.
- Sec. 606. Intelligence Community Counterintelligence Office at the Department of Commerce.
- Sec. 607. Countering hostile foreign cyber actors as a national intelligence priority.
- Sec. 608. Notification of criminal referrals regarding current or former intelligence community employees.
- Sec. 609. Modification of definitions in National Security Act of 1947 and scope of intelligence sharing responsibilities of Director of National Intelligence.
- Sec. 610. Prohibition on intelligence community use of adversary unmanned ground vehicles.
- Sec. 611. China-Taiwan Strategic Warning Task Force.
- Sec. 612. Limitations relating to Chinese products and services.
- Sec. 613. Limitation on intelligence community support for offensive cyber operations conducted by nongovernmental entities.
- Sec. 614. Biological intelligence activities of the intelligence community.
- Sec. 615. Prohibition on participation in prediction markets.
- Sec. 616. Repeal of certain report and briefing requirements.
- Sec. 617. Intelligence community personnel travel, allowances, and related expenses regulations.
- Sec. 618. Prohibition on sending and receiving objects using entities owned or controlled by persons or governments of certain countries.
- Sec. 619. Enhancing intelligence cooperation in the Indo-Pacific region.
- Sec. 620. Intelligence activities related to Ukraine.
- Sec. 621. Requirements relating to intelligence sharing with countries of significant concern to the United States.
- Sec. 622. United States-Israel intelligence sharing enhancement.

TITLE VII—ARTIFICIAL INTELLIGENCE MATTERS RELATING TO THE INTELLIGENCE COMMUNITY

- Sec. 701. Artificial intelligence exploitation guard and intelligence sharing.
- Sec. 702. Director of National Intelligence review of intelligence community use of artificial intelligence to support targeting.
- Sec. 703. Improvements for artificial intelligence policies, standards, and guidance for intelligence community.
- Sec. 704. Additional functions and requirements of Artificial Intelligence Security Center.
- Sec. 705. Reports on novel uses of artificial intelligence technology.
- Sec. 706. Clear labeling of artificial intelligence outputs for targeting workflows.
- Sec. 707. Research on use of artificial intelligence relating to inadvertent escalation.

- Sec. 708. Research on interaction of adversarial artificial intelligence systems with intelligence community systems.
- Sec. 709. Proliferation assessments regarding the export of artificial intelligence-related technologies.
- Sec. 710. Review of artificial intelligence security vulnerabilities under Vulnerabilities Equities Process.
- Sec. 711. Prohibition on certain artificial intelligence models on intelligence community systems.

TITLE VIII—OTHER MATTERS

- Sec. 801. Modification to notification requirements for authorized and ordered departures.
- Sec. 802. Identification of reallocable frequencies.
- Sec. 803. Protection of classified information relating to budget functions.
- Sec. 804. Review by Committee on Foreign Investment in the United States of transactions in real estate near intelligence community facilities.
- Sec. 805. Intelligence support to the U.S. International Development Finance Corporation.
- Sec. 806. Establishing processes and procedures for protecting Federal Reserve information.
- Sec. 807. Amendments to prohibit payments to obtain national security information or approvals.
- Sec. 808. Offenses involving espionage.
- Sec. 809. Parental bereavement leave.
- Sec. 810. Definition of foreign instrumentality for purposes of economic espionage prohibition.
- Sec. 811. Protection of trade secrets.
- Sec. 812. 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
 6 3 of the National Security Act of 1947 (50 U.S.C.
 7 3003).

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

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2027 for the conduct of the intelligence and intelligence-related activities of the Federal Government.

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

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

(b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AUTHORIZATIONS.—

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

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

1 (3) LIMITS ON DISCLOSURE.—The President
 2 shall not publicly disclose the classified Schedule of
 3 Authorizations or any portion of such Schedule ex-
 4 cept—

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

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

10 (C) as otherwise required by law.

11 **SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT AC-**
 12 **COUNT.**

13 (a) AUTHORIZATION OF APPROPRIATIONS.—There is
 14 authorized to be appropriated for the Intelligence Commu-
 15 nity Management Account of the Director of National In-
 16 telligence for fiscal year 2027 the sum of \$568,000,000.

17 (b) CLASSIFIED AUTHORIZATION OF APPROPRIA-
 18 TIONS.—In addition to amounts authorized to be appro-
 19 priated for the Intelligence Community Management Ac-
 20 count by subsection (a), there are authorized to be appro-
 21 priated for the Intelligence Community Management Ac-
 22 count for fiscal year 2027 such additional amounts as are
 23 specified in the classified Schedule of Authorizations re-
 24 ferred to in section 102(a).

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

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

8 **TITLE II—CENTRAL INTEL-**
9 **LIGENCE AGENCY RETIRE-**
10 **MENT AND DISABILITY SYS-**
11 **TEM**

12 **SEC. 201. AUTHORIZATION OF APPROPRIATIONS.**

13 There is authorized to be appropriated for the Cen-
14 tral Intelligence Agency Retirement and Disability Fund
15 \$514,000,000 for fiscal year 2027.

16 **TITLE III—MATTERS RELATING**
17 **TO THE OFFICE OF THE DI-**
18 **RECTOR OF NATIONAL INTEL-**
19 **LIGENCE**

20 **SEC. 301. APPOINTMENT OF DEPUTY DIRECTOR OF NA-**
21 **TIONAL INTELLIGENCE AND ASSISTANT DI-**
22 **RECTORS OF NATIONAL INTELLIGENCE.**

23 (a) REDESIGNATION OF PRINCIPAL DEPUTY DIREC-
24 TOR OF NATIONAL INTELLIGENCE AS DEPUTY DIRECTOR
25 OF NATIONAL INTELLIGENCE.—

1 (1) IN GENERAL.—Subsection (a) of section
 2 103A of the National Security Act of 1947 (50
 3 U.S.C. 3026) is amended—

4 (A) in the subsection heading, by striking
 5 “PRINCIPAL”; and

6 (B) by striking “Principal” each place it
 7 appears.

8 (2) CONFORMING AMENDMENTS.—Subsection
 9 (c) of such section is amended—

10 (A) in the subsection heading, by striking
 11 “PRINCIPAL”; and

12 (B) in paragraph (2)(B), by striking
 13 “Principal”.

14 (3) ADDITIONAL CONFORMING AMENDMENT.—

15 (A) NATIONAL SECURITY ACT OF 1947.—
 16 Such Act is further amended—

17 (i) in section 103(c)(2) (50 U.S.C.
 18 3025(c)(2)), by striking “Principal”;

19 (ii) in section 103I(b)(1) (50 U.S.C.
 20 3034(b)(1)), by striking “Principal”;

21 (iii) in section 106(a)(2)(A) (50
 22 U.S.C. 3041(a)(2)(A)), by striking “Prin-
 23 cipal”; and

24 (iv) in section 116(b) (50 U.S.C.
 25 3053(b)), by striking “Principal”.

(B) DAMON PAUL NELSON AND MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018, 2019, AND 2020.—Section 6310 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3351b) is amended by striking “Principal” each place it appears.

(C) NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2022.—Section 1683(b)(3) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(b)(3)) is amended by striking “Principal” both places it appears.

(b) ELIMINATION OF DEPUTY DIRECTORS OF NATIONAL INTELLIGENCE AND ESTABLISHMENT OF ASSISTANT DIRECTORS OF NATIONAL INTELLIGENCE.—

(1) IN GENERAL.—Section 103A(b) of the National Security Act of 1947 (50 U.S.C. 3026(b)) is amended—

(A) in the subsection heading, by striking “DEPUTY” and inserting “ASSISTANT”;

(B) in paragraph (1), by striking “may” and all that follows through the period at the end and inserting the following: “is an Assist-

ant Director of National Intelligence for Mission Integration and an Assistant Director of National Intelligence for Policy and Capabilities, who shall be appointed by the Director of National Intelligence.”; and

(C) in paragraph (2), by striking “Deputy” and inserting “Assistant”.

(2) CONFORMING AMENDMENTS.—The National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended—

(A) in section 102A(l)(4)(F) (50 U.S.C. 3024(l)(4)(F)), as redesignated by section 402(g)(1)(B), by striking “a Deputy” and inserting “an Assistant”; and

(B) in section 103(c) (50 U.S.C. 3025(c)), by striking paragraph (3).

(c) REFERENCES TO PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE IN LAW.—Any reference in law to the Principal Deputy Director of National Intelligence shall be treated as a reference to the Deputy Director of National Intelligence.

(d) CLERICAL AMENDMENTS.—

(1) SECTION HEADING.—Section 103A of such Act (50 U.S.C. 3026) is further amended, in the section heading, by striking “DEPUTY DIRECTORS OF

1 NATIONAL INTELLIGENCE” and inserting “DEPUTY
 2 DIRECTOR OF NATIONAL INTELLIGENCE AND AS-
 3 SISTANT DIRECTORS OF NATIONAL INTELLIGENCE”.

4 (2) TABLE OF CONTENTS.—The table of con-
 5 tents for such Act, in the matter preceding section
 6 2 of such Act, is amended by striking the item relat-
 7 ing to section 103A and inserting the following:

“Sec. 103A. Deputy Director of National Intelligence and Assistant Directors
 of National Intelligence.”.

8 **SEC. 302. REPEAL OF NATIONAL INTELLIGENCE MANAGE-**
 9 **MENT COUNCIL.**

10 (a) IN GENERAL.—Section 103M of the National Se-
 11 curity Act of 1947 (50 U.S.C. 3034d) is repealed.

12 (b) CLERICAL AMENDMENT.—The table of contents
 13 of such Act is amended by striking the item relating to
 14 section 103M.

15 **SEC. 303. REPEAL OF VARIOUS POSITIONS, UNITS, CEN-**
 16 **TERS, COUNCILS, AND OFFICES.**

17 (a) INTELLIGENCE COMMUNITY CHIEF DATA OFFI-
 18 CER.—

19 (1) REPEAL.—Title I of the National Security
 20 Act of 1947 (50 U.S.C. 3021 et seq.) is amended by
 21 striking section 103K (50 U.S.C. 3034b).

22 (2) CONFORMING AMENDMENT.—Section 103G
 23 of such Act (50 U.S.C. 3032) is amended by striking
 24 subsection (d).

1 (3) CLERICAL AMENDMENT.—The table of con-
 2 tents for such Act in the matter preceding section 2
 3 of such Act is amended by striking the item relating
 4 to section 103K.

5 (b) INTELLIGENCE COMMUNITY INNOVATION
 6 UNIT.—

7 (1) TERMINATION.—The Director of National
 8 Intelligence shall take such actions as may be nec-
 9 essary to terminate and wind down the operations of
 10 the Intelligence Community Innovation Unit before
 11 the date specified in paragraph (3).

12 (2) REPEAL.—

13 (A) IN GENERAL.—Title I of the National
 14 Security Act of 1947 (50 U.S.C. 3021 et seq.)
 15 is further amended by striking section 103L
 16 (50 U.S.C. 3034e).

17 (B) CLERICAL AMENDMENT.—The table of
 18 contents for such Act, in the matter preceding
 19 section 2 of such Act, is further amended by
 20 striking the item relating to section 103L.

21 (3) EFFECTIVE DATE.—The amendments made
 22 by this subsection shall take effect on the date that
 23 is 90 days after the date of the enactment of this
 24 Act.

1 (c) TECHNICAL AMENDMENT REGARDING EXPIRED
2 CLIMATE SECURITY ADVISORY COUNCIL.—

3 (1) REPEAL.—Title I of the National Security
4 Act of 1947 (50 U.S.C. 3021 et seq.) is further
5 amended by striking section 120 (50 U.S.C. 3060).

6 (2) CONFORMING AMENDMENT.—Section 331
7 of the National Defense Authorization Act for Fiscal
8 Year 2022 (Public Law 117–81; 10 U.S.C. 113
9 note) is amended by striking paragraph (2) and in-
10 serting the following:

11 “(2) The term ‘climate security’ means the ef-
12 fects of climate change on the following:

13 “(A) The national security of the United
14 States, including national security infrastruc-
15 ture.

16 “(B) Subnational, national, and regional
17 political stability.

18 “(C) The security of allies and partners of
19 the United States.

20 “(D) Ongoing or potential political vio-
21 lence, including unrest, rioting, guerrilla war-
22 fare, insurgency, terrorism, rebellion, revolution,
23 civil war, and interstate war.”.

24 (3) CLERICAL AMENDMENT.—The table of con-
25 tents for such Act, in the matter preceding section

1 2 of such Act, is further amended by striking the
 2 item relating to section 120.

3 (d) FRAMEWORK FOR CROSS-DISCIPLINARY EDU-
 4 CATION AND TRAINING.—

5 (1) REPEAL.—Subtitle A of title X of the Na-
 6 tional Security Act of 1947 (50 U.S.C. 3191 et seq.)
 7 is amended by striking section 1002 (50 U.S.C.
 8 3192).

9 (2) CLERICAL AMENDMENT.—The table of con-
 10 tents for such Act, in the matter preceding section
 11 2 of such Act, is further amended by striking the
 12 item relating to section 1002.

13 (e) FOREIGN LANGUAGES PROGRAM.—

14 (1) TERMINATION.—The Director of National
 15 Intelligence shall take such actions as may be nec-
 16 essary to terminate and wind down the operations of
 17 the Foreign Languages Program before the date
 18 specified in paragraph (5).

19 (2) REPEALS.—Subtitle B of such title (50
 20 U.S.C. 3201 et seq.) is amended by striking sections
 21 1011 (50 U.S.C. 3201, relating to program on ad-
 22 vancement of foreign languages critical to the intel-
 23 ligence community), 1012 (50 U.S.C. 3202, relating
 24 to education partnerships), and 1013 (50 U.S.C.
 25 3203, relating to voluntary services).

1 (3) CONFORMING AMENDMENTS.—Such subtitle
 2 is further amended by striking sections 1014 (50
 3 U.S.C. 3204, relating to regulations) and 1015 (50
 4 U.S.C. 3205, relating to definitions).

5 (4) CLERICAL AMENDMENTS.—The table of
 6 contents for such Act, in the matter preceding sec-
 7 tion 2 of such Act, is further amended by striking
 8 the items relating to subtitle B of title X.

9 (5) EFFECTIVE DATE.—The amendments made
 10 by this subsection shall take effect on the date that
 11 is 90 days after the date of the enactment of this
 12 Act.

13 (f) JOINT INTELLIGENCE COMMUNITY COUNCIL.—

14 (1) TERMINATION.—The Joint Intelligence
 15 Community Council is terminated.

16 (2) CONFORMING AMENDMENT.—Title I of the
 17 National Security Act of 1947 (50 U.S.C. 3021 et
 18 seq.) is amended by striking section 101A (50
 19 U.S.C. 3022).

20 (3) REPEAL OF REQUIREMENT TO CONSULT
 21 WITH JOINT INTELLIGENCE COMMUNITY COUNCIL
 22 FOR NATIONAL INTELLIGENCE PROGRAM BUDGET.—
 23 Section 102A(c)(1)(B) of the National Security Act
 24 of 1947 (50 U.S.C. 3024(c)(1)(B)) is amended by

1 striking “, as appropriate, after obtaining the advice
2 of the Joint Intelligence Community Council,”.

3 (4) CLERICAL AMENDMENT.—The table of con-
4 tents for such Act in the matter preceding section 2
5 of such Act is amended by striking the item relating
6 to section 101A.

7 **SEC. 304. TRANSFER OF NATIONAL INTELLIGENCE UNIVER-**
8 **SITY.**

9 (a) TRANSFER.—The Director of National Intel-
10 ligence shall transfer the functions of the National Intel-
11 ligence University to the National Defense University de-
12 scribed in section 2165 of title 10, United States Code.

13 (b) REPEAL.—Title X of the National Security Act
14 of 1947 (50 U.S.C. 3191 et seq.) is amended by striking
15 subtitle D (50 U.S.C. 3227 et seq.).

16 (c) CONFORMING AMENDMENTS.—

17 (1) TITLE 10.—Section 2151(b) of title 10,
18 United States Code, is amended by striking para-
19 graph (3).

20 (2) TITLE 17.—Section 105(d)(2) of title 17,
21 United States Code, is amended—

22 (A) by striking subparagraph (M); and

23 (B) by redesignating subparagraph (N) as
24 subparagraph (M).

1 (3) DAMON PAUL NELSON AND MATTHEW
 2 YOUNG POLLARD INTELLIGENCE AUTHORIZATION
 3 ACT FOR FISCAL YEARS 2018, 2019, AND 2020.—The
 4 Damon Paul Nelson and Matthew Young Pollard In-
 5 telligence Authorization Act for Fiscal Years 2018,
 6 2019, and 2020 (division E of Public Law 116–92)
 7 is amended by striking section 5324 (50 U.S.C.
 8 3334a).

9 (d) CLERICAL AMENDMENT.—The table of contents
 10 for the National Security Act of 1947 (50 U.S.C. 3002
 11 et seq.) is amended, in the matter preceding section 2 of
 12 such Act, by striking the items relating to subtitle D of
 13 title X.

14 **SEC. 305. LIMITATION ON DOMESTIC ACTIVITIES AT THE**
 15 **NATIONAL COUNTERTERRORISM CENTER.**

16 (a) DOMESTIC COUNTERTERRORISM INTEL-
 17 LIGENCE.—Subsection (e) of section 119 of the National
 18 Security Act of 1947 (50 U.S.C. 3056) is amended to read
 19 as follows:

20 “(e) LIMITATION ON DOMESTIC ACTIVITIES.—The
 21 Center may, consistent with applicable law, the direction
 22 of the President, and the guidelines referred to in section
 23 102A(b), receive and retain intelligence pertaining to do-
 24 mestic terrorism (as defined in section 2331 of title 18,
 25 United States Code) to enable the Center to collect, retain,

1 and disseminate intelligence pertaining only to inter-
 2 national terrorism (as defined in section 2331 of title 18,
 3 United States Code).”.

4 **SEC. 306. TIMELY PROVISION OF SECURITY DIRECTION TO**
 5 **INTELLIGENCE COMMUNITY WHISTLE-**
 6 **BLOWERS.**

7 (a) INTELLIGENCE COMMUNITY EMPLOYEES.—Sec-
 8 tion 103H(k)(5)(D)(ii)(II) of the National Security Act of
 9 1947 (50 U.S.C. 3033(k)(5)(D)(ii)(II)) is amended by in-
 10 serting “, unless the Director does not provide such direc-
 11 tion not later than 7 calendar days after the date on which
 12 the employee furnishes the statement required by sub-
 13 clause (I)” after “practices”.

14 (b) CENTRAL INTELLIGENCE AGENCY EMPLOY-
 15 EES.—Section 17(d)(5)(D)(ii)(II) of the Central Intel-
 16 ligence Agency Act of 1949 (50 U.S.C.
 17 3517(d)(5)(D)(ii)(II)) is amended by inserting “, unless
 18 the Director does not provide such direction not later than
 19 7 calendar days after the date on which the employee fur-
 20 nishes the statement required by subclause (I)” after
 21 “practices”.

22 **SEC. 307. NOTIFICATION OF CERTAIN DECLASSIFICATIONS.**

23 (a) IN GENERAL.—Title VIII of the National Secu-
 24 rity Act of 1947 (50 U.S.C. 3161 et seq.) is amended by
 25 adding at the end the following:

1 **“SEC. 806. NOTIFICATION OF CERTAIN**
2 **DECLASSIFICATIONS.**

3 “(a) NOTIFICATION TO CONGRESS BY DIRECTOR OF
4 NATIONAL INTELLIGENCE.—

5 “(1) IN GENERAL.—Immediately upon declas-
6 sifying, downgrading, or directing the declassifica-
7 tion or downgrading of information or intelligence
8 relating to intelligence sources, methods, or activities
9 pursuant to section 3.1(c) of Executive Order 13526
10 (50 U.S.C. 3161 note; relating to classified national
11 security information), or any successor order, the
12 Director of National Intelligence, or the Principal
13 Deputy Director of National Intelligence, as dele-
14 gated by the Director of National Intelligence, shall
15 notify the congressional intelligence committees and
16 the Archivist of the United States in writing of such
17 declassification, downgrading, or direction.

18 “(2) CONTENTS.—Each notification required by
19 paragraph (1) shall include a copy of the informa-
20 tion that has been, or has been directed to be, de-
21 classified or downgraded.

22 “(b) NOTIFICATION TO CONGRESS BY AGENCY
23 HEAD.—

24 “(1) IN GENERAL.—Immediately upon the de-
25 classification of information pursuant to section
26 3.1(d) of Executive Order 13526, or any successor

1 order, the head, or senior official, of a relevant ele-
 2 ment of the intelligence community shall notify the
 3 congressional intelligence committees, the Committee
 4 on Homeland Security and Governmental Affairs of
 5 the Senate, the Committee on Oversight and Gov-
 6 ernment Reform of the House of Representatives,
 7 and the Archivist of the United States in writing of
 8 such declassification.

9 “(2) CONTENTS.—Each notification required by
 10 paragraph (1) shall include a copy of the informa-
 11 tion that has been declassified.”.

12 (b) CLERICAL AMENDMENT.—The table of contents
 13 of the National Security Act of 1947 (50 U.S.C. 3001 et
 14 seq.) is amended by inserting after the item relating to
 15 section 805 the following:

“Sec. 806. Notification of certain declassifications.”.

16 **SEC. 308. NO POLICE, SUBPOENA, OR LAW ENFORCEMENT**
 17 **POWERS OR INTERNAL SECURITY FUNC-**
 18 **TIONS FOR DIRECTOR OF NATIONAL INTEL-**
 19 **LIGENCE.**

20 Section 102A of the National Security Act of 1947
 21 (50 U.S.C. 3024) is amended by adding at the end the
 22 following:

23 “(z) NO POLICE, SUBPOENA, OR LAW ENFORCE-
 24 MENT POWERS OR INTERNAL SECURITY FUNCTIONS.—
 25 The Director of National Intelligence shall have no police,

1 subpoena, or law enforcement powers or internal security
 2 functions.”.

3 **TITLE IV—MATTERS RELATING**
 4 **TO THE CENTRAL INTEL-**
 5 **LIGENCE AGENCY**

6 **SEC. 401. EXTENSION OF CENTRAL INTELLIGENCE AGENCY**

7 **AUTHORITY REGARDING UNMANNED AIR-**
 8 **CRAFT SYSTEMS.**

9 Section 15A(m) of the Central Intelligence Agency
 10 Act of 1949 (50 U.S.C. 3515a(m)) is amended by striking
 11 “December 31, 2027” and inserting “the date set forth
 12 in section 210G(j)(1) of the Homeland Security Act of
 13 2002 (6 U.S.C. 124n(j)(1))”.

14 **SEC. 402. HIGHER EDUCATION ACT OF 1965 SPECIAL RULE.**

15 Section 135 of the Higher Education Act of 1965 (20
 16 U.S.C. 1015d) is amended—

17 (1) by redesignating subsections (c) and (d) as
 18 subsections (d) and (e), respectively; and

19 (2) by inserting after subsection (b) the fol-
 20 lowing:

21 “(c) SPECIAL RULE.—With respect to a member of
 22 a qualifying Federal service who is an officer or employee
 23 of an element of the intelligence community, the term ‘per-
 24 manent duty station’, as used in this section, shall exclude

1 a permanent duty station that is within 50 miles of the
2 headquarters facility of such element.”.

3 **SEC. 403. MODIFICATION RELATING TO SECURITY PER-**
4 **SONNEL AT CERTAIN INSTALLATIONS.**

5 Section 15(a)(1)(D) of the Central Intelligence Agen-
6 cy Act of 1949 (50 U.S.C. 3515(a)(1)(D)) is amended by
7 inserting “or the National Reconnaissance Office” after
8 “Office of the Director of National Intelligence”.

9 **TITLE V—MATTERS RELATING**
10 **TO OTHER ELEMENTS OF THE**
11 **INTELLIGENCE COMMUNITY**

12 **SEC. 501. AUTHORITY OF NATIONAL SECURITY AGENCY TO**
13 **CORRELATE, EVALUATE, AND DISSEMINATE**
14 **CERTAIN INTELLIGENCE.**

15 The National Security Agency Act of 1959 (50
16 U.S.C. 3601 et seq.) is amended by adding at the end
17 the following:

18 **“SEC. 23. AUTHORITY TO CORRELATE, EVALUATE, AND DIS-**
19 **SEMINATE CERTAIN INTELLIGENCE.**

20 “The Director of the National Security Agency
21 may—

22 “(1) correlate and evaluate intelligence related
23 to national security; and

1 “(2) disseminate such intelligence to legislative
 2 and executive branch customers as the Director con-
 3 siders appropriate.”.

4 **SEC. 502. PROHIBITION ON AVAILABILITY OF FUNDS FOR**
 5 **RELOCATION OF OFFICE OF INTELLIGENCE**
 6 **AND ANALYSIS TO CERTAIN FACILITIES.**

7 None of the funds authorized to be appropriated by
 8 this Act or otherwise made available for fiscal year 2027
 9 for the National Intelligence Program (as defined in sec-
 10 tion 3 of the National Security Act of 1947 (50 U.S.C.
 11 3003)), may be obligated or expended to move or relocate
 12 the Office of Intelligence and Analysis of the Department
 13 of Homeland Security to any facility other than a facility
 14 owned by the Department of Homeland Security.

15 **SEC. 503. FUNDS FOR FOREIGN INTELLIGENCE ACTIVITIES**
 16 **CONDUCTED WITH AND BY THE NATIONAL**
 17 **RECONNAISSANCE OFFICE.**

18 (a) IN GENERAL.—Subchapter I of chapter 21 of title
 19 10, United States Code, is amended by inserting after sec-
 20 tion 421 the following:

21 **“§ 421a. Funds for foreign intelligence activities con-**
 22 **ducted with and by the National Recon-**
 23 **naissance Office**

24 “(a) USE OF APPROPRIATED FUNDS.—The Director
 25 of the National Reconnaissance Office may use appro-

1 priated funds available to the National Reconnaissance
2 Office for intelligence and communications purposes to
3 pay for the expenses of arrangements with foreign coun-
4 tries for intelligence activities conducted with and by the
5 National Reconnaissance Office.

6 “(b) USE OF FUNDS OTHER THAN APPROPRIATED
7 FUNDS.—The Director of the National Reconnaissance
8 Office may use funds other than appropriated funds to
9 pay for the expenses of arrangements with foreign coun-
10 tries for intelligence activities conducted with and by the
11 National Reconnaissance Office without regard for the
12 provisions of law relating to the expenditure of United
13 States Government funds, except that—

14 “(1) no such funds may be expended, in whole
15 or in part, by or for the benefit of the Department
16 of Defense for a purpose for which Congress had
17 previously denied funds;

18 “(2) proceeds from the sale of items or services
19 may be used only to purchase replacement items
20 similar to the items that are sold; and

21 “(3) the authority provided by this subsection
22 may not be used to acquire items or services for the
23 principal benefit of the United States.

24 “(c) REPORTS.—

1 “(1) USE OF APPROPRIATED FUNDS.—Any
 2 funds expended under the authority of subsection (a)
 3 shall be reported, pursuant to the provisions of title
 4 V of the National Security Act of 1947 (50 U.S.C.
 5 3091 et seq.), to—

6 “(A) the Select Committee on Intelligence,
 7 the Committee on Armed Services, and the
 8 Subcommittee on Defense of the Committee on
 9 Appropriations of the Senate; and

10 “(B) the Permanent Select Committee on
 11 Intelligence, the Committee on Armed Services,
 12 and the Subcommittee on Defense of the Com-
 13 mittee on Appropriations of the House of Rep-
 14 resentatives.

15 “(2) USE OF FUNDS OTHER THAN APPRO-
 16 PRIATED FUNDS.—Funds expended under the au-
 17 thority of subsection (b) shall be reported to the
 18 committees described in paragraph (1) pursuant to
 19 procedures jointly agreed upon by such committees
 20 and the Director of the National Reconnaissance Of-
 21 fice.”.

22 (b) CLERICAL AMENDMENT.—The table of sections
 23 at the beginning of such subchapter is amended by insert-
 24 ing after the item relating to section 421 the following:

“421a. Funds for foreign intelligence activities conducted with and by the Na-
 tional Reconnaissance Office.”.

1 **SEC. 504. MODIFICATION OF ANNUAL REPORT ON FEDERAL**
 2 **BUREAU OF INVESTIGATION CASE DATA.**

3 Section 512A(b)(6) of the National Security Act of
 4 1947 (50 U.S.C. 3111a(b)(6)) is amended by striking
 5 “country affiliation” and inserting “terrorist organiza-
 6 tion”.

7 **SEC. 505. ESTABLISHMENT OF OFFICE OF COUNTERINTEL-**
 8 **LIGENCE.**

9 Section 311 of title 31, United States Code, is
 10 amended—

11 (1) in subsection (a)—

12 (A) in paragraph (2), by striking “; and”
 13 and inserting a semicolon;

14 (B) by redesignating paragraph (3) as
 15 paragraph (4); and

16 (C) by inserting after paragraph (2), the
 17 following new paragraph (3):

18 “(3) identify and mitigate counterintelligence
 19 threats to the Department of the Treasury; and”;
 20 and

21 (2) by adding at the end the following new sub-
 22 section:

23 “(c) OFFICE OF COUNTERINTELLIGENCE.—There is
 24 established, within the Office of Intelligence and Analysis,
 25 the Office of Counterintelligence, which shall be respon-
 26 sible for implementing the policies and procedures across

1 the bureaus of the Department of the Treasury required
 2 to carry out the counterintelligence responsibilities de-
 3 scribed in subsection (a).”.

4 **SEC. 506. MODIFICATION OF RESPONSIBILITIES OF OFFICE**
 5 **OF INTELLIGENCE AND ANALYSIS.**

6 Section 201 of the Homeland Security Act of 2002
 7 (6 U.S.C. 121) is amended—

8 (1) in subsection (d)—

9 (A) in paragraph (1), by striking “in sup-
 10 port” and all that follows through “of the
 11 homeland.” and inserting “pertaining to foreign
 12 threats to the homeland, as determined by the
 13 Secretary.”;

14 (B) in paragraph (2)—

15 (i) by striking “terrorist attacks with-
 16 in” and inserting “foreign threats to”; and

17 (ii) by striking “attacks” each place it
 18 appears and inserting “threats”;

19 (C) in paragraph (3)(A), by striking “ter-
 20 rorist and other” and inserting “foreign”;

21 (D) in paragraph (6), by striking “ter-
 22 rorist attacks against” and inserting “foreign
 23 threats to”;

24 (E) by striking paragraphs (7), (17), and
 25 (23), and redesignating paragraphs (8), (9),

1 (10), (11), (12), (13), (14), (15), (16), (18),
 2 (19), (20), (21), and (22) as paragraphs (7),
 3 (8), (9), (10), (11), (12), (13), (14), (15), (16),
 4 (17), (18), (19), and (20), respectively;

5 (F) in paragraph (7), as so redesignated,
 6 by striking “threats of terrorism” and inserting
 7 “foreign threats”;

8 (G) in paragraph (9), as so redesignated,
 9 by striking “threats of terrorism in” and insert-
 10 ing “foreign threats to”; and

11 (H) in paragraph (12), as so redesignated,
 12 by striking “, other agencies” and all that fol-
 13 lows through “by the Department,”; and

14 (2) by adding at the end the following new sub-
 15 sections:

16 “(h) COLLECTION OF INTELLIGENCE AND INFORMA-
 17 TION.—In carrying out the duties and responsibilities of
 18 the Secretary pursuant to this section, the personnel of
 19 the Office of Intelligence and Analysis shall liaise and
 20 share intelligence and other information between federal
 21 agencies (including the components of the Department),
 22 State, local, or tribal governments, and the private sector.

23 “(i) PROHIBITION.—

1 “(1) UNITED STATES PERSON DEFINED.—In
 2 this subsection, the term ‘United States person’
 3 means—

4 “(A) a United States citizen;

5 “(B) an alien known by the Office of Intel-
 6 ligence and Analysis to be a permanent resident
 7 alien;

8 “(C) an unincorporated association sub-
 9 stantially composed of United States citizens or
 10 permanent resident aliens; or

11 “(D) a corporation incorporated in the
 12 United States, except for a corporation directed
 13 and controlled by 1 or more foreign govern-
 14 ments.

15 “(2) IN GENERAL.—Notwithstanding any other
 16 provision of law, the Office of Intelligence and Anal-
 17 ysis may not engage in the collection of information
 18 or intelligence targeting any United States person,
 19 or any clandestine collection.

20 “(j) INTELLIGENCE DEFINED.—In this section, the
 21 term ‘intelligence’ has the meaning given the terms foreign
 22 intelligence and counterintelligence, as defined paragraphs
 23 (2) and (3) of the National Security Act of 1947 (50
 24 U.S.C. 3003(2),(3)).”.

1 **SEC. 507. ROLE OF NATIONAL SECURITY AGENCY IN COL-**
2 **LECTION AND ANALYSIS OF SIGNALS INTEL-**
3 **LIGENCE.**

4 The National Security Agency Act of 1959 (50
5 U.S.C. 3601 et seq.) is amended by adding at the end
6 the following:

7 **“SEC. 23. SIGNALS INTELLIGENCE.**

8 “The Director of the National Security Agency
9 shall—

10 “(1) provide overall direction for and coordina-
11 tion of the collection and analysis of signals intel-
12 ligence by elements of the intelligence community
13 authorized to undertake such collection and analysis;
14 and

15 “(2) in coordination with other departments,
16 agencies, and elements of the United States Govern-
17 ment that are authorized to undertake such collec-
18 tion, ensure that—

19 “(A) the most effective use is made of re-
20 sources; and

21 “(B) appropriate account is taken of the
22 risks to the United States and those involved in
23 such collection.”.

1 **TITLE VI—GENERAL INTEL-**
 2 **LIGENCE COMMUNITY MAT-**
 3 **TERS**

4 **SEC. 601. AMENDMENTS TO PRESIDENTIAL APPOINTMENTS**
 5 **FOR INTELLIGENCE COMMUNITY POSITIONS.**

6 (a) APPOINTMENT OF DEPUTY DIRECTOR OF THE
 7 CENTRAL INTELLIGENCE AGENCY.—Section 104B(a) of
 8 the National Security Act of 1947 (50 U.S.C. 3037(a))
 9 is amended by inserting “, by and with the advice and
 10 consent of the Senate” after “President”.

11 (b) APPOINTMENT OF DEPUTY DIRECTOR OF THE
 12 NATIONAL SECURITY AGENCY.—Section 2 of the National
 13 Security Agency Act of 1959 (50 U.S.C. 3602) is amended
 14 by adding at the end the following:

15 “(c) There is a Deputy Director of the National Secu-
 16 rity Agency, who shall be appointed by the President, by
 17 and with the advice and consent of the Senate.”.

18 (c) APPOINTMENT OF DIRECTOR OF THE OFFICE OF
 19 INTELLIGENCE AND COUNTERINTELLIGENCE.—

20 (1) IN GENERAL.—Section 215(c) of the De-
 21 partment of Energy Organization Act (42 U.S.C.
 22 7144b(c)) is amended to read as follows:

23 “(c) DIRECTOR.—

24 “(1) APPOINTMENT.—The head of the Office
 25 shall be the Director of the Office of Intelligence and

1 Counterintelligence, who shall be appointed by the
2 President, by and with the advice and consent of the
3 Senate. The Director of the Office shall report di-
4 rectly to the Secretary.

5 “(2) TERM.—

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

8 “(B) REAPPOINTMENT.—The Director
9 shall be eligible for reappointment for 1 or more
10 terms.

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

12 “(A) be an employee in the Senior Execu-
13 tive Service, the Senior Intelligence Service, the
14 Senior National Intelligence Service, or any
15 other Service that the Secretary, in coordina-
16 tion with the Director of National Intelligence,
17 considers appropriate; and

18 “(B) have substantial expertise in matters
19 relating to the intelligence community, includ-
20 ing foreign intelligence and counterintel-
21 ligence.”.

22 (2) EFFECTIVE DATE.—The amendment made
23 by this section shall take effect on January 21,
24 2029.

1 (d) APPOINTMENT OF DIRECTOR OF THE NATIONAL
2 COUNTERTERRORISM CENTER.—Section 119(b)(1) of the
3 National Security Act of 1947 (50 U.S.C. 3056(b)(1)) is
4 amended by striking “President, by and with the advice
5 and consent of the Senate” and inserting “Director of Na-
6 tional Intelligence”.

7 (e) APPOINTMENT OF DIRECTOR THE NATIONAL
8 COUNTERINTELLIGENCE AND SECURITY CENTER.—Sec-
9 tion 902(a) of the Intelligence Authorization Act for Fiscal
10 Year 2003 (50 U.S.C. 3382(a)) is amended by striking
11 “President, by and with the advice and consent of the Sen-
12 ate” and inserting “Director of National Intelligence”.

13 (f) APPOINTMENT OF GENERAL COUNSEL OF THE
14 OFFICE OF THE DIRECTOR OF NATIONAL INTEL-
15 LIGENCE.—Section 103C(a) of the National Security Act
16 of 1947 (50 U.S.C. 3028(a)) is amended by striking “by
17 the President, by and with the advice and consent of the
18 Senate” and inserting “by the Director of National Intel-
19 ligence”.

20 (g) APPOINTMENT OF GENERAL COUNSEL OF THE
21 CENTRAL INTELLIGENCE AGENCY.—Section 20(a) of the
22 Central Intelligence Agency Act of 1949 (50 U.S.C.
23 3520(a)) is amended by striking “by the President, by and
24 with the advice and consent of the Senate” and inserting
25 “by the Director of the Central Intelligence Agency”.

1 **SEC. 602. PROCEDURES REGARDING DISSEMINATION OF**
2 **NONPUBLICLY AVAILABLE INFORMATION**
3 **CONCERNING UNITED STATES PERSONS.**

4 (a) PROCEDURES.—

5 (1) IN GENERAL.—Title V of the National Se-
6 curity Act of 1947 (50 U.S.C. 3091 et seq.) is
7 amended by adding at the end the following new sec-
8 tion:

9 **“SEC. 519. PROCEDURES REGARDING DISSEMINATION OF**
10 **NONPUBLICLY AVAILABLE INFORMATION**
11 **CONCERNING UNITED STATES PERSONS.**

12 “(a) PROCEDURES.—The head of each element of the
13 intelligence community, in consultation with the Director
14 of National Intelligence, shall develop and maintain proce-
15 dures for that element to respond to unmasking requests.

16 “(b) REQUIREMENTS.—The procedures required by
17 subsection (a) shall ensure, at a minimum, the following:

18 “(1) Each unmasking request submitted to a
19 disseminating element shall include, in writing—

20 “(A) information that identifies the dis-
21 seminated intelligence report containing the
22 United States person identifying information
23 requested;

24 “(B) the date the unmasking request was
25 submitted to the disseminating element;

1 “(C) the name, title, and organization of
2 the individual who submitted the unmasking re-
3 quest in an official capacity;

4 “(D) the name, title, and organization of
5 each individual who will receive the United
6 States person identifying information sought by
7 the unmasking request; and

8 “(E) a fact-based justification describing
9 why such United States person identifying in-
10 formation is required by each individual who
11 will receive the information to carry out the du-
12 ties of the individual.

13 “(2) An unmasking request may only be ap-
14 proved by the head of the disseminating element or
15 by officers or employees of such element to whom
16 the head has specifically delegated such authority.
17 When the disseminating element is not the origi-
18 nating element of the United States person identi-
19 fying information, the head of the disseminating ele-
20 ment shall obtain the concurrence of the head or
21 designee of the originating element before approving
22 the unmasking request.

23 “(3) The head of the disseminating element
24 shall retain records on all unmasking requests, in-

1 including the disposition of such requests, for not less
2 than 10 years.

3 “(4) The records described in paragraph (3)
4 shall include, with respect to each approved unmask-
5 ing request—

6 “(A) the name and title of the individual
7 of the disseminating element who approved the
8 request; and

9 “(B) the fact-based justification for the re-
10 quest.

11 “(5) The procedures shall include an exception
12 that—

13 “(A) allows for the immediate disclosure of
14 United States person identifying information in
15 the event of exigent circumstances or when a
16 delay would likely result in the significant loss
17 of intelligence; and

18 “(B) requires that promptly after such dis-
19 closure, the recipient of the United States per-
20 son identifying information make a written un-
21 masking request with respect to such informa-
22 tion.

23 “(6) If an unmasking request is made during a
24 period beginning on the date of a general election

1 for President and ending on the date on which such
2 President is inaugurated—

3 “(A) the documentation required by para-
4 graph (1) shall include whether—

5 “(i) the requesting entity knows or
6 reasonably believes that any United States
7 person identifying information sought is of
8 an individual who is a member of the tran-
9 sition team as identified by an apparent
10 successful candidate for the office of Presi-
11 dent or Vice President; or

12 “(ii) based on the intelligence report
13 to which the unmasking request pertains,
14 the disseminating element or the origi-
15 nating element knows or reasonably be-
16 lieves that any United States person iden-
17 tifying information sought is of an indi-
18 vidual who is a member of the transition
19 team as identified by an apparent success-
20 ful candidate for the office of President or
21 Vice President;

22 “(B) the approval made pursuant to para-
23 graph (2) of an unmasking request that con-
24 tains United States person identifying informa-
25 tion described in subparagraph (A) shall be

1 subject to the concurrence of the general coun-
2 sel of the disseminating element (or, in the ab-
3 sence of the general counsel, the principal dep-
4 uty general counsel, or, as applicable, the senior
5 Departmental legal officer supporting the dis-
6 seminating element) that the dissemination of
7 such United States person identifying informa-
8 tion is in accordance with the procedures re-
9 quired by subsection (a); and

10 “(C) consistent with due regard for the
11 protection from unauthorized disclosure of clas-
12 sified information relating to sensitive intel-
13 ligence sources and methods or other exception-
14 ally sensitive matters, the head of the dissemi-
15 nating element shall notify the chairmen and
16 ranking minority members of the congressional
17 intelligence committees, the Speaker and minor-
18 ity leader of the House of Representatives, and
19 the majority leader and minority leader of the
20 Senate of an approval described in subpara-
21 graph (B) not later than 14 days after the date
22 of such approval.

23 “(7) If an unmasking request concerns a nomi-
24 nee for or the holder of a Federal office, a member
25 of a transition team as identified by an eligible can-

1 didate for the office of the President, a Justice of
 2 the Supreme Court of the United States, or an indi-
 3 vidual nominated by the President to be a Justice of
 4 the Supreme Court of the United States, and such
 5 unmasking request is approved, the head of the dis-
 6 seminating element shall submit the documentation
 7 for the request to the congressional intelligence com-
 8 mittees not later than 14 days after the date of such
 9 approval.

10 “(c) ANNUAL REPORTS.—Not later than March 1 of
 11 each year, the head of each element of the intelligence
 12 community shall submit to the congressional intelligence
 13 committees a report documenting, with respect to the year
 14 covered by the report—

15 “(1) the total number of unmasking requests
 16 received by that element;

17 “(2) of such total number, the number of re-
 18 quests approved;

19 “(3) of such total number, the number of re-
 20 quests denied; and

21 “(4) for each number calculated under para-
 22 graphs (1) through (3), the number disaggregated
 23 by requesting entity.

24 “(d) CERTAIN PROCEDURES REGARDING CONGRES-
 25 SIONAL IDENTITY INFORMATION.—With respect to the

1 dissemination of congressional identity information, the
 2 head of each element of the intelligence community shall
 3 carry out this section in accordance with annex A of Intel-
 4 ligence Community Directive 112, or successor annex or
 5 directive.

6 “(e) EFFECT ON MINIMIZATION PROCEDURES.—The
 7 requirements of this section are in addition to—

8 “(1) any minimization procedures established
 9 under the Foreign Intelligence Surveillance Act of
 10 1978 (50 U.S.C. 1801 et seq.);

11 “(2) any procedures governing the collection,
 12 retention, or dissemination of information con-
 13 cerning United States persons established under Ex-
 14 ecutive Order 12333 (50 U.S.C. 3001 note; relating
 15 to United States intelligence activities) or successor
 16 order; and

17 “(3) any other provision of statute or Executive
 18 order the Director of National Intelligence considers
 19 relevant.

20 “(f) DEFINITIONS .—In this section:

21 “(1) APPARENT SUCCESSFUL CANDIDATE.—
 22 The term ‘apparent successful candidate’ means any
 23 apparent successful candidate for the office of Presi-
 24 dent or Vice President as determined pursuant to

1 the Presidential Transition Act of 1963 (3 U.S.C.
2 102 note).

3 “(2) CANDIDATE; FEDERAL OFFICE.—The
4 terms ‘candidate’ and ‘Federal office’ have the
5 meanings given those terms in section 301 of the
6 Federal Election Campaign Act of 1971 (52 U.S.C.
7 30101).

8 “(3) CONGRESSIONAL IDENTITY INFORMA-
9 TION.—The term ‘congressional identity information’
10 means information that identifies, by name or by in-
11 dividually identifying titles or characteristics—

12 “(A) any current Member of the Senate or
13 the House of Representatives;

14 “(B) any current staff officer for any Sen-
15 ator or Representative, whether paid or unpaid;
16 or

17 “(C) any current staff officer of any com-
18 mittee of the Senate or the House of Represent-
19 atives, whether paid or unpaid.

20 “(4) DISSEMINATING ELEMENT.—The term
21 ‘disseminating element’ means an element of the in-
22 telligence community that disseminated an intel-
23 ligence report subject to an unmasking request.

24 “(5) ELIGIBLE CANDIDATE.—The term ‘eligible
25 candidate’ has the meaning given that term in sec-

tion 3(h)(4) of the Presidential Transition Act of 1963 (3 U.S.C. 102 note).

“(6) ORIGINATING ELEMENT.—The term ‘originating element’ means an element of the intelligence community that originated information in a disseminated intelligence report subject to an unmasking request.

“(7) REQUESTING ENTITY.—The term ‘requesting entity’ means an entity of—

“(A) the United State Government; or

“(B) a State, local, Tribal, or territorial government.

“(8) UNITED STATES PERSON.—The term ‘United States person’ means a United States person as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) or section 3.5 of Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities).

“(9) UNITED STATES PERSON IDENTIFYING INFORMATION.—

“(A) IN GENERAL.—The term ‘United States person identifying information’ (commonly referred to as ‘United States Person Information’)—

1 “(i) means information that is reason-
 2 ably likely to identify one or more specific
 3 United States persons; and

4 “(ii) includes a single item of informa-
 5 tion and information that, when combined
 6 with other information, is reasonably likely
 7 to identify one or more specific United
 8 States persons.

9 “(B) DETERMINATION.—The determina-
 10 tion of whether information is reasonably likely
 11 to identify one or more specific United States
 12 persons may require assessment by a trained
 13 intelligence professional on a case-by-case basis.

14 “(10) UNMASKING REQUEST.—The term ‘un-
 15 masking request’ means a request to gain access to
 16 nonpublic United States person identifying informa-
 17 tion concerning a known unconsenting United States
 18 person that was omitted from a disseminated intel-
 19 ligence report by the originating element.”.

20 (2) CLERICAL AMENDMENT.—The table of con-
 21 tents preceding section 2 of such Act is amended by
 22 inserting after the item relating to section 518 the
 23 following new item:

“Sec. 519. Procedures regarding dissemination of nonpublicly available infor-
 mation concerning United States persons.”.

1 (b) DEVELOPMENT OF PROCEDURES.—The head of
 2 each element of the intelligence community shall develop
 3 the procedures required by section 519(a) of the National
 4 Security Act of 1947, as added by subsection (a)(1), by
 5 not later than 60 days after the date of the enactment
 6 of this Act.

7 (c) PUBLIC RELEASE.—Not later than 90 days after
 8 the date of the enactment of this Act, the Director of Na-
 9 tional Intelligence shall make publicly available the proce-
 10 dures for each element of the intelligence community re-
 11 quired by section 519(a) of the National Security Act of
 12 1947, as added by subsection (a)(1).

13 **SEC. 603. ANALYTIC STANDARDS FOR ALL-SOURCE INTEL-**
 14 **LIGENCE PRODUCTS.**

15 (a) IN GENERAL.—The National Security Act of
 16 1947 (50 U.S.C. 3001 et seq.) is amended by adding at
 17 the end the following:

18 **“SEC. 1115. ANALYTIC STANDARDS FOR ALL-SOURCE INTEL-**
 19 **LIGENCE PRODUCTS.**

20 “(a) DEFINITIONS.—In this section:

21 “(1) ALL-SOURCE INTELLIGENCE PRODUCT.—

22 The term ‘all-source intelligence product’—

23 “(A) means any intelligence product pub-
 24 lished by an element of the intelligence commu-
 25 nity using multiple types of intelligence for pur-

1 poses of providing an analytic assessment or
2 situational update; and

3 “(B) does not include a product containing
4 purely law enforcement information.

5 “(2) ASSUMPTION.—The term ‘assumption’
6 means a supposition used to frame or support an ar-
7 gument.

8 “(3) JUDGMENT.—The term ‘judgment’ means
9 a conclusion based on underlying intelligence infor-
10 mation, analysis, and assumptions.

11 “(b) ESTABLISHMENT.—

12 “(1) IN GENERAL.—The production of any all-
13 source intelligence product shall adhere to—

14 “(A) the analytic standards described in
15 subsection (c); and

16 “(B) any guidance or policy issued under
17 paragraph (2).

18 “(2) GUIDANCE AND POLICY.—The Director of
19 National Intelligence or any other head of an ele-
20 ment of the intelligence community may issue guid-
21 ance or policy that expands upon the standards de-
22 scribed in subsection (c) as such head considers ap-
23 propriate, except that any such guidance or policy
24 shall not contradict or otherwise circumvent such
25 standards.

1 “(c) ANALYTIC STANDARDS.—The standards de-
2 scribed in this subsection are the following:

3 “(1) OBJECTIVITY.—In producing any all-
4 source intelligence product, an analyst—

5 “(A) shall—

6 “(i) perform the analyst’s functions
7 with objectivity and with awareness of
8 their own assumptions and reasoning;

9 “(ii) employ reasoning techniques and
10 practical mechanisms that reveal and miti-
11 gate bias;

12 “(iii) be alert to influence by existing
13 analytic positions or judgments; and

14 “(iv) consider alternative perspectives
15 and contrary information; and

16 “(B) shall not be unduly constrained by
17 previous judgments when new developments in-
18 dicate a modification is necessary.

19 “(2) INDEPENDENT OF POLITICAL CONSIDER-
20 ATION.—Any all-source intelligence product shall not
21 be—

22 “(A) distorted by, or shaped for, advocacy
23 of a particular audience, agenda, or policy view-
24 point; or

1 “(B) influenced by the force of preference
2 for a particular policy.

3 “(3) TIMELY.—Any all-source intelligence prod-
4 uct shall be disseminated in time for the product to
5 be actionable by customers.

6 “(4) BASED ON ALL RELEVANT INFORMATION
7 AVAILABLE.—Any all-source intelligence product
8 shall be informed by all relevant information avail-
9 able.

10 “(5) ANALYTIC TRADECRAFT STANDARDS.—
11 Any all-source intelligence product shall adhere to
12 the following analytic tradecraft standards:

13 “(A) SOURCING.—Any all-source intel-
14 ligence product shall—

15 “(i) identify and properly describe the
16 quality and credibility of underlying
17 sources, data, and methodologies upon
18 which judgments are based; and

19 “(ii) use source descriptors in accord-
20 ance with sourcing guidance prescribed by
21 the Director of National Intelligence.

22 “(B) UNCERTAINTY.—Any all-source intel-
23 ligence product shall—

24 “(i) indicate and explain the basis for
25 the uncertainties associated with major

1 analytic judgments, specifically the likeli-
2 hood of occurrence of an event or develop-
3 ment, and the analyst's confidence in the
4 basis for the judgment;

5 “(ii) note causes of uncertainty, in-
6 cluding assumptions and gaps, and explain
7 how uncertainties affect analysis; and

8 “(iii) for expressions of likelihood or
9 probability, use one of the sets of terms
10 defined in Intelligence Community Direc-
11 tive 203.

12 “(C) DISTINGUISHING.—Any all-source in-
13 telligence product shall—

14 “(i) clearly distinguish statements
15 that convey underlying intelligence infor-
16 mation used in analysis from statements
17 that convey assumptions or judgments;

18 “(ii) state an assumption explicitly
19 when the assumption serves as the linchpin
20 of an argument or when the assumption
21 bridges key information gaps;

22 “(iii) explain the implications for
23 judgments if assumptions prove to be in-
24 correct; and

1 “(iv) as appropriate, identify indica-
2 tors that, if detected, would alter judg-
3 ments.

4 “(D) INCORPORATE ANALYSIS OF ALTER-
5 NATIVES.—Any all-source intelligence product
6 shall—

7 “(i) identify and assess plausible al-
8 ternative hypotheses;

9 “(ii) in discussing alternatives, ad-
10 dress factors such as associated assump-
11 tions, likelihood, or implications related to
12 United States interests; and

13 “(iii) identify indicators that, if de-
14 tected, would affect the likelihood of identi-
15 fied alternatives.

16 “(E) RELEVANCE.—Any all-source intel-
17 ligence product shall provide information and
18 insight on United States national security
19 issues.

20 “(F) ARGUMENTATION.—Any all-source
21 intelligence product shall—

22 “(i) present a clear main analytic
23 message up front;

24 “(ii) in the case of a product con-
25 taining multiple judgments, have a main

1 analytic message that is drawn collectively
2 from those judgments; and

3 “(iii) be effectively supported by rel-
4 evant intelligence information and coherent
5 reasoning.

6 “(G) ANALYTIC LINE.—Any all-source in-
7 telligence product shall—

8 “(i) state how its major judgments on
9 a topic are consistent with or represent a
10 change from major judgments in previously
11 published analysis, or that it represent ini-
12 tial coverage of a topic; and

13 “(ii) fully consider and bring to the
14 attention of customers significant dif-
15 ferences in analytic judgment, such as be-
16 tween two analytic elements of the intel-
17 ligence community.

18 “(H) ACCURACY.—Any all-source intel-
19 ligence product shall—

20 “(i) apply expertise and logic to make
21 the most accurate judgments and assess-
22 ments possible, based on the information
23 available and known information gaps; and

24 “(ii) express judgments as clearly and
25 precisely as possible, reducing ambiguity

1 by addressing the likelihood, timing, and
 2 nature of the outcome or development.

3 “(I) VISUALS.—Any all-source intelligence
 4 product shall incorporate effective visual infor-
 5 mation as appropriate. Any content of any all-
 6 source intelligence product depicted visually
 7 shall adhere to the analytic standards described
 8 in this subsection.

9 “(d) REQUIRED INFORMATION.—

10 “(1) IN GENERAL.—Except as provided in para-
 11 graph (2), any all-source intelligence product shall
 12 include a section dedicated to explaining the
 13 tradecraft related to the analytic tradecraft stand-
 14 ards described in subparagraphs (A), (B), (C), (D),
 15 and (G) of subsection (c)(5).

16 “(2) EXCEPTIONS.—The requirement of para-
 17 graph (1) shall not apply to—

18 “(A) any all source-intelligence product
 19 less than 300 words; or

20 “(B) any all-source intelligence product
 21 produced for the President’s Daily Brief.

22 “(e) TRACKING ADHERENCE TO ANALYTIC STAND-
 23 ARDS.—The Director of National Intelligence and each
 24 other head of an element of the intelligence community
 25 shall—

1 “(1) develop metrics for evaluating the perform-
 2 ance of their respective element in adhering to the
 3 analytic standards described in subsection (c); and

4 “(2) use such metrics to evaluate individual
 5 performance, develop analytic workforce training,
 6 and inform Congress on matters related to analytic
 7 performance.”.

8 (b) CLERICAL AMENDMENT.—The table of contents
 9 of such Act is amended by adding at the end the following:

“Sec. 1115. Analytic standards for all-source intelligence products.”.

10 **SEC. 604. LIMITATION ON USE OF INTELLIGENCE COMMU-**
 11 **NITY MANAGEMENT ACCOUNT FUNDS FOR**
 12 **CERTAIN ENTITIES.**

13 (a) IN GENERAL.—Title III of the National Security
 14 Act of 1947 (50 U.S.C. 3071 et seq.) is amended by add-
 15 ing at the end the following:

16 **“SEC. 314. LIMITATION ON USE OF INTELLIGENCE COMMU-**
 17 **NITY MANAGEMENT ACCOUNT FUNDS FOR**
 18 **CERTAIN ENTITIES.**

19 “Amounts appropriated for the Intelligence Commu-
 20 nity Management Account may not be obligated or ex-
 21 pended to provide financial or in-kind support for the pur-
 22 poses of analytic collaboration, including for any study,
 23 research, or assessment, to—

24 “(1) an entity that is described in section
 25 501(c)(3) of the Internal Revenue Code of 1986 and

1 exempt from taxation under section 501(a) of such
 2 Code, or otherwise describes itself as a think tank in
 3 any public document, that has received or expects to
 4 receive any financial or in-kind support from a for-
 5 eign government, except for a foreign government
 6 that is a member of the Five Eyes intelligence-shar-
 7 ing alliance; or

8 “(2) an entity that is organized for research or
 9 for engaging in advocacy in areas such as public pol-
 10 icy or political strategy that has received or expects
 11 to receive any financial or in-kind support from a
 12 government, or an entity affiliated with the military
 13 or intelligence services, of—

14 “(A) the People’s Republic of China;

15 “(B) the Russian Federation;

16 “(C) the Democratic People’s Republic of
 17 Korea;

18 “(D) the Islamic Republic of Iran;

19 “(E) the Bolivarian Republic of Venezuela;

20 or

21 “(F) the Republic of Cuba.”.

22 (b) CONFORMING AMENDMENT.—Section 103B(e) of
 23 such Act (50 U.S.C. 3027(e)) is amended by inserting
 24 “and subject to section 314” after “control of the Director
 25 of National Intelligence”.

1 (c) CLERICAL AMENDMENT.—The table of contents
 2 for such Act, in the matter preceding section 2 of such
 3 Act, is amended by inserting after the item relating to sec-
 4 tion 313 the following:

“Sec. 314. Limitation on use of Intelligence Community Management Account
 funds for certain entities.”.

5 **SEC. 605. BEN SASSE INTELLIGENCE COMMUNITY TECH-**
 6 **NOLOGY FELLOWSHIP PROGRAM.**

7 (a) IN GENERAL.—Title X of the National Security
 8 Act of 1947 (50 U.S.C. 3191 et seq.) is amended by in-
 9 serting after section 1002 the following:

10 **“SEC. 1003. BEN SASSE INTELLIGENCE COMMUNITY TECH-**
 11 **NOLOGY FELLOWSHIP PROGRAM.**

12 “(a) IN GENERAL.—There is established a program
 13 (in this section referred to as the ‘Program’) under which
 14 selected employees of the intelligence community may
 15 train at certain nongovernmental entities as technology
 16 fellows.

17 “(b) DESIGNATION.—The program shall be known as
 18 the ‘Ben Sasse Intelligence Community Technology Fel-
 19 lowship Program’.

20 “(c) AGREEMENTS.—

21 “(1) NONGOVERNMENTAL ENTITIES.—Each
 22 head of an element of the intelligence community de-
 23 scribed in paragraph (3) shall seek to enter into
 24 agreements with nongovernmental entities with expe-

1 rience in cutting-edge technology under which such
2 entities may host technology fellows under the Pro-
3 gram.

4 “(2) SELECTED EMPLOYEES.—For each em-
5 ployee of an element of the intelligence community
6 selected for participation in the Program in accord-
7 ance with subsection (e), the head of the element of
8 the intelligence community that selected the em-
9 ployee shall provide for a written agreement among
10 that element of the intelligence community, the non-
11 governmental entity concerned, and the employee.
12 The agreement shall—

13 “(A) require that the employee of the ele-
14 ment of the intelligence community, upon com-
15 pletion of the fellowship, serve in that element,
16 or elsewhere in the intelligence community if
17 approved by the head of the element that se-
18 lected the employee, for a period equal to twice
19 the length of the fellowship;

20 “(B) provide that if the employee of the
21 element of the intelligence community fails to
22 carry out the agreement, the employee shall be
23 liable to the United States for payment of all
24 expenses of the fellowship, unless that failure
25 was for good and sufficient reason, as deter-

1 mined by the head of the element that selected
2 the employee; and

3 “(C) contain language ensuring that the
4 employee of the element of the intelligence com-
5 munity does not improperly use information
6 that the employee knows relates to an acquisi-
7 tion or procurement of the element of the intel-
8 ligence community for the benefit or advantage
9 of the nongovernmental entity.

10 “(3) ELEMENTS DESCRIBED.—The elements of
11 the intelligence community described in this para-
12 graph are the following:

13 “(A) The Central Intelligence Agency.

14 “(B) The National Security Agency.

15 “(C) The National Geospatial-Intelligence
16 Agency.

17 “(D) The National Reconnaissance Office.

18 “(E) The Defense Intelligence Agency.

19 “(d) BOARD.—

20 “(1) IN GENERAL.—There is established a
21 board for the Program (in this section referred to as
22 the ‘Board’).

23 “(2) MEMBERSHIP.—The Board shall be com-
24 posed of the directors of science and technology, or

5 “(4) SELECTION CRITERIA.—The Board shall
6 establish selection criteria for the participation of
7 employees in the Program.

“(f) TERM.—An employee selected for participation in the Program may serve for one year as a technology fellow at a nongovernmental entity that has entered into an agreement under subsection (c)(1) with the head of the element of the intelligence community concerned.”.

“Sec. 1003. Ben Sasse Intelligence Community Technology Fellowship Program.”

20 SEC. 606. INTELLIGENCE COMMUNITY COUNTERINTEL-
21 LIGENCE OFFICE AT THE DEPARTMENT OF
22 COMMERCE.

•S 4615 PCS

1 (1) DEPARTMENT.—The term “Department”
2 means the Department of Commerce.

3 (2) SECRETARY.—The term “Secretary” means
4 the Secretary of Commerce.

5 (b) ESTABLISHMENT OF INTELLIGENCE COMMUNITY
6 COUNTERINTELLIGENCE OFFICE.—

7 (1) AGREEMENT WITH SECRETARY OF COM-
8 MERCE.—The Director of National Intelligence, act-
9 ing through the Director of the National Counter-
10 intelligence and Security Center, shall seek to enter
11 into an agreement with the Secretary under which
12 the Director of National Intelligence and the Sec-
13 retary shall establish within the Department, within
14 the Office of Secretary, an office, which shall be
15 known as the “Intelligence Community Counterintel-
16 ligence Office”, in accordance with this section.

17 (2) LOCATION.—The Intelligence Community
18 Counterintelligence Office established pursuant to
19 this section shall be physically located within the
20 headquarters of the Department and within reason-
21 able proximity to the offices of the leadership of the
22 Department.

23 (3) SECURITY.—The Director of the National
24 Counterintelligence and Security Center shall be re-
25 sponsible for the protection of classified information

1 and for the establishment and enforcement of all se-
2 curity-related controls within the Intelligence Com-
3 munity Counterintelligence Office.

4 (c) PERSONNEL.—

5 (1) DIRECTOR.—

6 (A) APPOINTMENT.—There shall be at the
7 head of the Intelligence Community Counter-
8 intelligence Office a Director who is appointed
9 by the Director of National Intelligence. The
10 Director of the Intelligence Community Coun-
11 terintelligence Office shall—

12 (i) be supervised and subject to per-
13 formance evaluations by the Director of
14 the National Counterintelligence and Secu-
15 rity Center, in consultation with the Sec-
16 retary;

17 (ii) be an employee of the intelligence
18 community with significant counterintel-
19 ligence experience; and

20 (iii) serve for a period of 3 years.

21 (B) RESPONSIBILITIES.—The Director of
22 the Intelligence Community Counterintelligence
23 Office shall carry out the following responsibil-
24 ities:

1 (i) Serving as the head of the Intel-
2 ligence Community Counterintelligence Of-
3 fice, with supervisory responsibility for the
4 Intelligence Community Counterintel-
5 ligence Office and any other personnel as-
6 signed to the Intelligence Community
7 Counterintelligence Office.

8 (ii) Advising the Secretary on counter-
9 intelligence and intelligence information.

10 (iii) Ensuring that counterintelligence
11 threat information and, as appropriate,
12 finished intelligence on topics related to
13 the functions of the Department, are pro-
14 vided to appropriate personnel of the de-
15 partment or agency without delay.

16 (iv) Ensuring critical intelligence rel-
17 evant to the Secretary is requested and
18 disseminated in a timely manner.

19 (v) Establishing, as appropriate,
20 mechanisms for collaboration through
21 which Department subject matter experts,
22 including those without security clearances,
23 can share information and expertise with
24 the intelligence community.

1 (vi) Correlating and evaluating coun-
2 terintelligence threats identified within in-
3 telligence community reporting, in coordi-
4 nation with the National Counterintel-
5 ligence and Security Center, and providing
6 appropriate dissemination of such intel-
7 ligence to officials of the Department with
8 a need-to-know.

9 (vii) Advising the Secretary on meth-
10 ods to improve the counterintelligence pos-
11 ture of the Department.

12 (viii) Where appropriate, supporting
13 the Department's leadership in engaging
14 with the National Security Council.

15 (ix) In coordination with the National
16 Counterintelligence and Security Center,
17 establishing counterintelligence partner-
18 ships to improve the counterintelligence de-
19 fense of the Department.

20 (2) DEPUTY DIRECTOR.—There shall be within
21 the Intelligence Community Counterintelligence Of-
22 fice a Deputy Director who is appointed by the Sec-
23 retary, in coordination with the Director of National
24 Intelligence. The Deputy Director shall—

(A) be supervised and subject to performance evaluations by the Secretary, in consultation with the Director of the National Counterintelligence and Security Center;

(B) be a current or former employee of the Department with significant experience within the Department; and

(C) serve at the pleasure of the Secretary.

(3) OTHER EMPLOYEES.—

(A) JOINT DUTY ASSIGNMENT.—There shall be within the Intelligence Community Counterintelligence Office such other employees as the Director of National Intelligence, in consultation with the Secretary, determines appropriate. Employment at the Intelligence Community Counterintelligence Office is an intelligence community joint duty assignment. A permanent change of station to the Intelligence Community Counterintelligence Office shall be for a period of not less than 2 years.

(B) SUPERVISION.—The Director of the Intelligence Community Counterintelligence Office shall be responsible for the supervision and management of employees assigned to the Intelligence Community Counterintelligence Office,

1 including employees assigned by program ele-
2 ments of the intelligence community and other
3 Federal departments and agencies, as appro-
4 priate.

5 (C) JOINT DUTY OR ASSIGNED PERSONNEL
6 REIMBURSEMENT.—The Director of National
7 Intelligence shall reimburse a program element
8 of the intelligence community or a Federal de-
9 partment or agency for any permanent change
10 of station employee assigned to the Intelligence
11 Community Counterintelligence Office from
12 amounts authorized to be appropriated for the
13 Office of the Director of National Intelligence.

14 (D) OPERATION UNDER AUTHORITY OF DI-
15 RECTOR OF NATIONAL INTELLIGENCE.—Em-
16 ployees assigned to the Intelligence Community
17 Counterintelligence Office under this paragraph
18 shall operate under the authorities of the Direc-
19 tor of National Intelligence for the duration of
20 their assignment or period of employment with-
21 in the Intelligence Community Counterintel-
22 ligence Office, except for temporary duty as-
23 signment employees.

24 (E) INCENTIVE PAY.—

1 (i) IN GENERAL.—An employee who
2 accepts employment at the Intelligence
3 Community Counterintelligence Office dur-
4 ing the 120-day period after the date of
5 the establishment of the Intelligence Com-
6 munity Counterintelligence Office shall re-
7 ceive an incentive payment, which shall be
8 payable by the Director of National Intel-
9 ligence, in an amount equal to 10 percent
10 of the base annual pay of the employee.
11 Such an employee who completes 2 years
12 of service in the Intelligence Community
13 Counterintelligence Office may receive an
14 incentive payment in an amount equal to
15 10 percent of the base annual pay of the
16 employee if the Director of the Intelligence
17 Community Counterintelligence Office de-
18 termines the performance of the employee
19 is exceptional.

20 (ii) ELIGIBILITY.—An employee is
21 only eligible for an incentive payment
22 under clause (i) if the employee enters into
23 an agreement with the Director of Na-
24 tional Intelligence to serve in the Intel-

1 ligence Community Counterintelligence Of-
2 fice for a period of at least 2 years.

3 (d) FUNDING.—To the extent and in such amounts
4 as specifically provided in advance in appropriations Acts
5 for the purposes detailed in this subsection, the Director
6 of National Intelligence may expend such sums as are au-
7 thorized within the National Intelligence Program of the
8 Office of the Director of National Intelligence for—

9 (1) the renovation, furnishing, and equipping of
10 a Federal building, as necessary, to meet the secu-
11 rity and operational requirements of the Intelligence
12 Community Counterintelligence Office;

13 (2) the provision of connectivity to the Intel-
14 ligence Community Counterintelligence Office to en-
15 able briefings, secure audio and video communica-
16 tions, and collaboration between employees of the
17 Department and the intelligence community at the
18 unclassified, secret, and top secret levels;

19 (3) the provision of other information tech-
20 nology systems and devices, such as computers,
21 printers, and phones, for use by employees of the In-
22 telligence Community Counterintelligence Office;

23 (4) the assignment of employees of the intel-
24 ligence community to support the operation of the

1 Intelligence Community Counterintelligence Office;
2 and

3 (5) the provision of other personal services nec-
4 essary for the operation of the Intelligence Commu-
5 nity Counterintelligence Office.

6 (e) DEADLINE FOR ESTABLISHMENT OF THE INTEL-
7 LIGENCE COMMUNITY COUNTERINTELLIGENCE OF-
8 FICE.—

9 (1) ESTABLISHMENT.—Not later than January
10 1, 2028, the Director of National Intelligence shall
11 seek to establish, in accordance with this section, the
12 Intelligence Community Counterintelligence Office
13 within the Department.

14 (2) REPORT.—Not later than 180 days after
15 the date of the enactment of this Act, the Director
16 of National Intelligence shall submit to the congres-
17 sional intelligence committees, the Committee on Ap-
18 propriations of the Senate, and the Committee on
19 Appropriations of the House of Representatives a re-
20 port on the plan to establish the Intelligence Com-
21 munity Counterintelligence Office required under
22 paragraph (1). Such report shall include the costs
23 and schedule associated with establishing the Intel-
24 ligence Community Counterintelligence Office.

1 **SEC. 607. COUNTERING HOSTILE FOREIGN CYBER ACTORS**
2 **AS A NATIONAL INTELLIGENCE PRIORITY.**

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

4 (1) In 2025, foreign malicious cybercriminal or-
5 ganizations, such as foreign scam centers that en-
6 gage in sophisticated investment fraud, cyber-en-
7 abled extortion activity, and impersonation-based
8 fraud, stole at least \$7,566,000,000 from Americans
9 according to the Federal Bureau of Investigation’s
10 Internet Crime Complaint Center, which has empha-
11 sized that these estimates are conservative and only
12 includes losses reported to the Federal Bureau of In-
13 vestigation.

14 (2) According to the Consumer Federation of
15 America, Americans are losing an estimated
16 \$119,000,000,000 each year to online scams.

17 (3) Investigative reporting, Federal indictments,
18 and sanctions designations issued by the Depart-
19 ment of the Treasury have revealed the extent to
20 which foreign malicious cybercriminal organizations
21 collaborate with foreign governments, illicit finance
22 actors, and foreign militia groups whose activities
23 present a threat to the economic and national secu-
24 rity of the United States.

25 (4) Foreign malicious cybercriminal organiza-
26 tions rely extensively on communications and finan-

1 cial services of United States companies, enabling
 2 the organizations' targeting of vulnerable Americans.

3 (5) Financial insecurity generated by foreign
 4 malicious cybercriminal organizations presents a
 5 counterintelligence threat to the United States intel-
 6 ligence community.

7 (b) SENSE OF CONGRESS.—

8 (1) IN GENERAL.—It is the sense of Congress
 9 that—

10 (A) foreign malicious cybercriminal organi-
 11 zations, and foreign affiliates associated with
 12 those organizations, constitute hostile foreign
 13 cyber actors and are valid targets for intel-
 14 ligence operations under existing intelligence
 15 authorities; and

16 (B) the Director of National Intelligence
 17 should treat collection, analysis, and disruption
 18 toward hostile foreign cyber actors as a national
 19 intelligence priority as part of the National In-
 20 telligence Priorities Framework.

21 (2) HOSTILE FOREIGN CYBER ACTORS.—The
 22 hostile foreign cyber actors described in paragraph
 23 (1) include, at a minimum, the following:

24 (A) Prince Group.

25 (B) Huione Group.

1 (C) L.Y.P. Group.

2 (D) Jin Bei Group.

3 (E) Funnall Technology Inc.

4 (F) TransAsia International holding Group
5 Thailand Company Limited.

6 (G) The Democratic Karen Benevolent
7 Army.

8 (H) HH Bank Cambodia PLC.

9 (c) REPORT.—

10 (1) IN GENERAL.—Not later than 180 days
11 after the date of the enactment of this Act, the Di-
12 rector of National Intelligence, in consultation with
13 the Director of the Federal Bureau of Investigation,
14 shall submit to Congress a report on hostile foreign
15 cyber actors, such as foreign scam centers.

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

18 (A) An identification of the individuals and
19 entities operating as hostile foreign cyber ac-
20 tors, including foreign scam centers, that pose
21 the most significant threat.

22 (B) An identification of the locations from
23 which the individuals and entities identified
24 under subparagraph (A) operate.

1 (C) A description of the infrastructure,
2 tactics, and techniques hostile foreign cyber ac-
3 tors, including foreign scam centers, commonly
4 use, including reliance on any products or serv-
5 ices subject to the jurisdiction of the United
6 States.

7 (D) A description of any relationships be-
8 tween the individuals and entities that operate
9 as hostile foreign cyber actors, including foreign
10 scam centers, and their governments or coun-
11 tries of origin that could impede the ability to
12 counter threats from such centers.

13 (E) An identification of communications
14 and financial services providers subject to the
15 jurisdiction of the United States that provide
16 enabling services to individuals and entities
17 identified under subparagraph (A).

18 (F) A description of any relationships that
19 the individuals and entities identified under
20 subparagraph (A) have with transnational orga-
21 nized crime groups.

22 (3) FORM; PUBLIC AVAILABILITY.—The report
23 required by paragraph (1) shall be submitted in un-
24 classified form, but may include a classified annex.

1 The unclassified form of the report shall be made
2 available to the public.

3 **SEC. 608. NOTIFICATION OF CRIMINAL REFERRALS RE-**
4 **GARDING CURRENT OR FORMER INTEL-**
5 **LIGENCE COMMUNITY EMPLOYEES.**

6 (a) IN GENERAL.—Title V of the National Security
7 Act of 1947 (50 U.S.C. 3091 et seq.) is amended by add-
8 ing at the end the following:

9 **“SEC. 519. NOTIFICATION OF CRIMINAL REFERRALS RE-**
10 **GARDING CURRENT OR FORMER INTEL-**
11 **LIGENCE COMMUNITY EMPLOYEES.**

12 “If an element of the intelligence community makes
13 a criminal referral to the Department of Justice regarding
14 a current or former employee of any element of the intel-
15 ligence community, the general counsel of the element of
16 the intelligence community that made the referral shall no-
17 tify the congressional intelligence committees of the refer-
18 ral on the date such referral is made and provide to the
19 congressional intelligence committees a summary of the
20 referral.”.

21 (b) CLERICAL AMENDMENT.—The table of contents
22 of the National Security Act of 1947 (50 U.S.C. 3001 et
23 seq.) is amended by inserting after the item relating to
24 section 518 the following:

“Sec. 519. Notification of criminal referrals regarding current or former intel-
ligence community employees.”.

1 **SEC. 609. MODIFICATION OF DEFINITIONS IN NATIONAL SE-**
2 **CURITY ACT OF 1947 AND SCOPE OF INTEL-**
3 **LIGENCE SHARING RESPONSIBILITIES OF DI-**
4 **RECTOR OF NATIONAL INTELLIGENCE.**

5 (a) DEFINITIONS.—Section 3 of the National Secu-
6 rity Act of 1947 (50 U.S.C. 3003) is amended—

7 (1) in paragraph (1), by striking “includes”
8 and inserting “means”; and

9 (2) in paragraph (5)—

10 (A) in the matter before subparagraph (A),
11 by striking “refer to all” and inserting
12 “means”;

13 (B) by amended subparagraph (B) to read
14 as follows:

15 “(B) involves foreign threats to the United
16 States, its people, property, or interests.”.

17 (b) SCOPE OF INTELLIGENCE SHARING RESPON-
18 SIBILITIES.—Section 102A(f)(1) of such Act (50 U.S.C.
19 3024(f)(1)) is amended, in the first sentence, by inserting
20 “, and other Federal agencies as the Director considers
21 appropriate,” after “community”.

22 **SEC. 610. PROHIBITION ON INTELLIGENCE COMMUNITY**
23 **USE OF ADVERSARY UNMANNED GROUND VE-**
24 **HICLES.**

25 (a) DEFINITIONS.—In this section:

1 (1) COVERED FOREIGN COUNTRY.—The term
2 “covered foreign country” means any of the fol-
3 lowing:

4 (A) The People’s Republic of China.

5 (B) The Russian Federation.

6 (C) The Islamic Republic of Iran.

7 (D) The Democratic People’s Republic of
8 Korea.

9 (2) COVERED FOREIGN ENTITY.—The term
10 “covered foreign entity” means an entity that is
11 domiciled in a covered foreign country, or subject to
12 influence or control by the government of a covered
13 foreign country as determined by the Secretary of
14 Homeland Security or the Secretary of Defense, and
15 any subsidiary or affiliate of such an entity.

16 (3) COVERED UNMANNED GROUND VEHICLE
17 SYSTEM.—The term “covered unmanned ground ve-
18 hicle system”—

19 (A) means a mechanical device that—

20 (i) is capable of locomotion, naviga-
21 tion, or movement on the ground; and

22 (ii) operates at a distance from one or
23 more operators or supervisors based on
24 commands or in response to sensor data,
25 or through any combination thereof; and

1 (B) includes—

2 (i) remote surveillance vehicles, auton-
3 omous patrol technologies, mobile robotics,
4 and humanoid robots; and

5 (ii) the vehicle, its payload, and any
6 external device used to control the vehicle.

7 (b) PROHIBITION ON PROCUREMENT OF COVERED
8 UNMANNED GROUND VEHICLE SYSTEMS FROM COVERED
9 FOREIGN ENTITIES.—

10 (1) IN GENERAL.—Except as provided under
11 paragraph (2), the head of an element of the intel-
12 ligence community may not procure any covered un-
13 manned ground vehicle system that is manufactured
14 or assembled by a covered foreign entity.

15 (2) EXEMPTION.—The heads of elements of the
16 intelligence community are exempt from the restric-
17 tion under paragraph (1) if the procurement is re-
18 quired in the national interest of the United States
19 and—

20 (A) is for the sole purposes of research,
21 evaluation, training, testing, or analysis for
22 electronic warfare, information warfare oper-
23 ations, cybersecurity, or development of un-
24 manned ground vehicle system or counter-un-
25 manned ground vehicle system technology;

(B) is for the sole purposes of conducting counterterrorism or counterintelligence activities, protective missions, or Federal criminal or national security investigations, including forensic examinations, or for electronic warfare, information warfare operations, cybersecurity, or development of an unmanned ground vehicle system or counter-unmanned ground vehicle technology; or

(C) is an unmanned ground vehicle system that, as procured or as modified after procurement but before operational use, can no longer transfer to, or download data from, a covered foreign entity and otherwise poses no national security cybersecurity risks as determined by the exempting official.

(c) PROHIBITION ON OPERATION OF COVERED UNMANNED GROUND VEHICLE SYSTEMS FROM COVERED FOREIGN ENTITIES.—

(1) PROHIBITION.—

(A) IN GENERAL.—Beginning on the date that is one year after the date of the enactment of this Act and except as provided in paragraph (2), no element of the intelligence community may operate a covered unmanned ground vehi-

1 cle system manufactured or assembled by a cov-
2 ered foreign entity.

3 (B) APPLICABILITY TO CONTRACTED
4 SERVICES.—The prohibition under subpara-
5 graph (A) applies to any covered unmanned
6 ground vehicle systems that are being used by
7 any element of the intelligence community
8 through the method of contracting for the serv-
9 ices of covered unmanned ground vehicle sys-
10 tems.

11 (2) EXEMPTION.—The heads of the elements of
12 the intelligence community are exempt from the re-
13 striction under paragraph (1) if the operation is re-
14 quired in the national interest of the United States
15 and—

16 (A) is for the sole purposes of research,
17 evaluation, training, testing, or analysis for
18 electronic warfare, information warfare oper-
19 ations, cybersecurity, or development of un-
20 manned ground vehicle system or counter-un-
21 manned ground vehicle system technology;

22 (B) is for the sole purposes of conducting
23 counterterrorism or counterintelligence activi-
24 ties, protective missions, or Federal criminal or
25 national security investigations, including foren-

sic examinations, or for electronic warfare, information warfare operations, cybersecurity, or development of an unmanned ground vehicle system or counter-unmanned ground vehicle system technology; or

(C) is an unmanned ground vehicle system that, as procured or as modified after procurement but before operational use, can no longer transfer to, or download data from, a covered foreign entity and otherwise poses no national security cybersecurity risks as determined by the exempting official.

(d) PROHIBITION ON USE OF FEDERAL FUNDS FOR PROCUREMENT AND OPERATION WITHIN THE INTELLIGENCE COMMUNITY OF COVERED UNMANNED GROUND VEHICLE SYSTEMS MANUFACTURED BY CERTAIN FOREIGN ENTITIES.—

(1) IN GENERAL.—Beginning on the date that is one year after the date of the enactment of this Act and except as provided in paragraph (2), no Federal funds awarded to an element of the intelligence community through a contract, grant, or cooperative agreement, or otherwise made available may be used—

1 (A) to procure a covered unmanned ground
2 vehicle system that is manufactured or assem-
3 bled by a covered foreign entity; or

4 (B) in connection with the operation of
5 such a robot or unmanned ground vehicle sys-
6 tem.

7 (2) EXEMPTION.—The heads of elements of the
8 intelligence community are exempt from the restric-
9 tion under paragraph (1) if the procurement or op-
10 eration is required in the national interest of the
11 United States and—

12 (A) is for the sole purposes of research,
13 evaluation, training, testing, or analysis for
14 electronic warfare, information warfare oper-
15 ations, cybersecurity, or development of un-
16 manned ground vehicle system or counter-un-
17 manned ground vehicle system technology;

18 (B) is for the sole purposes of conducting
19 counterterrorism or counterintelligence activi-
20 ties, protective missions, or Federal criminal or
21 national security investigations, including foren-
22 sic examinations, or for electronic warfare, in-
23 formation warfare operations, cybersecurity, or
24 development of an unmanned ground vehicle

1 system or counter-unmanned ground vehicle
2 system technology; or

3 (C) is an unmanned ground vehicle system
4 that, as procured or as modified after procure-
5 ment but before operational use, can no longer
6 transfer to, or download data from, a covered
7 foreign entity and otherwise poses no national
8 security cybersecurity risks as determined by
9 the exempting official.

10 **SEC. 611. CHINA-TAIWAN STRATEGIC WARNING TASK**
11 **FORCE.**

12 (a) ESTABLISHMENT.—Not later than 60 days after
13 the date of the enactment of this Act, the Director of Na-
14 tional Intelligence and the Undersecretary of Defense for
15 Intelligence and Security shall establish a task force to
16 be known as the China-Taiwan Strategic Warning Task
17 Force (referred to in this section as the “Task Force”)
18 to lead the efforts of the intelligence community with re-
19 spect to providing indications and warning of any military
20 aggression by the People’s Republic of China against Tai-
21 wan.

22 (b) OBJECTIVES.—The objectives of the Task Force
23 are the following:

24 (1) The synchronization of all intelligence com-
25 munity efforts related to China-Taiwan indications

1 and warning, including the generation of indicators
2 and development of collection requirements related
3 to such indicators.

4 (2) The coordination of analysis related to
5 China-Taiwan indications and warning and the de-
6 velopment of analytic methodologies for use across
7 the intelligence community in conducting analysis re-
8 lated to China-Taiwan indications and warning.

9 (3) The development and implementation of in-
10 formation technology solutions to synchronize the ac-
11 cess of the intelligence community to information re-
12 lating to indications and warning.

13 (c) MEMBERSHIP.—The Task Force shall be com-
14 posed of the following members (or their designees):

15 (1) The Director of National Intelligence.

16 (2) The Undersecretary of Defense for Intel-
17 ligence and Security.

18 (3) The Director of the Defense Intelligence
19 Agency.

20 (4) The Director of the Central Intelligence
21 Agency.

22 (5) The Director for Intelligence for the United
23 States Indo-Pacific Command.

24 (6) The Director of the National-Geospatial In-
25 telligence Agency.

1 (7) The Director of the National Security Agen-
2 cy.

3 (8) The Assistant Secretary of the Treasury for
4 Intelligence and Analysis.

5 (9) The Assistant Secretary of State for Intel-
6 ligence and Research.

7 (10) Such other heads of the elements of the in-
8 telligence community that the Director of National
9 Intelligence and the Undersecretary of Defense for
10 Intelligence and Security determine appropriate.

11 (d) LEADERSHIP; ORGANIZATION; MEETINGS.—

12 (1) CO-CHAIRS.—The Director of National In-
13 telligence (or a designee of the Director) and the
14 Undersecretary of Defense for Intelligence and Secu-
15 rity (or a designee of the Undersecretary) shall be
16 co-chairs of the Task Force.

17 (2) WORKING GROUPS.—The Task Force may
18 create subordinate working groups as determined by
19 the co-chairs.

20 (3) MEETING FREQUENCY.—The Task Force
21 shall meet regularly but not less than quarterly.

22 (e) STAFFING.—

23 (1) IN GENERAL.—The Task Force may hire
24 staff and create joint duty assignments assigned to

1 the Task Force. The Task Force may not exceed 25
2 full-time equivalent staff in total.

3 (2) AGENCY LIAISON.—Each member listed in
4 subsection (b) shall appoint a senior intelligence offi-
5 cer from the agency concerned to serve as a liaison
6 to the Task Force. Such liaison shall be responsible
7 for coordinating the participation and support of the
8 agency concerned to the Task Force.

9 (f) INITIAL REPORTS.—. Not later than 180 days
10 after the date of the enactment of this Act, the Task Force
11 shall submit to the congressional intelligence committees
12 and the congressional defense committees a report on the
13 status of the Task Force, including—

14 (1) a summary of the efforts of the intelligence
15 community with respect to China-Taiwan indications
16 and warning;

17 (2) a summary of efforts by the Task Force to
18 develop a common set of indicators and organize col-
19 lection efforts by the intelligence community against
20 such indicators;

21 (3) a description of the resources provided by
22 each Task Force member towards efforts with re-
23 spect to China-Taiwan indications and warning,
24 disaggregated by—

1 (A) dollars spent or planned to be spent
 2 during fiscal year 2027 ; and

3 (B) total full-time equivalent personnel;
 4 and

5 (4) recommendations to improve the collection
 6 and analysis of the intelligence community with re-
 7 spect to China-Taiwan indications and warning.

8 (g) SUNSET.—The provisions of this section shall ter-
 9 minate on the date that is 5 years after the date of the
 10 enactment of this Act.

11 **SEC. 612. LIMITATIONS RELATING TO CHINESE PRODUCTS**
 12 **AND SERVICES.**

13 (a) PROHIBITION ON USE BY INTELLIGENCE COM-
 14 MUNITY.—

15 (1) IN GENERAL.—Paragraph (1) of subsection
 16 (e) of section 6604 of the Intelligence Authorization
 17 Act for Fiscal Year 2026 (50 U.S.C. 3334m note;
 18 division F of Public Law 119–60) is amended to
 19 read as follows:

20 “(1) COVERED APPLICATION.—The term ‘cov-
 21 ered application’ means—

22 “(A) the DeepSeek application or any suc-
 23 cessor application or service; or

1 “(B) any product or service from any enti-
2 ty of the People’s Republic of China that is in-
3 cluded on—

4 “(i) the Entity List maintained by the
5 Bureau of Industry and Security of the
6 Department of Commerce;

7 “(ii) the list (sometimes known as the
8 ‘Non-SDN Chinese Military-Industrial
9 Complex Companies List’) maintained by
10 the Office of Foreign Assets Control of the
11 Department of the Treasury under Execu-
12 tive Order 13959, as amended by Execu-
13 tive Order 14032 (50 U.S.C. 1701 note;
14 relating to addressing the threat from se-
15 curities investments that finance certain
16 companies of the People’s Republic of
17 China), or any successor order; or

18 “(iii) the list of Chinese military com-
19 panies required under section 1260H of
20 the William M. (Mac) Thornberry National
21 Defense Authorization Act for Fiscal Year
22 2021 (10 U.S.C. 113 note; Public Law
23 116–283) and maintained by the Depart-
24 ment of Defense.”.

1 (2) CONFORMING AMENDMENT.—The heading
 2 for such section is amended by striking
 3 “**DEEPSEEK**” and inserting “**PRODUCTS AND**
 4 **SERVICES FROM PEOPLE’S REPUBLIC OF**
 5 **CHINA**”.

6 (b) LIMITATION ON PROCUREMENT BY INTEL-
 7 LIGENCE COMMUNITY.—Section 414 of the Intelligence
 8 Authorization Act for Fiscal Year 2022 (28 U.S.C. 532
 9 note; division X of Public Law 117–103) is amended—

10 (1) in the section heading, by striking “**BY**
 11 **FEDERAL BUREAU OF INVESTIGATION**”;

12 (2) in subsection (a)—

13 (A) in the matter before paragraph (1), by
 14 striking “Director of the Federal Bureau of In-
 15 vestigation” and inserting “head of an element
 16 of the intelligence community”;

17 (B) in paragraph (1), by striking “Federal
 18 Bureau of Investigation” and inserting “ele-
 19 ment”; and

20 (C) in paragraph (3), by striking “Director
 21 (or a designee of the Director)” and inserting
 22 “head”;

23 (3) in subsection (b), by striking “the Director
 24 (or a designee of the Director, as applicable) ap-
 25 proves a recommendation pursuant to subsection

1 (a)(3), the Director shall” and inserting “the head
 2 of an element of the intelligence community ap-
 3 proves a recommendation pursuant to subsection
 4 (a)(3), the head shall”;

5 (4) in subsection (c), by amending paragraph
 6 (2) to read as follows:

7 “(2) PEOPLE’S REPUBLIC OF CHINA PRODUCT
 8 OR SERVICE.—The term ‘People’s Republic of China
 9 product or service’ means—

10 “(A) an information or communication
 11 technology product manufactured in China,
 12 Hong Kong, or Macau and designed, developed,
 13 or maintained by a firm that is domiciled in
 14 China, Hong Kong, or Macau; or

15 “(B) an information or communication
 16 technology product or service provided or manu-
 17 factured by—

18 “(i) an entity that is fully or partially
 19 owned or controlled by, or otherwise con-
 20 nected to, the government of China; or

21 “(ii) an entity included on the list
 22 submitted by the Director of National In-
 23 telligence under section 6706(c) of the In-
 24 telligence Authorization Act for Fiscal

1 Year 2026 (division F of Public Law 119–
2 60; 139 Stat. 1648).”.

3 **SEC. 613. LIMITATION ON INTELLIGENCE COMMUNITY SUP-**
4 **PORT FOR OFFENSIVE CYBER OPERATIONS**
5 **CONDUCTED BY NONGOVERNMENTAL ENTI-**
6 **TIES.**

7 (a) IN GENERAL.—The National Security Act of
8 1947 (50 U.S.C. 3001 et seq.) is amended by adding at
9 the end the following:

10 **“SEC. 1115. LIMITATION ON INTELLIGENCE COMMUNITY**
11 **SUPPORT FOR OFFENSIVE CYBER OPER-**
12 **ATIONS CONDUCTED BY NONGOVERN-**
13 **MENTAL ENTITIES.**

14 “(a) IN GENERAL.—An element of the intelligence
15 community may not provide intelligence or support for an
16 offensive cyber operation conducted by a nongovernmental
17 entity, unless such an entity—

18 “(1) is conducting the offensive cyber operation
19 on behalf of such element and is operating under the
20 authorities and supervision of such element; or

21 “(2) is otherwise authorized by the President of
22 the United States to conduct the offensive cyber op-
23 eration.

24 “(b) DEFINITIONS.—In this section:

11 (b) CLERICAL AMENDMENT.—The table of contents
12 of such Act is amended by adding at the end the following:

13 SEC. 614. BIOLOGICAL INTELLIGENCE ACTIVITIES OF THE
14 INTELLIGENCE COMMUNITY.

18 "SEC. 124. BIOLOGICAL INTELLIGENCE ACTIVITIES OF THE
19 INTELLIGENCE COMMUNITY.

“(1) BIOLOGICAL DATA.—The term ‘biological data’ means multiomic information and other relevant information, including associated descriptors, derived from the structure, function, or process of a

1 biological system, that is measured, collected, or ag-
2 gregated for analysis, including information from
3 humans, animals, plants, or microbes.

4 “(2) BIOLOGICAL INTELLIGENCE.—The term
5 ‘biological intelligence’ includes the information col-
6 lected or disseminated by the intelligence community
7 concerning biological threats through genomic sur-
8 veillance, immunological monitoring, environmental
9 sampling, multiomic analysis, and other scientific
10 methodologies.

11 “(3) BIOLOGICAL THREAT.—The term ‘biologi-
12 cal threat’ includes any naturally occurring infec-
13 tious disease, engineered pathogen, toxin, or other
14 biological agent that poses a risk to human, animal,
15 or plant health or to the national security of the
16 United States.

17 “(b) DETERMINATION; DISSEMINATION.—The Direc-
18 tor of National Intelligence, in such coordination with the
19 Secretary of Defense as the Director considers appro-
20 priate, shall, consistent with applicable Federal law and
21 Executive Order 12333 (50 U.S.C. 3001 note; relating to
22 United States intelligence activities)—

23 “(1) determine which United States agencies
24 would benefit from receiving anonymized biological
25 data and biological intelligence in support of detec-

1 tion, characterization, and attribution of foreign bio-
2 logical threats; and

3 “(2) disseminate such anonymized biological
4 data and biological intelligence to agencies identified
5 under paragraph (1).

6 “(c) STANDARDS; DATABASES.—Not later than 1
7 year after the date of the enactment of this section, the
8 Director of National Intelligence, in such coordination
9 with the Secretary of Defense as the Director considers
10 appropriate, shall—

11 “(1) ensure standards for the collection and
12 data formats of anonymized biological data and bio-
13 logical intelligence are, to the extent possible, con-
14 sistent with standards used by other United States
15 agencies, including by—

16 “(A) providing for standardized data cat-
17 egorization and tagging of biological data;

18 “(B) considering standardized scientific
19 and laboratory equipment and data collection
20 methodologies; and

21 “(C) minimizing collection of any biological
22 data that is likely to contain biological or
23 genomic information specific to any United
24 States person, including any derived data that
25 is specific to any United States person; and

1 “(2) facilitate the establishment and mainte-
 2 nance of streamlined and unified accesses to data-
 3 bases of biological intelligence collected by the intel-
 4 ligence community or the Department of Defense.

5 “(d) PRIORITY.—In carrying out subsections (b) and
 6 (c), the Director of National Intelligence shall prioritize
 7 supporting capabilities, including the development of tech-
 8 nical tools, that enable the early detection, characteriza-
 9 tion, and attribution of naturally occurring, novel, or engi-
 10 neered pathogens that could threaten the United States.”.

11 (b) CLERICAL AMENDMENT.—The table of contents
 12 of such Act is amended by inserting after the item relating
 13 to section 123 the following:

“Sec. 124. Biological intelligence activities of the intelligence community.”.

14 **SEC. 615. PROHIBITION ON PARTICIPATION IN PREDICTION**
 15 **MARKETS.**

16 (a) IN GENERAL.—Title III of the National Security
 17 Act of 1947 (50 U.S.C. 3071 et seq.) is amended by in-
 18 serting after section 304 the following:

19 **“SEC. 304A. PROHIBITION ON PARTICIPATION IN PRE-**
 20 **DICTION MARKETS.**

21 “(a) IN GENERAL.—Except as may be necessary to
 22 conduct authorized intelligence activities, a covered indi-
 23 vidual may not participate in a prediction market on any
 24 topic relating to nonpublic information to which the cov-

1 ered individual has access by virtue of being a covered in-
 2 dividual, during—

3 “(1) the period during which the covered indi-
 4 vidual is employed or contracted by an element of
 5 the intelligence community; or

6 “(2) the two-year period beginning on the date
 7 on which the covered individual ceases to be em-
 8 ployed or contracted by such an element.

9 “(b) POLICY.—Not later than 45 days after the date
 10 of the enactment of this section, the Director of National
 11 Intelligence shall issue a policy implementing the prohibi-
 12 tion in subsection (a), including—

13 “(1) establishing appropriate penalties for vio-
 14 lating the prohibition; and

15 “(2) providing notice to all covered individuals.

16 “(c) DEFINITIONS.—In this section:

17 “(1) COVERED INDIVIDUAL.—The term ‘cov-
 18 ered individual’ means an employee or contractor, or
 19 a former employee or contractor, of an element of
 20 the intelligence community who holds a security
 21 clearance.

22 “(2) PREDICTION MARKET.—The term ‘pre-
 23 diction market’ means a platform, company, or serv-
 24 ice that allows agreements, contracts, transactions,
 25 or swaps between users over the outcome of non-fi-

1 nancial future events, such as sports, military ac-
 2 tions, and elections.”.

3 (b) CLERICAL AMENDMENT.—The table of contents
 4 of such Act is amended by inserting after the item relating
 5 to section 304 the following:

“Sec. 304A. Prohibition on participation in prediction markets.”.

6 **SEC. 616. REPEAL OF CERTAIN REPORT AND BRIEFING RE-**
 7 **QUIREMENTS.**

8 (a) OVERSIGHT OF FOREIGN INFLUENCE IN ACA-
 9 DEMIA.—Section 5713 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. 3369b)
 12 is repealed.

13 (b) REPORT ON EFFORTS TO ILLICITLY ACQUIRE
 14 SATELLITES AND RELATED ITEMS.—Section 1261 of the
 15 National Defense Authorization Act for Fiscal Year 2013
 16 (22 U.S.C. 2778 note; Public Law 112–239) is amended
 17 by striking subsection (e).

18 (c) MONITORING MINERAL INVESTMENTS UNDER
 19 BELT AND ROAD INITIATIVE OF THE PEOPLE’S REPUB-
 20 LIC OF CHINA.—Section 7003 of the Energy Act of 2020
 21 (50 U.S.C. 3372) is amended by striking subsection (d).

22 (d) BRIEFING ON PROTOCOLS FOR CERTAIN INTEL-
 23 LIGENCE COMMUNITY EMPLOYEES AND DEPENDENTS.—
 24 Section 605(g) of the Intelligence Authorization Act for

1 Fiscal Year 2022 (50 U.S.C. 3334k(g)) is amended by
2 striking paragraph (3).

3 (e) PROGRAM ON USE OF INTELLIGENCE RESOURCES
4 IN EFFORTS TO SANCTION FOREIGN OPIOID TRAF-
5 FICKERS.—Section 7231 of the Fentanyl Sanctions Act
6 (21 U.S.C. 2331) is amended—

7 (1) by striking subsection (c); and

8 (2) by redesignating subsection (d) as sub-
9 section (c).

10 (f) PERIODIC REPORT ON POSITIONS IN THE INTEL-
11 LIGENCE COMMUNITY THAT CAN BE CONDUCTED WITH-
12 OUT ACCESS TO CLASSIFIED INFORMATION, NETWORKS,
13 OR FACILITIES.—Section 6610 of the Damon Paul Nelson
14 and Matthew Young Pollard Intelligence Authorization
15 Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C.
16 3352e) is repealed.

17 (g) REVIEW OF SHARED INFORMATION TECHNOLOGY
18 SERVICES FOR PERSONNEL VETTING.—Section 7701 of
19 the Intelligence Authorization Act for Fiscal Year 2024
20 (division G of Public Law 118–31; 137 Stat. 1100) is re-
21 pealed.

22 (h) SUPPLY CHAIN AND COUNTERINTELLIGENCE
23 RISK MANAGEMENT TASK FORCE.—Section 6306 of the
24 Damon Paul Nelson and Matthew Young Pollard Intel-
25 ligence Authorization Act for Fiscal Years 2018, 2019,

1 and 2020 (50 U.S.C. 3370) is amended by striking sub-
2 section (e).

3 (i) REPORT ON BEST PRACTICES TO PROTECT PRI-
4 VACY, CIVIL LIBERTIES, AND CIVIL RIGHTS OF CHINESE
5 AMERICANS.—Section 620 of the Intelligence Authoriza-
6 tion Act for Fiscal Year 2021 (50 U.S.C. 3240) is re-
7 pealed.

8 (j) ENFORCEMENT OF CYBERSECURITY REQUIRE-
9 MENTS FOR NATIONAL SECURITY SYSTEMS; REPORT ON
10 EXEMPTIONS.—Section 6309(f) of the Intelligence Au-
11 thorization Act for Fiscal Year 2023 (44 U.S.C. 3557
12 note; division F of Public Law 117–263) is amended by
13 striking paragraph (3).

14 (k) REPORT ON COLLABORATION BETWEEN INTEL-
15 LIGENCE COMMUNITY AND DEPARTMENT OF COMMERCE
16 TO COUNTER FOREIGN COMMERCIAL THREATS.—Section
17 6514(b) of the Intelligence Authorization Act for Fiscal
18 Year 2023 (50 U.S.C. 3370b(b)) is amended by striking
19 paragraph (6).

20 (l) TIMELINESS STANDARD FOR RENDERING DETER-
21 MINATIONS OF TRUST FOR PERSONNEL VETTING; RE-
22 VIEWS.—Section 7702(a) of the Intelligence Authorization
23 Act for Fiscal Year 2024 (50 U.S.C. 3352h(a)) is amend-
24 ed by striking paragraph (2).

1 (m) BRIEFINGS ON STATUS OF INTELLIGENCE COM-
2 MUNITY INNOVATION UNIT.—Subsections (c) and (d) of
3 section 7502 of the Intelligence Authorization Act for Fis-
4 cal Year 2024 (Public Law 118–31; 137 Stat. 1082) are
5 repealed.

6 (n) ANNUAL TRAINING REQUIREMENT AND REPORT
7 REGARDING ANALYTIC STANDARDS.—Section 6312 of the
8 Intelligence Authorization Act for Fiscal Year 2023 (50
9 U.S.C. 3364 note; Public Law 117–263) is amended—

10 (1) by striking subsections (c) and (d); and
11 (2) by redesignating subsections (e) and (f) as
12 subsections (c) and (d), respectively.

13 (o) ANNUAL REPORTS REGARDING INTELLIGENCE
14 COMMUNITY PUBLIC-PRIVATE TALENT EXCHANGES.—
15 Section 6506 of the Intelligence Authorization Act for Fis-
16 cal Year 2025 (Public Law 118–159; 138 Stat. 2497) is
17 amended by striking subsection (e).

18 (p) SOFTWARE LICENSING.—Section 109 of the Na-
19 tional Security Act of 1947 (50 U.S.C. 3044) is amend-
20 ed—

21 (1) by striking subsection (c); and
22 (2) by redesignating subsection (d) as sub-
23 section (c).

1 (q) REVIEW AND UPDATE OF POSITION DESIGNA-
 2 TION GUIDANCE.—Section 7 of the SECRET Act of 2018
 3 (Public Law 115–173; 132 Stat. 1294) is amended—

4 (1) by striking subsection (c); and

5 (2) by redesignating subsection (d) as sub-
 6 section (c).

7 (r) REPORT ON INDEPENDENT STUDY ON ECONOMIC
 8 IMPACT OF MILITARY INVASION OF TAIWAN BY PEOPLE’S
 9 REPUBLIC OF CHINA.—Section 7407 of the Intelligence
 10 Authorization Act for Fiscal year 2024 (Public Law 118–
 11 31; 137 Stat. 1075) is amended—

12 (1) by striking subsection (c); and

13 (2) by redesignating subsection (d) as sub-
 14 section (c).

15 **SEC. 617. INTELLIGENCE COMMUNITY PERSONNEL TRAV-**
 16 **EL, ALLOWANCES, AND RELATED EXPENSES**
 17 **REGULATIONS.**

18 (a) CENTRAL INTELLIGENCE AGENCY.—Section 4 of
 19 the Central Intelligence Act of 1949 (50 U.S.C. 3505) is
 20 amended by adding at the end the following new sub-
 21 section:

22 “(c) BIENNIAL REVIEWS AND REPORTS.—Not later
 23 than September 30, 2027, and not less frequently than
 24 once every 2 years thereafter, the Director shall—

1 “(1) review the regulations covered by this sec-
2 tion; and

3 “(2) not later than 10 days after completing a
4 review under paragraph (1), submit to the congres-
5 sional intelligence committees the findings of the Di-
6 rector with respect to the review, including identi-
7 fication of any changes to the regulations or per-
8 sonnel coverage thereof that the Director determines
9 to be necessary for the performance of intelligence
10 functions.”.

11 (b) OFFICE OF DIRECTOR OF NATIONAL INTEL-
12 LIGENCE.—Section 102A of the National Security Act of
13 1947 (50 U.S.C. 3024) is amended by adding at the end
14 the following new subsection:

15 “(z) BIENNIAL REVIEWS AND REPORTS REGARDING
16 INTELLIGENCE COMMUNITY PERSONNEL TRAVEL, AL-
17 LOWANCES, AND RELATED EXPENSES REGULATIONS.—
18 Not later than September 30, 2027, and not less fre-
19 quently than once every 2 years thereafter, in order to re-
20 flect the requirements of the Office of the Director of Na-
21 tional Intelligence not taken into account in the formula-
22 tion of Government-wide travel procedures covered by this
23 section, the Director shall—

24 “(1) review such requirements; and

1 “(2) not later than 10 days after completing a
 2 review under paragraph (1), submit to the congres-
 3 sional intelligence committees the findings of the Di-
 4 rector with respect to the review, including any regu-
 5 lations that the Director determines to be necessary
 6 for the performance of intelligence functions.”.

7 **SEC. 618. PROHIBITION ON SENDING AND RECEIVING OB-**
 8 **JECTS USING ENTITIES OWNED OR CON-**
 9 **TROLLED BY PERSONS OR GOVERNMENTS OF**
 10 **CERTAIN COUNTRIES.**

11 (a) DEFINITION OF COVERED NATION.—In this sec-
 12 tion, the term “covered nation” has the meaning given
 13 such term in section 4872(f) of title 10, United States
 14 Code.

15 (b) IN GENERAL.—

16 (1) LIST REQUIRED.—Not later than 90 days
 17 after the date of the enactment of this Act, the Di-
 18 rector of National Intelligence, in coordination with
 19 the Director of the Central Intelligence Agency, shall
 20 develop a list of products, intellectual property, tech-
 21 nology, and any other objects that the Directors de-
 22 termine—

23 (A) affect the national security of the
 24 United States; and

1 (B) if acquired by a covered nation, would
2 pose a threat to the national security of the
3 United States.

4 (2) FORM.—The list required by paragraph (1)
5 may be in classified form.

6 (c) PROHIBITION.—Except as provided in subsection
7 (d), no element of the intelligence community may send
8 or receive any product, intellectual property, technology,
9 or other object as identified pursuant to subsection (b)
10 within the United States using an entity, including any
11 shipping company, that is owned or substantially con-
12 trolled by a person or a governmental entity domiciled in
13 a covered nation.

14 (d) WAIVER.—The head of an element of the intel-
15 ligence community—

16 (1) may waive the prohibition in subsection (c)
17 for the element on a case by case basis if the head
18 determines that in the particular case, sending or re-
19 ceiving any product, intellectual property, tech-
20 nology, or other object by an entity identified pursu-
21 ant to subsection (b) is necessary for the national
22 security of the United States; and

23 (2) not later than 3 days after issuing such
24 waiver, shall notify the Director of National Intel-
25 ligence of the waiver.

1 (e) NOTIFICATION.—Not later than 30 days after the
 2 head of an element of the intelligence community issues
 3 a waiver described in subsection (d), such head shall sub-
 4 mit to the congressional intelligence committees a written
 5 notice of the waiver, which shall include—

6 (1) a justification for the waiver, including the
 7 product, intellectual property, technology, or other
 8 object subject to the waiver; and

9 (2) a description of the national security threat
 10 mitigation measures implemented for permitting the
 11 activity that otherwise would be prohibited under
 12 subsection (c).

13 **SEC. 619. ENHANCING INTELLIGENCE COOPERATION IN**
 14 **THE INDO-PACIFIC REGION.**

15 (a) DEFINITION OF INTELLIGENCE COOPERATION.—
 16 In this section, the term “intelligence cooperation” means
 17 activities authorized under the provisions of law adminis-
 18 tered by the heads of the elements of the intelligence com-
 19 munity, including the collection, analysis, production, and
 20 dissemination of information, intelligence, and imagery.

21 (b) STATEMENT OF POLICY.—It is the policy of the
 22 United States to consider intelligence cooperation with al-
 23 lies and partners of the United States in the Indo-Pacific
 24 region a priority national security investment that will
 25 help deter aggression, reinforce regional stability, and re-

1 duce the risk of miscalculation, all of which will advance
2 the national security and economic prosperity of the
3 United States by helping to ensure a free and open Indo-
4 Pacific region.

5 (c) REQUIREMENTS.—

6 (1) IN GENERAL.—The Director of National In-
7 telligence shall, acting in close coordination with
8 such heads of elements of the intelligence community
9 as the Director considers relevant and the members
10 of the Five Eyes intelligence-sharing alliance, under-
11 take efforts to bolster and improve—

12 (A) the intelligence foundations of alliances
13 between the United States and Australia,
14 Japan, New Zealand, the Philippines, the Re-
15 public of Korea, and Thailand; and

16 (B) intelligence cooperation between the
17 United States and other regional partners, such
18 as India and Vietnam.

19 (2) PRIORITY AREAS FOR ENHANCED COOPERA-
20 TION.—Efforts undertaken pursuant to paragraph
21 (1) shall include efforts—

22 (A) to address the speed and complexity of
23 potential strategic and operational contingencies
24 in the Indo-Pacific region, including any sce-
25 narios involving adversarial efforts to limit the

1 freedom of navigation through critical maritime
2 chokepoints threaten supply chain security;

3 (B) relatedly, to ensure shared situational
4 awareness across the full spectrum of potential
5 contingencies, including military indications and
6 warnings;

7 (C) to enhance maritime, air, and space
8 domain awareness, with the goal of providing
9 decision advantage;

10 (D) to inform collective defense planning
11 and response by further integrating intelligence
12 cooperation into joint and combined operational
13 planning activities, exercises, and wargames fo-
14 cused on regional contingencies, including the
15 Rim of the Pacific;

16 (E) to encourage intelligence cooperation
17 with Taiwan, consistent with United States law
18 and policy; and

19 (F) to promote multilateral intelligence
20 sharing and collaboration among allies and
21 partners of the United States, such as through
22 the United States–Japan–Republic of Korea tri-
23 lateral mechanism and the United States–
24 Japan–Philippines trilateral mechanism.

1 **SEC. 620. INTELLIGENCE ACTIVITIES RELATED TO**
2 **UKRAINE.**

3 (a) STATEMENT OF POLICY.—

4 (1) IN GENERAL.—Section 3 of the Support for
5 the Sovereignty, Integrity, Democracy, and Eco-
6 nomic Stability of Ukraine Act of 2014 (22 U.S.C.
7 8902) is amended—

8 (A) in paragraph (16), by striking “; and”
9 and inserting a semicolon;

10 (B) in paragraph (17), by striking the pe-
11 riod at the end and inserting “; and”; and

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

13 “(18) to assist Ukraine in maintaining a cred-
14 ible defense and deterrence capability, including
15 through the provision of intelligence support, as a
16 means of advancing the national security of the
17 United States, regional stability, and the protection
18 of United States interests in Europe.”.

19 (2) DEFINITION.—Section 2 of such Act (22
20 U.S.C. 8901) is amended—

21 (A) by redesignating paragraphs (3) and
22 (4) as paragraphs (5) and (6), respectively; and

23 (B) by inserting after paragraph (2) the
24 following:

25 “(3) CREDIBLE DEFENSE AND DETERRENCE
26 CAPABILITY.—The term ‘credible defense and deter-

1 rence capability’ means the ability to defend against
2 and deter any credible conventional military threat
3 from the Russian Federation acting unilaterally or
4 in concert with partners, through the use of conven-
5 tional military means, possessed in sufficient quan-
6 tity, including weapons platforms and munitions,
7 and command, control, communication, intelligence,
8 surveillance, and reconnaissance capabilities.

9 “(4) INTELLIGENCE SUPPORT.—The term ‘in-
10 telligence support’ means activities authorized under
11 the provisions of law governing the heads of the ele-
12 ments of the intelligence community, including the
13 collection, analysis, production, and dissemination of
14 information, intelligence, and imagery.”.

15 (b) REQUIREMENT RELATING TO INTELLIGENCE
16 SUPPORT ABSENT AN ARMISTICE OR COMPREHENSIVE
17 POLITICAL SETTLEMENT.—Until Ukraine and the Rus-
18 sian Federation voluntarily and freely enter into an armi-
19 stice or comprehensive political settlement of the conflict,
20 the Director of National Intelligence, in coordination with
21 the Director of the Central Intelligence Agency, the Direc-
22 tor of the Defense Intelligence Agency, and the heads of
23 any other relevant element of the intelligence community,
24 shall continue to ensure the provision of intelligence sup-

1 port to the Government of Ukraine for purposes of ad-
2 vancing United States policy goals in Ukraine.

3 (c) PAUSES IN INTELLIGENCE SUPPORT.—

4 (1) IN GENERAL.—Intelligence support to
5 Ukraine required under this section shall not be sus-
6 pended or limited unless the Director of National In-
7 telligence, in coordination with the Director of the
8 Central Intelligence Agency and the Director of the
9 Defense Intelligence Agency, identifies a specific and
10 identifiable national security concern.

11 (2) NOTIFICATION.—Not later than 15 days
12 after making the decision to pause, terminate, re-
13 strict, or otherwise materially downgrade intelligence
14 support to Ukraine, the Director of National Intel-
15 ligence, in coordination with the heads of the ele-
16 ments of the intelligence community, shall submit to
17 the congressional intelligence committees a notifica-
18 tion that includes—

19 (A) a detailed description of the reason for
20 the pause, termination, restriction, or material
21 downgrade of intelligence support;

22 (B) the expected duration of the pause,
23 termination, restriction, or material downgrade;
24 and

1 (C) the anticipated impact of such decision
2 on the ability of Ukraine to conduct effective
3 military operations.

4 (3) FORM.—A notification submitted under
5 paragraph (2) shall be in unclassified form, but may
6 include an classified annex.

7 (d) REQUIREMENT RELATING TO INTELLIGENCE
8 SUPPORT IN THE EVENT OF ARMISTICE OR COMPREHEN-
9 SIVE POLITICAL SETTLEMENT.—

10 (1) IN GENERAL.—If Ukraine and the Russian
11 Federation voluntarily and freely enter into an armi-
12 stice or a comprehensive political settlement, the Di-
13 rector of National Intelligence, in coordination with
14 the heads of the other relevant elements of the intel-
15 ligence community, shall adjust the intelligence sup-
16 port to Ukraine to support implementation of the ar-
17 mistice or the comprehensive political settlement
18 and, consistent with the national security interests
19 of the United States, support building and sus-
20 taining the capacity of Ukraine to detect, deter, and
21 repel any future Russian attack against the territory
22 of Ukraine.

23 (2) REPORT ON MODIFICATIONS TO UNITED
24 STATES INTELLIGENCE SUPPORT.—Not later than
25 30 days after an armistice or a comprehensive polit-

1 ical settlement is entered into force, the Director of
2 the Central Intelligence Agency, in coordination with
3 the heads of the other relevant elements of the intel-
4 ligence community, including the Director of the De-
5 fense Intelligence Agency, the Director of the Na-
6 tional Security Agency, and the Director of the Na-
7 tional Geospatial-Intelligence Agency, shall submit to
8 the congressional intelligence committees a report
9 that includes—

10 (A) a description of the details of the armi-
11 stice or the comprehensive political settlement
12 of the conflict in Ukraine, including a descrip-
13 tion of the role of the intelligence community in
14 monitoring the adherence by the parties to spe-
15 cific elements of the agreement;

16 (B) an assessment of the vulnerabilities
17 that Ukraine will face under the terms of the
18 agreement and potential measures that the in-
19 telligence community or other parties could take
20 to help mitigate such vulnerabilities;

21 (C) a description of the modifications to
22 ongoing intelligence support the Director of the
23 Central Intelligence Agency has authorized in
24 light of the changed situation on the ground in
25 Ukraine in order to help build and sustain the

1 capacity of Ukraine to detect, deter, and repel
2 any future Russian attack against the territory
3 of Ukraine;

4 (D) an assessment of the implications of
5 the armistice or comprehensive political settle-
6 ment for the national security interests of the
7 United States in Europe, including the capacity
8 of the United States and the North Atlantic
9 Treaty Organization to deter future aggression
10 by the Russian Federation; and

11 (E) a description and assessment of any
12 cooperative arrangements that Ukraine has
13 with other countries, including member coun-
14 tries of the North Atlantic Treaty Organization,
15 that the intelligence community assesses would
16 contribute to deterring a future attack or act of
17 aggression by the Russian Federation aimed at
18 occupying or seizing the territory of Ukraine.

19 (3) FORM.—The report required by paragraph
20 (2) shall be submitted in unclassified form, but may
21 include a classified annex.

22 (4) EARLY WARNING.—The Director of Na-
23 tional Intelligence, in coordination with the heads of
24 any other relevant elements of the intelligence com-
25 munity, shall provide to Ukraine and member coun-

1 tries of the North Atlantic Treaty Organization in-
2 telligence and early warning to allow for an appro-
3 priate and timely response with respect to any po-
4 tential attack or act of aggression against Ukraine
5 by the Russian Federation.

6 (5) NOTIFICATION.—

7 (A) IN GENERAL.—The Director of Na-
8 tional Intelligence shall promptly notify each
9 Member of the congressional intelligence com-
10 mittees not later than 5 days after any intel-
11 ligence element provides Ukraine any intel-
12 ligence pursuant to paragraph (4).

13 (B) CONTENTS.—A notification submitted
14 pursuant to subparagraph (A) shall include—

15 (i) a description of the specific threat-
16 ened attack or act of aggression shared
17 with Ukraine;

18 (ii) the date on which the intelligence
19 was provided to Ukraine;

20 (iii) details of the channel through
21 which the intelligence was shared, includ-
22 ing the names and titles of the relevant in-
23 telligence community officers and Ukrain-
24 ian government officials;

1 (iv) the response of the Government
2 of Ukraine upon receiving the intelligence;

3 (v) an assessment produced by the
4 Defense Intelligence Agency, in coordina-
5 tion with other relevant elements of intel-
6 ligence community, as to what support
7 Ukraine might require in order to deter or
8 repel the threatened attack or act of ag-
9 gression; and

10 (vi) a summary of subsequent actions
11 that the Director of National Intelligence,
12 in coordination with the Director of the
13 Central Intelligence Agency, the Director
14 of the Defense Intelligence Agency, and
15 other heads of relevant elements of the in-
16 telligence community, directed be taken to
17 support Ukraine in defending against or
18 otherwise responding to the threatened at-
19 tack or act of aggression.

20 (C) FORM.—A notification submitted pur-
21 suant to subparagraph (A) shall be in unclassi-
22 fied form, but may include a classified annex.

23 (e) REQUIREMENT RELATING TO INTELLIGENCE

24 SUPPORT IN THE EVENT OF AN ARMED ATTACK ON

1 UKRAINE IN VIOLATION OF AN ARMISTICE OR COM-
2 PREHENSIVE POLITICAL SETTLEMENT.—

3 (1) IN GENERAL.—In the event of an armed at-
4 tack by the Russian Federation on Ukraine that vio-
5 lates an armistice or a comprehensive political settle-
6 ment, the Director of National Intelligence, in co-
7 ordination with the Director of the Central Intel-
8 ligence Agency, the Director of the Defense Intel-
9 ligence Agency, and the heads of other relevant ele-
10 ments of the intelligence community, shall imme-
11 diately resume the provision of intelligence support
12 to the Government of Ukraine at a level the Direc-
13 tors deem necessary to support military operations
14 of the Government of Ukraine that are intended, or
15 reasonably expected, to help the Armed Forces of
16 Ukraine defend or liberate the territory of Ukraine
17 and prevent such territory of Ukraine from being oc-
18 cupied or attacked by the Russian Federation.

19 (2) NOTIFICATION.—

20 (A) IN GENERAL.—The Director of Na-
21 tional Intelligence shall promptly notify the con-
22 gressional intelligence committees not later than
23 5 days after resuming intelligence support pur-
24 suant to paragraph (1).

1 (B) CONTENTS.—A notification submitted
2 pursuant to subparagraph (A) shall include—

3 (i) a description of the specific attack
4 or act of aggression against Ukraine;

5 (ii) a description of any intelligence
6 support that Ukraine requested from the
7 United States;

8 (iii) an assessment of the support that
9 Ukraine might require in order to deter or
10 repel the attack or act of aggression;

11 (iv) a description of any intelligence
12 support that the Director has authorized
13 to be provided to Ukraine; and

14 (v) a description of the response of
15 the Government of Ukraine upon receiving
16 the intelligence support.

17 (C) FORM.—A notification submitted pur-
18 suant to subparagraph (A) shall be in unclassi-
19 fied form, but may include a classified annex.

20 (3) SUNSET.—

21 (A) IN GENERAL.—The provision of intel-
22 ligence support for Ukraine under this sub-
23 section shall cease on the date that is 120 days
24 after the date on which the Government of
25 Ukraine and the Government of the Russian

1 Federation agree to reinstate the armistice or
2 comprehensive political settlement that was vio-
3 lated or a new armistice or comprehensive polit-
4 ical settlement is entered into force.

5 (B) RECOMMENCEMENT.—Upon the ces-
6 sation of the provision of intelligence support
7 under subparagraph (A), the Director of the
8 Central Intelligence Agency, in coordination
9 with the heads of any other relevant elements
10 of the intelligence community, shall resume the
11 provision of intelligence support to Ukraine
12 pursuant to subsection (d).

13 (f) DEFINITIONS.—In this section:

14 (1) ARMISTICE; COMPREHENSIVE POLITICAL
15 SETTLEMENT.—The terms “armistice” and “com-
16 prehensive political settlement” mean a formal writ-
17 ten agreement between the Government of Ukraine
18 and the Government of the Russian Federation that
19 has the effect of permanently ending the armed con-
20 flict between both nations.

21 (2) INTELLIGENCE SUPPORT.—The term “intel-
22 ligence support” means activities authorized under
23 the provisions of law governing the heads of the ele-
24 ments of the intelligence community, including the

1 collection, analysis, production, and dissemination of
2 information, intelligence, and imagery.

3 (3) SPECIFIC AND IDENTIFIABLE NATIONAL SE-
4 CURITY CONCERN.—The term “specific and identifi-
5 able national security concern” includes the fol-
6 lowing:

7 (A) Credible intelligence that an element of
8 the Government of Ukraine has been com-
9 promised by the Russian Federation or another
10 foreign adversary.

11 (B) Protection of sources and methods.

12 (C) A voluntary request from the Govern-
13 ment of Ukraine to pause intelligence support.

14 (D) Credible intelligence that an element
15 of the Government of Ukraine receiving United
16 States intelligence support engaged in a pattern
17 of human rights violations, atrocities, or viola-
18 tions of the law of armed conflict.

19 (4) TERRITORY OF UKRAINE.—The term “terri-
20 tory of Ukraine” means all territory internationally
21 recognized to be the sovereign territory of Ukraine
22 on February 19, 2014, including Crimea and the
23 territory that the Russian Federation claims to have
24 annexed in Kherson and Zaporizhzhia.

1 **SEC. 621. REQUIREMENTS RELATING TO INTELLIGENCE**
2 **SHARING WITH COUNTRIES OF SIGNIFICANT**
3 **CONCERN TO THE UNITED STATES.**

4 Section 102A(j) of the National Security Act of 1947
5 (50 U.S.C. 3024(j)) is amended—

6 (1) by striking “Under the direction” and in-
7 serting the following:

8 “(1) IN GENERAL.—Under the direction”; and

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

10 “(2) NOTIFICATION REQUIRED.—

11 “(A) IN GENERAL.—Not later than 48
12 hours after a decision to pause, terminate, or
13 otherwise restrict or materially downgrade intel-
14 ligence support or intelligence activities (as de-
15 fined in section 501(f)), including information,
16 intelligence, and imagery collection authorized
17 under Executive Order 12333 (50 U.S.C. 3001
18 note; relating to United States intelligence ac-
19 tivities), to the government of a country of sig-
20 nificant concern to the United States, the Di-
21 rector of National Intelligence shall submit to
22 the congressional intelligence committees a noti-
23 fication of such decision.

24 “(B) ELEMENTS.—The notification re-
25 quired in subsection (a) shall include—

1 “(i) a detailed description of the rea-
 2 son for the pause, termination, restriction,
 3 or material downgrade of intelligence sup-
 4 port;

5 “(ii) a description of the change in in-
 6 telligence sharing;

7 “(iii) the categories of information af-
 8 fected;

9 “(iv) the expected duration of the
 10 pause, termination, restriction, or material
 11 downgrade; and

12 “(v) the anticipated impact of such
 13 decision on regional security and the na-
 14 tional security objectives of the United
 15 States.

16 “(C) COUNTRY OF SIGNIFICANT CONCERN
 17 TO THE UNITED STATES DEFINED.—In this
 18 subsection, the term ‘country of significant con-
 19 cern to the United States’ means—

20 “(i) Israel;

21 “(ii) Ukraine;

22 “(iii) Taiwan; and

23 “(iv) any other country designated as
 24 such by the President.”.

1 **SEC. 622. UNITED STATES-ISRAEL INTELLIGENCE SHARING**
2 **ENHANCEMENT.**

3 (a) STATEMENT OF POLICY.—It is the policy of the
4 United States—

5 (1) to maintain and strengthen the strategic se-
6 curity partnership with Israel as a means of advanc-
7 ing the national defense of the United States, re-
8 gional stability, and the protection of United States
9 personnel and interests in the Middle East;

10 (2) to enhance intelligence collaboration
11 through robust intelligence sharing and analytic
12 partnership with Israel to counter terrorism, pro-
13 liferation networks, cyber threats, state and nonstate
14 aggressors, terror financing, sanctions evasion, and
15 other transnational security challenges that threaten
16 both Israel and the United States;

17 (3) to deter and counter destabilizing activities
18 by the Government of Iran and Iran-aligned state
19 and nonstate actors that threaten Israel, United
20 States forces, and regional partners;

21 (4) to ensure that security assistance and de-
22 fense cooperation are structured to help Israel main-
23 tain its qualitative military edge, consistent with
24 United States law and broader regional security con-
25 siderations;

1 (5) to encourage and support the expansion of
2 regional security architectures that include Israel
3 and willing regional partners, with a focus on inte-
4 grated air and missile defense, maritime security,
5 early warning systems, and intelligence-sharing
6 frameworks; and

7 (6) to leverage security coordination with Israel
8 to enhance force protection, early warning, and crisis
9 response capabilities for United States military and
10 diplomatic personnel in the region.

11 (b) SENSE OF CONGRESS.—It is the sense of Con-
12 gress that—

13 (1) Israel remains a critical United States secu-
14 rity partner whose defense and intelligence capabili-
15 ties provide a strategic advantage that contributes to
16 enhanced operational effectiveness and technological
17 superiority;

18 (2) timely and actionable intelligence sharing
19 between the United States and Israel has saved
20 United States personnel and property in the region
21 and should remain a central pillar of the bilateral se-
22 curity relationship;

23 (3) the evolving threat environment in the Mid-
24 dle East—including missile proliferation, unmanned
25 systems, cyber operations, terror financing, and

1 proxy warfare—requires sustained and adaptive co-
 2 operation between the United States and Israel;

3 (4) the United States-Israel security partner-
 4 ship has historically benefitted from bipartisan sup-
 5 port, which strengthens the partnership’s credibility,
 6 durability, and deterrent value; and

7 (5) expanding normalization and practical secu-
 8 rity cooperation between Israel and regional states
 9 can serve as a force multiplier for collective deter-
 10 rence and integrated defense.

11 (c) REQUIREMENTS RELATING TO INTELLIGENCE

12 SHARING.—

13 (1) IN GENERAL.—Title XI of the National Se-
 14 curity Act of 1947 (50 U.S.C. 3231 et seq.) is
 15 amended by adding at the end the following:

16 **“SEC. 1115. REQUIREMENTS RELATING TO INTELLIGENCE**
 17 **SHARING.**

18 **“(a) INTELLIGENCE SHARING WITH ISRAEL.—**

19 **“(1) IN GENERAL.—**The President, acting
 20 through the Director of National Intelligence and, as
 21 necessary, the Secretary of Defense, shall, subject to
 22 applicable law and the protection of intelligence
 23 sources and methods, expand and enhance intel-
 24 ligence sharing with the Government of Israel.

1 “(2) SCOPE OF INTELLIGENCE SHARING.—In-
2 telligence sharing carried out under this subsection
3 shall include the sharing of information relating to
4 cybersecurity threats, terrorism, sanctions evasion,
5 plans and intentions of state and nonstate actors,
6 adversarial technology proliferation, missile threats,
7 unmanned aerial systems, cruise missiles, ballistic
8 missiles, air and space domain awareness, and other
9 aerial threats relevant to the defense of Israel,
10 United States forces and interests in the region, and
11 regional security partners.

12 “(3) LIMITATIONS ON REDUCTION OF INTEL-
13 LIGENCE SHARING.—

14 “(A) IN GENERAL.—Intelligence sharing
15 and related security information exchanges with
16 the Government of Israel shall not be sus-
17 pended, reduced, or otherwise materially limited
18 except on the basis of a specific and identifiable
19 national security concern determined by the
20 President, such as the protection of intelligence
21 sources and methods, counterintelligence risk,
22 or another significant security consideration.

23 “(B) DOCUMENTATION REQUIREMENT.—
24 The President shall document any determina-
25 tion to suspend, reduce, or otherwise materially

1 limit intelligence sharing or related security in-
2 formation exchanges with the Government of
3 Israel, including a description of the national
4 security rationale supporting the change.

5 “(4) CONGRESSIONAL NOTIFICATION.—

6 “(A) IN GENERAL.—Not later than 15
7 days after the date of any decision to materially
8 increase, suspend, reduce, or otherwise alter in-
9 telligence sharing or related security informa-
10 tion exchanges with the Government of Israel,
11 the President shall notify the congressional in-
12 telligence committees of such decision.

13 “(B) ELEMENTS.—Each notification re-
14 quired by subparagraph (A) shall include the
15 following:

16 “(i) A description of the change in in-
17 telligence sharing or security information
18 exchange.

19 “(ii) The categories of information af-
20 fected.

21 “(iii) The national security objectives
22 served by the change.

23 “(iv) In the case of a suspension or
24 reduction, the specific national security
25 concern supporting the change.

1 “(v) An assessment of the anticipated
2 impact on regional security, United States
3 forces, and integrated air and missile de-
4 fense cooperation.

5 “(b) INTELLIGENCE SHARING AND ANALYTIC CO-
6 OPERATION WITH ABRAHAM ACCORDS COUNTRIES.—

7 “(1) IN GENERAL.—The President, acting
8 through the Director of National Intelligence and, as
9 necessary, the Secretary of Defense, shall, consistent
10 with applicable law and security agreements, expand
11 and enhance intelligence sharing and analytic co-
12 operation with countries that have normalized rela-
13 tions with Israel pursuant to the Abraham Accords
14 (as defined in section 64(k) of the State Department
15 Basic Authorities Act of 1956 (22 U.S.C. 2735a(k))
16 in order to strengthen regional security integration.

17 “(2) PRIORITY AREAS.—In carrying out para-
18 graph (1), the President shall prioritize the sharing
19 of appropriate intelligence and information relating
20 to—

21 “(A) counterterrorism threats and net-
22 works, including state and nonstate aggressors,
23 and terror financing;

24 “(B) cybersecurity threats, vulnerabilities,
25 and defensive best practices;

1 “(C) air and missile defense early warning
2 and threat tracking;

3 “(D) geospatial, overhead, and other imag-
4 ing intelligence relevant to shared security con-
5 cerns; and

6 “(E) maritime security threats, including
7 threats to freedom of navigation, commercial
8 shipping, sanctions evasion, and regional mari-
9 time stability.

10 “(3) SAFEGUARDS.—

11 “(A) ADOPTION OF GUIDELINES.—The Di-
12 rector of National Intelligence, in coordination
13 with the Secretary of Defense, shall adopt
14 guidelines for intelligence sharing and analytic
15 cooperation carried out under this subsection
16 that ensure appropriate safeguards—

17 “(i) to protect intelligence sources and
18 methods; and

19 “(ii) to ensure that recipients main-
20 tain adequate security protections con-
21 sistent with United States requirements.

22 “(B) RESTRICTIONS ON ACCESS.—If the
23 Director of National Intelligence determines
24 that a recipient of intelligence sharing or ana-
25 lytic cooperation carried out under this sub-

1 section has any intelligence, defense, or techno-
2 logical information sharing relationship with an
3 adversarial nation, the Director shall restrict all
4 access of such recipient to such intelligence
5 sharing and analytic cooperation.

6 “(c) REPORT REQUIRED.—

7 “(1) IN GENERAL.—Not later than 180 days
8 after the date of the enactment of this section, and
9 annually thereafter for 5 years, the President shall
10 submit to the appropriate congressional committees
11 a report on the status of United States intelligence
12 sharing with the Government Israel and, as appro-
13 priate, regional partners.

14 “(2) MATTERS TO BE INCLUDED.—Each report
15 required by paragraph (1) shall include, to the ex-
16 tent consistent with the protection of intelligence
17 sources and methods, the following:

18 “(A) A description of the categories of in-
19 telligence and security information shared by
20 the United States Government with the Govern-
21 ment of Israel.

22 “(B) An assessment of progress toward
23 seamlessly integrating Israel into regional air
24 and missile defense and early warning architec-
25 tures with partner countries, including those

1 that have normalized relations with Israel pur-
2 suant to the Abraham Accords.

3 “(C) A description of how such intelligence
4 sharing has contributed, if at all, to—

5 “(i) improved detection, tracking,
6 warning, interception, or deterrence of aer-
7 ial threats, including missiles and un-
8 manned systems, for Israel, United States
9 forces, or regional partners; and

10 “(ii) the overall stability and coordina-
11 tion of security in the region.

12 “(D) An assessment of progress in improv-
13 ing interoperability among technology networks
14 of the United States, Israel, and partner coun-
15 tries.

16 “(E) A description of efforts to secure
17 technology networks and data from cyber
18 threats and unauthorized access.

19 “(F) An identification of any legal, policy,
20 technical, counterintelligence, or security bar-
21 riers limiting deeper intelligence integration, in-
22 cluding risks to intelligence sources and meth-
23 ods.

24 “(G) A summary of any significant in-
25 creases or reductions in intelligence sharing

1 during the reporting period and the national se-
 2 curity rationale for such changes.

3 “(3) FORM.—Each report required by para-
 4 graph (1) report shall be submitted in unclassified
 5 form but may include a classified annex.

6 “(4) APPROPRIATE CONGRESSIONAL COMMIT-
 7 TEES DEFINED.—In this subsection, the term ‘ap-
 8 propriate congressional committees’ means—

9 “(A) the congressional intelligence commit-
 10 tees; and

11 “(B) to the extent Department of Defense
 12 information is implicated, the congressional de-
 13 fense committees (as defined in section 101(a)
 14 of title 10, United States Code).”.

15 (2) CLERICAL AMENDMENT.—The table of con-
 16 tents for such Act is amended by adding at the end
 17 the following:

“Sec. 1115. Requirements relating to intelligence sharing.”.

18 **TITLE VII—ARTIFICIAL INTEL-**
 19 **LIGENCE MATTERS RELATING**
 20 **TO THE INTELLIGENCE COM-**
 21 **MUNITY**

22 **SEC. 701. ARTIFICIAL INTELLIGENCE EXPLOITATION**
 23 **GUARD AND INTELLIGENCE SHARING.**

24 (a) DEFINITIONS.—In this section:

1 (1) ARTIFICIAL INTELLIGENCE MODEL.—The
2 term “artificial intelligence model” means a capa-
3 bility or series of capabilities combined that can, for
4 a given set of objectives, generate outputs such as
5 predictions, recommendations, or decisions without
6 human intervention or input.

7 (2) CENTER.—The term “Center” means the
8 Artificial Intelligence Security Center of the Na-
9 tional Security Agency.

10 (3) CLASSIFIED INFORMATION.—The term
11 “classified information” has the meaning given such
12 term in section 805 of the National Security Act of
13 1947 (50 U.S.C. 3164).

14 (4) CLEARED INDUSTRY PERSONNEL.—The
15 term “cleared industry personnel” means employees
16 or representatives of a covered person who hold an
17 appropriate security clearance and have a dem-
18 onstrated need to know.

19 (5) CONGRESSIONAL INTELLIGENCE COMMIT-
20 TEES.—The term “congressional intelligence com-
21 mittees” has the meaning given such term in section
22 3 of the National Security Act of 1947 (50 U.S.C.
23 3003).

24 (6) COVERED PERSON.—The term “covered
25 person” means a non-Federal person who—

1 (A) is a United States citizen;

2 (B) develops, deploys, or operates artificial
3 intelligence models or critical enabling infra-
4 structure; and

5 (C) provides the services described in sub-
6 paragraph (B) to an element of the intelligence
7 community or Department of Defense.

8 (7) DIRECTOR.—The term “Director” means
9 the Director of the National Security Agency.

10 (8) INTELLIGENCE.—The term “intelligence”
11 has the meaning given such term in section 3 of the
12 National Security Act of 1947 (50 U.S.C. 3003).

13 (9) INTELLIGENCE COMMUNITY.—The term
14 “intelligence community” has the meaning given
15 such term in section 3 of the National Security Act
16 of 1947 (50 U.S.C. 3003).

17 (10) SECURITY CLEARANCE.—The term “secu-
18 rity clearance” means an authorization to access
19 classified information.

20 (11) THREAT INFORMATION.—The term
21 “threat information” means information on—

22 (A) efforts by foreign adversary countries
23 to use products or research of covered persons
24 or other entities or individuals to generate syn-
25 thetic media for foreign-directed influence cam-

1 paigns, develop and manage computer network
2 exploitation campaigns, design or develop weap-
3 ons systems, or enhance surveillance capabilities
4 in ways that undermine the privacy or threaten
5 the security of citizens of the United States;

6 (B) threats posed by foreign adversary
7 countries, including indications of compromise
8 to networks associated with covered persons
9 and other entities and individuals, or other
10 technical indicators, indicating a compromise to
11 the confidentiality, integrity, or availability of
12 an artificial intelligence system, or to the supply
13 chain of an artificial intelligence system, includ-
14 ing training or test data, frameworks or soft-
15 ware libraries, training or inference computing
16 environments, or other components necessary
17 for the training, management, or maintenance
18 of an artificial intelligence system;

19 (C) activity of foreign entities of concern
20 to clandestinely, fraudulently, or otherwise mali-
21 ciously access the systems of covered persons
22 for purposes of illicit technology transfer or oth-
23 erwise gaining unfair economic advantage, in-
24 cluding through techniques to extract a model's
25 technical capabilities to replicate, develop, or

1 improve a foreign artificial intelligence model
2 without authorization by the covered person;

3 (D) activity of foreign entities of concern
4 to sabotage or otherwise clandestinely degrade
5 artificial intelligence systems or the supply
6 chain of an artificial intelligence system, includ-
7 ing training or test data, frameworks or soft-
8 ware libraries, training or inference computing
9 environments, or other components necessary
10 for the training, management, or maintenance
11 of an artificial intelligence system; and

12 (E) observations, emerging concerns, or
13 other inputs from vendors or researchers re-
14 garding relevant malicious or clandestine activ-
15 ity of foreign entities of concern toward an arti-
16 ficial intelligence system, its supply chain, or
17 other necessary components.

18 (b) ESTABLISHMENT OF PILOT PROGRAM ON SHAR-
19 ING OF INTELLIGENCE AND THREAT INFORMATION WITH
20 COVERED PERSONS.—

21 (1) IN GENERAL.—Not later than 180 days
22 after the date of the enactment of this Act, the Di-
23 rector shall, acting through the Center, establish a
24 pilot program to assess the feasibility and advis-
25 ability of facilitating the secure sharing with covered

1 persons of intelligence and threat information ger-
2 mane to the exploitation of access to United States
3 artificial intelligence systems and enabling infra-
4 structure to engage in intelligence collection, intellec-
5 tual property theft, and other malicious activities.

6 (2) PARTICIPATION.—The Director may not se-
7 lect covered persons to participate in the pilot in a
8 manner that provides a competitive advantage or
9 procurement preference to any covered person, to
10 the detriment of another covered person.

11 (3) DURATION.—The Director shall carry out
12 the pilot program established pursuant to paragraph
13 (1) during the 3-year period beginning on the date
14 of the establishment of the pilot program.

15 (c) PARTICIPATION REQUIREMENTS.—

16 (1) CRITERIA.—The Director shall establish cri-
17 teria governing engagement with covered persons
18 under the pilot program required by subsection (b),
19 which may include criteria relating to the following:

20 (A) Relevance to national security.

21 (B) The ability to protect classified or sen-
22 sitive intelligence information.

23 (C) Cybersecurity and information security
24 maturity.

1 (D) Agreement to comply with intelligence
2 handling, use, and nondisclosure requirements.

3 (E) The availability of cleared personnel of
4 covered persons or willingness of covered per-
5 sons to increase the number of cleared per-
6 sonnel.

7 (2) NATURE OF PARTICIPATION.—Participation
8 in the pilot program shall not be construed as a cer-
9 tification, endorsement, or regulatory approval by
10 the United States Government of any artificial intel-
11 ligence system or commercial activity and the Direc-
12 tor may not exclude a covered person from partici-
13 pating on the basis of political or ideological view-
14 points of the covered person or its employees.

15 (d) INTELLIGENCE SHARING STRUCTURE.—

16 (1) AUTHORIZED MODES.—Under the pilot pro-
17 gram required by subsection (b), the Director may,
18 acting through the Center, authorize the sharing of
19 intelligence and threat information as described in
20 paragraph (1) of such subsection through—

21 (A) bilateral exchanges between elements
22 of the intelligence community and a covered
23 person;

1 (B) multilateral exchanges among covered
2 persons, as determined appropriate by the Di-
3 rector; or

4 (C) another designated intelligence-sharing
5 mechanism operated or overseen by the Direc-
6 tor.

7 (2) LIMITATION.—Any mechanism established
8 under this section shall be limited to the dissemina-
9 tion of intelligence and threat information and shall
10 not establish standards, requirements, or best prac-
11 tices governing artificial intelligence development or
12 deployment.

13 (e) TAILORING, HANDLING, AND PROTECTION OF IN-
14 TELLIGENCE.—

15 (1) PROCEDURES REQUIRED.—The Director
16 shall, acting through the Center, codify procedures
17 to tailor, sanitize, or downgrade the classification
18 level of intelligence shared under the pilot program
19 required by subsection (b) to ensure usability while
20 protecting intelligence sources and methods.

21 (2) EXAMPLES OF PROCEDURES.—The proce-
22 dures developed under paragraph (1) may include
23 the following:

24 (A) The use of tear lines and segregable
25 summaries.

1 (B) The preparation of classified annexes
2 where necessary.

3 (C) Criteria governing the classification
4 level of shared intelligence.

5 (D) The appropriate use of cleared indus-
6 try personnel.

7 (3) HANDLING REQUIREMENTS.—The Director
8 shall, acting through the Center, codify policies gov-
9 erning the handling, storage, and dissemination of
10 intelligence shared under the pilot program required
11 by subsection (b), including audit and compliance
12 mechanisms.

13 (f) PERMISSIBLE USE AND NONDISCLOSURE.—

14 (1) PERMISSIBLE USE.—Intelligence shared
15 under the pilot program required by subsection (b)
16 may be used solely for detecting, preventing, or miti-
17 gating malicious foreign activity exploiting access to
18 United States artificial intelligence systems and ena-
19 bling infrastructure to engage in intelligence collec-
20 tion, intellectual property theft, and other malicious
21 activities.

22 (2) NONDISCLOSURE.—A covered person may
23 not disclose to any person who is not a covered per-
24 son or an element of the intelligence community any
25 intelligence shared with the covered person under

1 the pilot program required by subsection (b), except
2 as expressly authorized by the Director acting
3 through the Center.

4 (g) PRIVACY AND CIVIL LIBERTIES.—In planning
5 and coordinating the pilot program required by subsection
6 (b), the Director shall, acting through the Center, consult
7 with the Civil Liberties Protection Officer of the Office
8 of the Director of National Intelligence.

9 (h) EVALUATION AND REPORTING.—

10 (1) EVALUATION.—The Director shall, acting
11 through the Center, continuously evaluate the effec-
12 tiveness and risks of the pilot program established
13 under subsection (b).

14 (2) REPORT.—

15 (A) IN GENERAL.—Not later than 90 days
16 before the date on which the pilot program re-
17 quired by paragraph (1) of subsection (b) ter-
18 minates pursuant to paragraph (2) of such sub-
19 section, the Director shall, acting through the
20 Center, submit to the congressional intelligence
21 committees a report assessing—

22 (i) the effectiveness of intelligence
23 sharing under the pilot program;

24 (ii) the adequacy of safeguards for
25 sources, methods, and privacy;

1 (iii) the scope of participation; and

2 (iv) whether the program should be
3 modified, extended, or terminated.

4 (B) FORM.—The report submitted pursu-
5 ant to subparagraph (A) shall be submitted in
6 unclassified form, but may include a classified
7 annex.

8 (i) RULE OF CONSTRUCTION.—Nothing in this sec-
9 tion shall be construed—

10 (1) to authorize the collection of intelligence on
11 United States persons not authorized by another
12 provision of law;

13 (2) to require the disclosure of classified infor-
14 mation to unauthorized persons; or

15 (3) to establish commercial, competition, or
16 technology policy outside the purview of the intel-
17 ligence community.

18 (j) EXEMPTION FROM DISCLOSURE; PROTECTION.—
19 Any information shared by a covered person or other enti-
20 ty or individual with the United States Government pursu-
21 ant to this section—

22 (1) shall be exempt from disclosure and with-
23 held, without discretion, from the public, pursuant
24 to section 552(b)(3)(B) of title 5, United States
25 Code, and any other provision of United States law

1 or law of any State, political subdivision or agency
 2 thereof, or Tribe requiring disclosure of information
 3 or records; and

4 (2) shall not be deemed a waiver of any applica-
 5 ble privilege or protection, including trade secret
 6 protection.

7 **SEC. 702. DIRECTOR OF NATIONAL INTELLIGENCE REVIEW**
 8 **OF INTELLIGENCE COMMUNITY USE OF ARTI-**
 9 **FICIAL INTELLIGENCE TO SUPPORT TAR-**
 10 **GETING.**

11 (a) DEFINITIONS.—In this subsection:

12 (1) DIRECTOR.—The term “Director” means
 13 the Director of National Intelligence.

14 (2) INTELLIGENCE.—The term “Intelligence”
 15 has the meaning given the term in section 3 of the
 16 National Security Act of 1947 (50 U.S.C. 3003).

17 (b) REVIEWS RELATED TO INTELLIGENCE COMMU-
 18 NITY USE OF ARTIFICIAL INTELLIGENCE TO SUPPORT
 19 TARGETING.—

20 (1) POLICY AND PROCEDURE REVIEWS.—

21 (A) IN GENERAL.—Not later than 60 days
 22 after the date of the enactment of this Act, the
 23 Director shall review and assess the policies and
 24 procedures that govern the use by the intel-
 25 ligence community of artificial intelligence tech-

1 nologies in the production, or review, of intel-
2 ligence used by the United States to inform tar-
3 geting decisions with lethal effects.

4 (B) ELEMENTS.—In carrying out the re-
5 view and assessment required by subparagraph
6 (A), the Director shall—

7 (i) assess whether policies and proce-
8 dures of the intelligence community that
9 were in effect on the day before the date
10 of the enactment of this Act adequately ad-
11 dress risks posed by the use of artificial in-
12 telligence technologies in the targeting
13 analysis and development and civilian
14 harm mitigation processes; and

15 (ii) ensure the review covers all poli-
16 cies of the intelligence community that re-
17 gard the production or review of intel-
18 ligence, regardless of which element first
19 produced the intelligence.

20 (2) WORKFLOW REVIEWS.—Not later than 90
21 days after the date of the enactment of this Act, the
22 Director shall review and assess all workflows of the
23 intelligence community that incorporate artificial in-
24 telligence used by the United States to inform tar-
25 geting decisions with lethal effects.

1 (c) ARTIFICIAL INTELLIGENCE ERRORS EXPLOR-
2 ATORY ANALYSIS.—In carrying out the reviews required
3 by subsection (b), the Director shall direct the National
4 Intelligence Council to conduct a structured, exploratory
5 analysis that—

6 (1) assess ways in which frontier artificial intel-
7 ligence models could exhibit bias or cause errors that
8 undermine intelligence or other information provided
9 by the intelligence community that informs targeting
10 accuracy;

11 (2) identify the specific point and cause of
12 error; and

13 (3) provide proposed process mitigations to
14 catch and correct such mistakes.

15 (d) CONSULTATION.—In carrying out the review and
16 assessments required by subsection (b), the Director shall
17 consult with the heads of the elements of the intelligence
18 community whose intelligence is commonly consulted to in-
19 form targeting decisions with lethal effects, such as the
20 National Geospatial-Intelligence Agency, the Defense In-
21 telligence Agency, the National Security Agency, and the
22 Central Intelligence Agency, to solicit input on potential
23 negative consequences resulting from artificial intelligence
24 supported analysis, and possible ways to mitigate such
25 consequences.

1 (e) POLICIES AND DIRECTIVES.—The Director shall
2 issue or adjust such policies and directives to the intel-
3 ligence community as the Director considers appropriate
4 to improve risk mitigation in light of the review carried
5 out under subsection (b).

6 (f) REPORT.—

7 (1) IN GENERAL.—Not later than 180 days
8 after the date of the enactment of this Act, the Di-
9 rector shall submit to the congressional intelligence
10 committees a report on the reviews and assessments
11 carried out under subsection (b) as well as a sum-
12 mary of any new policies and directives issued pur-
13 suant to subsection (e).

14 (2) CONTENTS.—The report required by para-
15 graph (1) shall include the following:

16 (A) A description of contributions of the
17 intelligence community to targeting workflows,
18 such as identification of points of interest, pat-
19 tern of life analysis, review of proposed targets,
20 target selection, and civilian impact reviews, as
21 well as the understanding of the intelligence
22 community of the delineation of roles and re-
23 sponsibilities with the Armed Forces where ap-
24 plicable.

1 (B) Identification of any artificial intel-
2 ligence tools utilized and for what tasks or pur-
3 poses they are used.

4 (C) The level of autonomy afforded to the
5 tools, and whether human review of artificial in-
6 telligence system outputs is required to be con-
7 ducted prior to dissemination of materials.

8 (D) The scope of individuals expected to
9 have access to the materials described in sub-
10 paragraph (C).

11 (E) An explanation of whether and how
12 the capability limitations of artificial intel-
13 ligence tools available to personnel of the intel-
14 ligence community are communicated to users,
15 including the cutoff date for the tool's training
16 data, databases to which it does or does not
17 have access rights, and the tasks the model has
18 been trained for or approved for use.

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

1 **SEC. 703. IMPROVEMENTS FOR ARTIFICIAL INTELLIGENCE**
2 **POLICIES, STANDARDS, AND GUIDANCE FOR**
3 **INTELLIGENCE COMMUNITY.**

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

7 (1) in subsection (b)—

8 (A) by redesignating paragraph (3) as
9 paragraph (4); and

10 (B) by inserting after paragraph (2) the
11 following:

12 “(3) STUDY FOR TRACKING DATA GENERATED
13 OR MODIFIED BY AN ARTIFICIAL INTELLIGENCE SYS-
14 TEM.—The Chief Artificial Intelligence Officer of the
15 Intelligence Community, in coordination with the
16 Chief Artificial Intelligence Officer of each element
17 of the intelligence community, shall examine whether
18 the intelligence community should identify intel-
19 ligence information generated or materially modified
20 by an artificial intelligence system, including deter-
21 mining what methods are necessary to preserve such
22 information throughout the intelligence lifecycle.”;

23 (2) in subsection (d), by adding at the end the
24 following:

25 “(3) PROCESS FOR REVIEW OF ARTIFICIAL IN-
26 TELLIGENCE TESTING METHODOLOGIES AND

1 BENCHMARKS.—Consistent with applicable classi-
2 fication and access policies, the Chief Artificial Intel-
3 ligence Officer of the Intelligence Community, in co-
4 ordination with the Chief Artificial Intelligence Offi-
5 cer of each element of the intelligence community,
6 shall—

7 “(A) establish a process to review artificial
8 intelligence testing methodologies and bench-
9 marks employed within each element; and

10 “(B) ensure such methodologies and
11 benchmarks remain commensurate with the ca-
12 pabilities and impacts of systems being evalu-
13 ated.”; and

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

15 “(f) PROCESS TO SYSTEMATICALLY TRACK AND
16 EVALUATE INCIDENTS.—Not later than 180 days after
17 the date of the enactment of this subsection, the Chief
18 Artificial Intelligence Officer of the Intelligence Commu-
19 nity, in coordination with the National Manager for Na-
20 tional Security Systems, shall establish a process to sys-
21 tematically track and evaluate incidents associated with
22 compromises to the confidentiality, integrity, or avail-
23 ability of artificial intelligence systems within each ele-
24 ment of the intelligence community.

1 “(g) POLICIES FOR AGENTIC ARTIFICIAL INTEL-
2 LIGENCE SYSTEMS AND PROCESSES.—

3 “(1) DEFINITION OF AGENTIC ARTIFICIAL IN-
4 TELLIGENCE SYSTEM OR PROCESS.—In this sub-
5 section, the term ‘agentic artificial intelligence sys-
6 tem or process’—

7 “(A) means an artificial intelligence system
8 or process that, given an objective or instruc-
9 tion—

10 “(i) determines the action or sequence
11 of actions to be taken to accomplish that
12 objective; and

13 “(ii) is capable of executing such ac-
14 tions directly on information systems, data,
15 or external services; and

16 “(B) does not include a system or process
17 that solely generates informational or advisory
18 output for a human operator to act upon.

19 “(2) REVIEW OF THE ADEQUACY OF EXISTING
20 IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT
21 SYSTEMS FOR INFORMATION WITHIN THE INTEL-
22 LIGENCE COMMUNITY.—

23 “(A) IN GENERAL.—Consistent with au-
24 thority under section 102A(g) of the National
25 Security Act of 1947 (50 U.S.C. 3024(g)), the

1 Director of National Intelligence, in coordina-
2 tion with the National Manager for National
3 Security Systems, shall—

4 “(i) not later than 1 year after the
5 date of the enactment of this paragraph,
6 complete a review of the adequacy of exist-
7 ing identity, credential, and access man-
8 agement systems for information within
9 the intelligence community used by agentic
10 artificial intelligence systems and proc-
11 esses; and

12 “(ii) not permit access to any infor-
13 mation within the intelligence community
14 by an external department or agency for
15 use in an agentic artificial intelligence sys-
16 tem or process until the review required by
17 clause (i) is completed.

18 “(B) EVALUATION OF EFFECTIVENESS OF
19 MECHANISMS FOR AGENTIC ARTIFICIAL INTEL-
20 LIGENCE SYSTEMS AND PROCESSES TO AU-
21 THENTICATE AS NON-HUMAN ACTORS.—The re-
22 view required by subparagraph (A)(i) shall in-
23 clude an evaluation of the effectiveness of mech-
24 anisms for agentic artificial intelligence systems
25 and processes to authenticate as non-human ac-

tors, including the appropriate delegation of clearance entitlements and the traceability of any action taken by an agentic artificial intelligence system or process to a cleared individual on whose behalf the agentic artificial intelligence system or process is acting.

“(3) POLICY GUIDANCE.—Upon completion of the review required by paragraph (2), the Director of National Intelligence, in coordination with the Director of the National Security Agency, the Director of the National Reconnaissance Office, and the Director of the National Geospatial-Intelligence Agency, shall issue appropriate policy guidance on—

“(A) the use of agentic artificial intelligence systems and processes within the intelligence community; and

“(B) the access of agentic artificial intelligence systems and processes to information within the intelligence community.

“(4) SPECIFIC ISSUES RELATING TO AGENTIC ARTIFICIAL INTELLIGENCE SYSTEMS AND PROCESSES.—In carrying out paragraph (3), the Director of National Intelligence, at a minimum and to the extent such requirements are not already replicated in existing processes or policies, consider—

1 “(A) establishing a taxonomy of autonomy
2 and security risks associated with agentic artificial
3 intelligence systems and processes that op-
4 erate on, or have the possibility of accessing, in-
5 formation within the intelligence community;
6 and

7 “(B) establishing technical controls, proc-
8 esses, and other mitigation measures to address
9 the risks identified under subparagraph (A), in-
10 cluding, at a minimum—

11 “(i) requirements that any element of
12 the intelligence community or external de-
13 partment or agency incorporating informa-
14 tion from an intelligence community ele-
15 ment as part of an agentic artificial intel-
16 ligence system or process provide the rel-
17 evant element of the intelligence commu-
18 nity controlling such information with doc-
19 umentation of—

20 “(I) the properties of the agentic
21 artificial intelligence system or proc-
22 ess, including the range of additional
23 systems or data sources it may access
24 (whether as a system or process input
25 or as an agent action), the permis-

1 sions and classification entitlements
2 associated with such access, as well as
3 any relevant model or system docu-
4 mentation, such as model and system
5 cards;

6 “(II) anticipated mission use
7 cases for any access to information
8 within the intelligence community in
9 the context of an agentic artificial in-
10 telligence system or process, including
11 whether any use case constitutes a
12 high-impact artificial intelligence use
13 as those terms are defined under ex-
14 isting Federal policies;

15 “(III) procedures to notify rel-
16 evant intelligence community elements
17 controlling such information of any
18 changes to the properties of the
19 agentic artificial intelligence system or
20 process, to permissions and classifica-
21 tion entitlements, or to anticipated
22 use cases of such system or process,
23 that might significantly limit the util-
24 ity, confidentiality, integrity, or avail-
25 ability of such information; and

1 “(IV) procedures for intelligence
2 community elements to promptly no-
3 tify external intelligence community
4 elements or departments or agencies
5 of any material changes to upstream
6 classified data or systems that might
7 significantly limit or impair the util-
8 ity, confidentiality, integrity, or avail-
9 ability of any downstream agentic ar-
10 tificial intelligence system or process
11 maintained by that external intel-
12 ligence community element or depart-
13 ment or agency;

14 “(ii) policies and procedures to log
15 any actions, as well as associated inputs,
16 taken by an agentic artificial intelligence
17 system or process to information within
18 the intelligence community, including
19 mechanisms to reverse or negate unauthor-
20 ized actions or actions that pose a risk to
21 the user intent or confidentiality, integrity,
22 or availability of such information;

23 “(iii) policies and procedures for safe-
24 guards, continuous monitoring, and the de-
25 tection of security incidents or other unex-

1 pected behavior of an agentic artificial in-
2 telligence system or process, or failures of
3 associated safeguards, that may pose a
4 threat to the confidentiality, availability, or
5 integrity of information within the intel-
6 ligence community;

7 “(iv) policies and procedures for sys-
8 tem-level controls of agentic artificial intel-
9 ligence systems and processes, tailored to
10 address each system or process component;
11 and

12 “(v) criteria for the selection of inter-
13 operability standards for agentic artificial
14 intelligence systems and processes, with
15 preference, to the extent practicable, for
16 standards that are openly specified, gov-
17 erned in a vendor-neutral manner, sup-
18 ported by multiple model providers, exten-
19 sible to future requirements, and subject to
20 ongoing independent security review.”.

1 **SEC. 704. ADDITIONAL FUNCTIONS AND REQUIREMENTS OF**
 2 **ARTIFICIAL INTELLIGENCE SECURITY CEN-**
 3 **TER.**

4 Section 6504 of the Intelligence Authorization Act for
 5 Fiscal Year 2025 (division F of Public Law 118–159) is
 6 amended—

7 (1) in subsection (c)—

8 (A) by redesignating paragraph (3) as
 9 paragraph (4); and

10 (B) by inserting after paragraph (2) the
 11 following new paragraph (3):

12 “(3) Making available a research test-bed to
 13 private sector and academic researchers, on a sub-
 14 sidized basis, to engage in artificial intelligence secu-
 15 rity research, including through the secure provision
 16 of access in a secure environment for pre-deployment
 17 testing of to proprietary third-party models with the
 18 consent of the vendors of the models.”;

19 (2) by redesignating subsection (d) as sub-
 20 section (f); and

21 (3) by inserting after subsection (c) the fol-
 22 lowing:

23 “(d) TEST-BED REQUIREMENTS.—

24 “(1) ACCESS AND TERMS OF USAGE.—

25 “(A) RESEARCHER ACCESS.—The Director
 26 shall establish terms of usage governing re-

1 searcher access to the test-bed made available
2 under subsection (c)(3), with limitations on re-
3 searcher publication only to the extent nec-
4 essary to protect classified information or pro-
5 prietary information concerning third-party
6 models provided through the consent of model
7 vendors.

8 “(B) AVAILABILITY TO FEDERAL AGEN-
9 CIES.—The Director shall ensure that the test-
10 bed made available under subsection (c)(3) is
11 also made available to other Federal agencies
12 on a cost-recovery basis.

13 “(2) USE OF CERTAIN INFRASTRUCTURE AND
14 OTHER RESOURCES.—In carrying out subsection
15 (c)(3), the Director shall leverage, to the greatest ex-
16 tent practicable, infrastructure and other resources
17 provided under section 5.2 of Executive Order
18 14110 (88 Fed. Reg. 75191; relating to safe, secure,
19 and trustworthy development and use of artificial in-
20 telligence).

21 “(3) VOLUNTARY SECURITY GUIDANCE.—In
22 order to incentivize participation by vendors of lead-
23 ing commercial models and to promote the national
24 security of the United States, the Director shall
25 share relevant guidance, informed by pre-deployment

1 testing in the secure test-bed environment identified
 2 in subsection (c), to inform voluntary vendor actions
 3 to mitigate against potential security threats to such
 4 models, or the ability of foreign actors to utilize such
 5 models for computer network exploitation cam-
 6 paigns, the design or development of weapons sys-
 7 tems, or to further foreign surveillance capabilities.”.

8 **SEC. 705. REPORTS ON NOVEL USES OF ARTIFICIAL INTEL-**
 9 **LIGENCE TECHNOLOGY.**

10 (a) DEFINITION.—In this section, the term “novel
 11 use of artificial intelligence technology” means—

12 (1) an artificial intelligence capability or series
 13 of capabilities combined that has not previously been
 14 included in an intelligence community element’s in-
 15 ventory of artificial intelligence use cases consistent
 16 with guidance issued pursuant to section 6702(b) of
 17 the Intelligence Authorization Act for Fiscal Year
 18 2023 (50 U.S.C. 3334m(b));

19 (2) a use of an artificial intelligence capability
 20 that contravenes a restriction on the use of artificial
 21 intelligence contained in such an inventory; or

22 (3) a use of an artificial intelligence capability
 23 that constitutes a high-impact artificial intelligence
 24 use as that term is defined under policies of the ex-
 25 ecutive branch.

1 (b) IN GENERAL.—Not later than 90 days after the
2 date of the enactment of this Act, and every 180 days
3 thereafter, the Director of National Intelligence, in coordi-
4 nation with the heads of the other elements of the intel-
5 ligence community, shall submit to the congressional intel-
6 ligence committees a consolidated report detailing any
7 novel use of artificial intelligence technology that any ele-
8 ment of the intelligence community is considering employ-
9 ing within the one-year period following submission of
10 such report.

11 (c) CONTENTS.—Each report submitted pursuant to
12 subsection (b) shall describe the proposed novel use of ar-
13 tificial intelligence technology, including—

- 14 (1) hardware and software requirements;
- 15 (2) the proposed application of the technology;
- 16 (3) the risks and advantages assessed with re-
17 spect to the proposed novel use;
- 18 (4) any specific risk mitigation measures con-
19 templated, including measures specific to the pro-
20 posed novel use;
- 21 (5) any test and evaluation activities conducted
22 in conjunction with the proposed novel use;
- 23 (6) any additional test and evaluation activity
24 that is still needed, and whether the intelligence

1 community has resources to conduct and fund such
2 activity; and

3 (7) any estimated cost increases anticipated in
4 connection with the proposed novel use.

5 (d) FORM.—Each report submitted pursuant to sub-
6 section (b) shall be submitted in classified form.

7 (e) SUNSET.—This section shall expire on October 1,
8 2032.

9 **SEC. 706. CLEAR LABELING OF ARTIFICIAL INTELLIGENCE**

10 **OUTPUTS FOR TARGETING WORKFLOWS.**

11 Not later than 60 days after the date of the enact-
12 ment of this Act, the Director of National Intelligence
13 shall, in coordination with the Chief Artificial Intelligence
14 Officers of the elements of the intelligence community, es-
15 tablish a policy that applies to elements of the intelligence
16 community, which generate intelligence that could reason-
17 ably be judged useful to develop or inform targeting with
18 lethal effects, and that requires—

19 (1) labeling of outputs from any artificial intel-
20 ligence system used in the development of such intel-
21 ligence are clearly marked to indicate—

22 (A) that artificial intelligence was used;

23 (B) the artificial intelligence system or
24 model used;

1 (C) the manner in which, or task for
2 which, the artificial intelligence was used; and

3 (D) a point of contact such as the relevant
4 Chief Artificial Intelligence Officer, who can ad-
5 dress questions about data inputs, system ac-
6 cess, or artificial intelligence system perform-
7 ance; and

8 (2) the label or indicator that is used pursuant
9 to paragraph (1) is attached to the resulting data or
10 work product in a manner that remains prominent
11 and visible to any person who subsequently interacts
12 with that data on a system of the intelligence com-
13 munity, regardless of organizational affiliation of the
14 person or the role of the person in developing the
15 data.

16 **SEC. 707. RESEARCH ON USE OF ARTIFICIAL INTEL-**
17 **LIGENCE RELATING TO INADVERTENT ESCA-**
18 **LATION.**

19 (a) REQUIREMENT.—Not later than 90 days after the
20 date of the enactment of this Act and subject to the avail-
21 ability of appropriations, the Director of the Intelligence
22 Advanced Research Projects Activity, in coordination with
23 the Chief Artificial Intelligence Officer of the Intelligence
24 Community, shall commence a research campaign to deep-
25 en the understanding of the intelligence community with

1 respect to specific ways in which the use of artificial intel-
2 ligence systems by the intelligence community could con-
3 tribute to inadvertent escalation with foreign nations or
4 actors.

5 (b) ELEMENTS.—The research campaign required by
6 subsection (a) shall include—

7 (1) the identification of scenarios in which arti-
8 ficial intelligence capabilities could contribute to in-
9 advertent escalation with foreign nations or actors,
10 including—

11 (A) analytic judgments that fail to prop-
12 erly consider or weigh alternative explanations;

13 (B) automation of imagery classification or
14 signals intelligence;

15 (C) distinguishing between civilians and
16 authorized targets;

17 (D) operational uses of artificial intel-
18 ligence, such as time-constrained uses that do
19 not allow for independent verification; and

20 (E) such other scenarios as identified by
21 the Director or participating subject matter ex-
22 perts;

23 (2) a simulation of select scenarios to discern
24 where miscommunication or miscalculations have a
25 higher likelihood of occurrence; and

1 (3)(A) an identification of potential mitigations
2 for vulnerabilities discovered; or

3 (B) if no mitigation could be identified, an
4 identification of vulnerabilities that require follow-up
5 action by the intelligence community.

6 (c) BRIEFINGS.—

7 (1) CONGRESS.—Not later than 180 days after
8 the date of the enactment of this Act, or 30 days
9 after the date of completion of the research cam-
10 paign required by subsection (a), whichever occurs
11 first, the Director of the Intelligence Advanced Re-
12 search Projects Activity, in coordination with the
13 Chief Artificial Intelligence Officer of the Intel-
14 ligence Community, shall brief the congressional in-
15 telligence committees on the findings and rec-
16 ommendations of the research campaign.

17 (2) INTELLIGENCE COMMUNITY.—The Director
18 of the Intelligence Advanced Research Projects Ac-
19 tivity, in coordination with the Chief Artificial Intel-
20 ligence Officer of the Intelligence Community, shall
21 brief the heads and Chief Artificial Intelligence Offi-
22 cers of the elements of the intelligence community
23 on the findings and recommendations of the research
24 campaign required by subsection (a), as appropriate.

1 **SEC. 708. RESEARCH ON INTERACTION OF ADVERSARIAL**
2 **ARTIFICIAL INTELLIGENCE SYSTEMS WITH**
3 **INTELLIGENCE COMMUNITY SYSTEMS.**

4 (a) REQUIREMENT.—Not later than 90 days after the
5 date of the enactment of this Act and subject to the avail-
6 ability of appropriations, the Director of the Intelligence
7 Advanced Research Projects Activity, in coordination with
8 the Chief Artificial Intelligence Officer of the Intelligence
9 Community, shall commence a research campaign to deep-
10 en the understanding of the intelligence community with
11 respect to novel dynamics and vulnerabilities that may
12 arise when an adversarial artificial intelligence system
13 interacts directly with systems of, or contracted by, the
14 intelligence community that include artificial intelligence
15 components.

16 (b) ELEMENTS.—The research campaign required by
17 subsection (a) shall—

18 (1) pursue sandbox demonstrations with fron-
19 tier artificial intelligence models or leverage other
20 tactics necessary to uncover vulnerabilities to intel-
21 ligence community systems, infrastructure, or per-
22 sonnel that may result from—

23 (A) the accelerated development of artifi-
24 cial intelligence capabilities by foreign nations;

25 (B) the increasing access that non-state
26 and criminal actors have to commercial artifi-

1 cial intelligence tools that can identify
 2 vulnerabilities and propose or orchestrate at-
 3 tacks; and

4 (C) the potential for artificial intelligence
 5 systems to interact directly with each other dur-
 6 ing an attack; and

7 (2) pursue findings, including—

8 (A) an identification of potential mitiga-
 9 tions for unique vulnerabilities discovered; or

10 (B) if no mitigation could be identified, an
 11 identification of vulnerabilities that require fol-
 12 low-up action by the intelligence community.

13 (c) BRIEFINGS.—

14 (1) CONGRESS.—Not later than 180 days after
 15 the date of the enactment of this Act, or 30 days
 16 after the date of completion of the research cam-
 17 paign required by subsection (a), whichever occurs
 18 first, the Director of the Intelligence Advanced Re-
 19 search Projects Activity, in coordination with the
 20 Chief Artificial Intelligence Officer of the Intel-
 21 ligence Community, shall brief the congressional in-
 22 telligence committees on the findings and rec-
 23 ommendations of the research campaign.

24 (2) INTELLIGENCE COMMUNITY.—The Director
 25 of the Intelligence Advanced Research Projects Ac-

1 tivity, in coordination with the Chief Artificial Intel-
 2 ligence Officer of the Intelligence Community, shall
 3 brief the heads and Chief Artificial Intelligence Offi-
 4 cers of the elements of the intelligence community
 5 on the findings and recommendations of the research
 6 campaign required by subsection (a), as appropriate.

7 **SEC. 709. PROLIFERATION ASSESSMENTS REGARDING THE**
 8 **EXPORT OF ARTIFICIAL INTELLIGENCE-RE-**
 9 **LATED TECHNOLOGIES.**

10 (a) DEFINITIONS.—In this section:

11 (1) ARTIFICIAL INTELLIGENCE TECHNOLOGY.—

12 The term “artificial intelligence technology”
 13 means—

14 (A) any United States-origin model
 15 weights;

16 (B) semiconductor manufacturing equip-
 17 ment; and

18 (C) any other item classified under—

19 (i) Export Control Classification
 20 Number 3A090 or 4A090 of the Commerce
 21 Control List or corresponding entries in
 22 the Export Administration Regulations, as
 23 in effect on the date of the enactment of
 24 this Act; or

1 (ii) any subsequent revisions to the
2 Commerce Control List as amended by the
3 Bureau of Industry and Security to impose
4 more restrictive parameters.

5 (2) COMMERCE CONTROL LIST.—The term
6 “Commerce Control List” means the Commerce
7 Control List set forth in Supplement No. 1 to part
8 774 of the Export Administration Regulations.

9 (3) UNITED STATES ARTIFICIAL INTELLIGENCE
10 STACK.—The term “United States artificial intel-
11 ligence stack” means the United States artificial in-
12 telligence integrated circuits, cloud infrastructure,
13 and models.

14 (4) EXPORT CONTROL TERMS.—The terms “ex-
15 port”, “Export Administration Regulations”, “in-
16 country transfer”, “reexport”, and “United States
17 person” have the meanings given those terms in sec-
18 tion 1742 of the Export Control Reform Act of 2018
19 (50 U.S.C. 4801).

20 (b) STATEMENT OF POLICY.—It shall be the policy
21 of the United States to restrict access to the most sophisti-
22 cated artificial intelligence integrated circuits and models
23 that United States adversaries may seek to use against
24 the United States, while also exporting the full United

1 States artificial intelligence stock to allies and partners
2 who adhere to stringent national security standards.

3 (c) REQUIREMENT.—Not fewer than 90 days before
4 the Secretary of Commerce grants a license for the export,
5 reexport, or in-country transfer of artificial intelligence
6 technology, or before the United States joins an agreement
7 on artificial intelligence with a foreign government, the Di-
8 rector of National Intelligence, acting through the Na-
9 tional Intelligence Council, and in coordination with the
10 Director of the Central Intelligence Agency, the Assistant
11 Secretary of State for Intelligence and Research, the Di-
12 rector of the National Security Agency, and the heads of
13 other appropriate elements of the intelligence community,
14 shall provide to the President and the congressional intel-
15 ligence committees a written assessment containing a com-
16 prehensive analysis regarding the risks associated with
17 such action.

18 (d) SUBSTANCE.—Each report submitted under sub-
19 section (c) shall include the assessment of the intelligence
20 community of the consequences of the action concerned
21 for United States national security, including assessment
22 of—

23 (1) the recipient country's export control sys-
24 tem with respect to artificial intelligence technology,

1 including integrated circuits, integrated circuit de-
2 sign software, tools, and manufacturing equipment;

3 (2) information on any past, present, or ex-
4 pected interactions, including commercial ties and
5 cooperation, between commercial entities or govern-
6 ment entities in the recipient country and other
7 countries of proliferation concern, including the Peo-
8 ple's Republic of China and the Russian Federation;

9 (3) actual or suspected transfers of artificial in-
10 telligence technology to such countries, including the
11 People's Republic of China and the Russian Federa-
12 tion;

13 (4) the consequences that onward proliferation
14 of United States artificial intelligence technology
15 from the recipient would have for United States ef-
16 forts to both deny adversaries access to advanced ar-
17 tificial intelligence technology and maintain a signifi-
18 cant competitive advantage in frontier artificial in-
19 telligence development, integrated design, and inte-
20 grated manufacturing, especially relative to the
21 progress of the People's Republic of China and the
22 Russian Federation;

23 (5) the capacity of the intelligence community
24 and United States commercial entities to have near

1 real-time awareness of the any potential technology
2 leakage or export violations by the recipient country;

3 (6) potential measures that the intelligence
4 community assesses could reasonably be taken by
5 the recipient country to mitigate both the prolifera-
6 tion concerns identified by the intelligence commu-
7 nity and the consequences of any potential onward
8 proliferation as detailed in paragraph (4);

9 (7) in the case of the grant of a license, specific
10 measures that the intelligence community will take
11 to evaluate compliance with any associated restric-
12 tions or compliance requirements;

13 (8) whether export of artificial intelligence tech-
14 nology would reinforce United States artificial intel-
15 ligence dominance;

16 (9) the intended and likely end-uses, including
17 military, intelligence, and domestic surveillance ap-
18 plications, and whether such uses are consistent with
19 United States national security interests; and

20 (10) current and planned agreements and ar-
21 rangements between the United States and the gov-
22 ernment of the recipient country.

23 (e) FORM.—Each report submitted under subsection
24 (c) shall be submitted in unclassified form, but may in-
25 clude a classified annex.

1 **SEC. 710. REVIEW OF ARTIFICIAL INTELLIGENCE SECURITY**
 2 **VULNERABILITIES UNDER VULNERABILITIES**
 3 **EQUITIES PROCESS.**

4 (a) DEFINITIONS.—In this section:

5 (1) ARTIFICIAL INTELLIGENCE SECURITY VUL-
 6 NERABILITY.—The term “artificial intelligence secu-
 7 rity vulnerability” means a weakness in an artificial
 8 intelligence system that could be exploited by a third
 9 party to subvert, without authorization, the privacy,
 10 integrity, or availability of an artificial intelligence
 11 system, including through techniques such as—

- 12 (A) evasion attacks;
- 13 (B) poisoning attacks;
- 14 (C) privacy-based attacks;
- 15 (D) model theft or extraction attacks; and
- 16 (E) attacks designed to circumvent or de-
 17 grade the safety, alignment, or access control
 18 mechanisms of an artificial intelligence system.

19 (2) ARTIFICIAL INTELLIGENCE SYSTEM.—The
 20 term “artificial intelligence system” means a capa-
 21 bility or series of capabilities combined that can, for
 22 a given set of objectives, generate outputs such as
 23 predictions, recommendations, or decisions without
 24 human intervention or input.

25 (3) VULNERABILITIES EQUITIES POLICY AND
 26 PROCESS DOCUMENT.—The term “Vulnerabilities

1 Equities Policy and Process document” means the
2 executive branch document entitled “Vulnerabilities
3 Equities Policy and Process for the United States
4 Government” dated November 15, 2017.

5 (4) VULNERABILITIES EQUITIES PROCESS.—
6 The term “Vulnerabilities Equities Process” means
7 the interagency review of vulnerabilities carried out
8 pursuant to the Vulnerabilities Equities Policy and
9 Process document or any successor document.

10 (b) EVALUATION; REPORT.—Not later than 90 days
11 after the date of the enactment of this Act, the Director
12 of the National Security Agency shall—

13 (1) evaluate whether the existing Vulnerabilities
14 Equities Process sufficiently accommodates the sub-
15 mission and review of artificial intelligence security
16 vulnerabilities; and

17 (2) submit to the congressional intelligence
18 committees a report describing the applicability of
19 the Vulnerabilities Equities Process to such
20 vulnerabilities, including whether the submission and
21 review of such vulnerabilities under the
22 Vulnerabilities Equities Process would result in an
23 unduly large volume of notifications to affected ven-
24 dors and, if so, an assessment of mechanisms to
25 manage the volume of such notifications.

1 (c) PROCESS.—In carrying out subsection (b), if the
2 Director of the National Security Agency determines that
3 the existing Vulnerabilities Equities Process does not suf-
4 ficiently accommodate the submission and review of artifi-
5 cial intelligence security vulnerabilities identified by ele-
6 ments of the intelligence community, and that such
7 vulnerabilities present public interest considerations mer-
8 iting review under the Vulnerabilities Equities Process,
9 the Director shall establish a process for the submission
10 and review of such vulnerabilities under the Vulnerabilities
11 Equities Process not later than 30 days after the date of
12 such determination.

13 (d) BRIEFING ON VULNERABILITIES IDENTIFIED BY
14 ARTIFICIAL INTELLIGENCE SYSTEMS.—Not later than 90
15 days after the date of the enactment of this Act, the Direc-
16 tor of the National Security Agency shall provide the con-
17 gressional intelligence committees with a briefing on—

18 (1) the volume of vulnerabilities of information
19 systems identified by artificial intelligence systems;

20 (2) the impact of any change in such volume on
21 the functioning of the Vulnerabilities Equities Proc-
22 ess; and

23 (3) whether the increasingly rapid discovery
24 and exploitation of such vulnerabilities by external

1 cyber actors using artificial intelligence systems ma-
2 terially alters the equity of disclosure.

3 (e) CONSULTATION REQUIRED.—The Director of the
4 National Security Agency shall carry out subsections (b),
5 (c), and (d) in consultation with—

6 (1) the Director of the Central Intelligence
7 Agency;

8 (2) the Director of the Federal Bureau of In-
9 vestigation; and

10 (3) other entities as the Director of the Na-
11 tional Security Agency considers appropriate.

12 **SEC. 711. PROHIBITION ON CERTAIN ARTIFICIAL INTEL-**
13 **LIGENCE MODELS ON INTELLIGENCE COM-**
14 **MUNITY SYSTEMS.**

15 (a) DEFINITIONS.—In this section:

16 (1) ARTIFICIAL INTELLIGENCE MODEL.—The
17 term “artificial intelligence model” means a capa-
18 bility or series of capabilities combined that can, for
19 a given set of objectives, generate outputs such as
20 predictions, recommendations, or decisions without
21 human intervention or input.

22 (2) CHILD PORNOGRAPHY.—The term “child
23 pornography” has the meaning given that term in
24 section 2256 of title 18, United States Code.

1 (3) COVERED APPLICATION.—The term “cov-
2 ered application” means any specific artificial intel-
3 ligence model that has been confirmed by a head of
4 an element of the intelligence community, or their
5 designee, as—

6 (A) failing to comply with the National In-
7 stitute of Standard and Technology Artificial
8 Intelligence Risk Management Framework:
9 Generative Artificial Intelligence Profile with
10 respect to “obscene, degrading, and/or abusive
11 content”, or a successor standard or frame-
12 work, to the extent the framework applies to
13 synthetic child sexual abuse material or non-
14 consensual intimate images of adults;

15 (B) subject to a Federal court determina-
16 tion that such artificial intelligence model has
17 generated content depicting child pornography;
18 or

19 (C) subject to a Federal court determina-
20 tion that such artificial intelligence model has
21 generated non-consensual intimate visual depic-
22 tions of an identifiable adult or a minor.

23 (4) INTIMATE VISUAL DEPICTION.—The term
24 “intimate visual depiction” has the meaning given
25 that term in section 1309 of the Violence Against

1 Women Act Reauthorization Act of 2022 (15 U.S.C.
2 6851).

3 (b) PROHIBITION.—

4 (1) IN GENERAL.—The acquisition or use of
5 any covered application on national security systems
6 operated by an element of the intelligence commu-
7 nity or by a contractor of such element is prohibited
8 unless the appropriate safeguards described in sub-
9 section (c) can be implemented.

10 (2) IMPLEMENTATION.—

11 (A) INITIAL REMOVAL.—Not later than
12 180 days after the date of the enactment of this
13 Act, any covered application shall be required to
14 be removed from national security systems op-
15 erated by an element of the intelligence commu-
16 nity or a contractor of such element.

17 (B) SUBSEQUENT REMOVALS.—Beginning
18 after the 180-day period described in subpara-
19 graph (A), any artificial intelligence model that
20 becomes a covered application shall be required
21 to be removed from national security systems
22 operated by an element of the intelligence com-
23 munity or a contractor of such element not
24 later than 180 days after the date that the
25 model is confirmed by the head of an element

1 of the intelligence community, or their designee,
2 to be a covered application.

3 (c) SAFEGUARDS.—

4 (1) IN GENERAL.—The head of an element of
5 the intelligence community may implement addi-
6 tional safeguards that prohibit the generation of
7 child pornography or non-consensual intimate visual
8 depictions of an identifiable adult or a minor.

9 (2) CERTIFICATION REQUIRED.—The head of
10 an element of the intelligence community shall cer-
11 tify to the Director of National Intelligence that
12 safeguards implemented under paragraph (1) are
13 sufficient to prevent misuse of covered applications
14 to generate child pornography or intimate visual de-
15 pictions of a minor.

16 (3) CONGRESSIONAL NOTIFICATION.—The head
17 of an element of the intelligence community that
18 issues a certification pursuant to paragraph (2) shall
19 notify the congressional intelligence committees of
20 such certification not later than 7 days after issuing
21 such certification. Such a notification shall identify
22 the safeguards implemented pursuant to paragraph
23 (1).

24 (d) NATIONAL SECURITY AND RESEARCH WAIVER.—

1 (1) IN GENERAL.—The head of an element of
2 the intelligence community may issue a waiver for
3 any artificial intelligence model that would otherwise
4 be subject to the prohibition under subsection (b) if
5 the head identifies a national security or research
6 justification for such artificial intelligence model
7 that benefits the intelligence community.

8 (2) CONGRESSIONAL NOTIFICATION.—Not later
9 than 7 days after issuing a waiver pursuant to para-
10 graph (1), the head of the element of the intelligence
11 community that issues such waiver shall submit to
12 the congressional intelligence committees a notifica-
13 tion that includes—

14 (A) an identification of the national secu-
15 rity or research justification for such usage;

16 (B) an estimate of the approximate cost of
17 such usage; and

18 (C) a plan to implement a safeguard in
19 such a way as to allow for continued usage con-
20 sistent with the general prohibition described in
21 subsections (b)(1) and (c)(1).

22 (e) CURE.—If a covered application is identified for
23 removal or is disqualified from use or acquisition pursuant
24 to this section, the head of an element of the intelligence
25 community may offer the provider of the covered applica-

tion an opportunity to cure performance to avoid removal pursuant to subsection (b)(2).

TITLE VIII—OTHER MATTERS

SEC. 801. MODIFICATION TO NOTIFICATION REQUIREMENTS FOR AUTHORIZED AND ORDERED DEPARTURES.

Section 5173(e) of the Department of State Authorization Act for Fiscal Year 2026 (22 U.S.C. 4865 note; division E of Public Law 119–60) is amended—

(1) in paragraph (1), by inserting “, the Permanent Select Committee on Intelligence, the Committee on Armed Services,” after “Foreign Affairs”; and

(2) in paragraph (2), by inserting “, the Select Committee on Intelligence, the Committee on Armed Services,” after “Foreign Relations”.

SEC. 802. IDENTIFICATION OF REALLOCABLE FREQUENCIES.

Section 113 of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 923) is amended—

(1) in subsection (h)(7)(A)—

(A) in clause (i), by redesignating subclauses (I) and (II) as items (aa) and (bb), re-

1 spectively, and adjusting the margins accord-
2 ingly;

3 (B) by redesignating clauses (i) and (ii) as
4 subclauses (I) and (II), respectively, and adjust-
5 ing the margins accordingly;

6 (C) by striking “If any of the information”
7 and inserting the following:

8 “(i) IN GENERAL.—If a portion of the
9 information”; and

10 (D) by adding at the end the following:

11 “(ii) FULL CLASSIFICATION.—Not-
12 withstanding paragraphs (5) and (6), if
13 the classification of information required to
14 be included in the transition plan of a Fed-
15 eral entity prohibits even the public release
16 of a redacted transition plan, as deter-
17 mined by the head of the Federal entity,
18 the Federal entity shall—

19 “(I) notify the NTIA that the en-
20 tire transition plan must be classified
21 and that even a redacted version can-
22 not be made public; and

23 “(II) classify the transition plan
24 in accordance with the levels of mate-

1 rials contained in the transition
2 plan.”; and

3 (2) in subsection (l)—

4 (A) by striking “For purposes of” and in-
5 serting the following:

6 “(1) IN GENERAL.—For purposes of”; and

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

8 “(2) ELEMENTS OF THE INTELLIGENCE COM-
9 MUNITY.—Notwithstanding paragraph (1) or any
10 other provision of this part, each element of the in-
11 telligence community (as defined in section 3 of the
12 National Security Act of 1947 (50 U.S.C. 3003))
13 shall be considered a Federal entity and shall be eli-
14 gible to receive payment from the Spectrum Reloca-
15 tion Fund for any auction-related relocation or shar-
16 ing costs incurred by the element regardless of the
17 existence of a Government station license.”.

18 **SEC. 803. PROTECTION OF CLASSIFIED INFORMATION RE-**
19 **LATING TO BUDGET FUNCTIONS.**

20 (a) REQUIREMENT.—

21 (1) IN GENERAL.—Chapter 11 of title 31,
22 United States Code, is amended by adding at the
23 end the following new section:

1 **“§ 1127. Protection of classified information relating**
2 **to budget functions**

3 “(a) PROTECTION OF CLASSIFIED INFORMATION.—
4 Notwithstanding any other provision of law, not later than
5 September 30, 2028, each covered official shall ensure
6 that the department or agency of the official uses secure
7 systems that meet the requirements to protect classified
8 information, including with respect to the location at
9 which the system is located or accessed, to carry out any
10 of the following activities of the department or agency:

11 “(1) Formulating, developing, and submitting
12 the budget of the department or agency (including
13 the budget justification materials submitted to Con-
14 gress) under the National Intelligence Program.

15 “(2) Apportioning, allotting, issuing warrants
16 for the disbursement of, and obligating and expend-
17 ing funds under the National Intelligence Program.

18 “(3) Carrying out Federal financial manage-
19 ment service functions or related activities of the in-
20 telligence community.

21 “(b) WAIVER.—The Director of National Intel-
22 ligence, in consultation with the Secretary of Defense, the
23 Secretary of the Treasury, and the Director of the Office
24 of Management and Budget, may issue a waiver to a head
25 of an element of the intelligence community with respect
26 to a requirement under subsection (a) if the Director of

1 National Intelligence certifies to the congressional intel-
2 ligence committees that—

3 “(1) one or more of the Federal financial man-
4 agement service functions or related activities of the
5 element under the National Intelligence Program—

6 “(A) are appropriately carried out using a
7 system that does not meet the requirements to
8 protect classified information; and

9 “(B) such use does not represent a signifi-
10 cant counterintelligence risk; or

11 “(2) complying with a specified requirement
12 under subsection (a) would result in an increased
13 counterintelligence threat to a classified program or
14 activity.

15 “(c) DISPLAY OF INFORMATION IN PUBLIC RE-
16 PORTS.—Notwithstanding any other provision of law, in
17 making public a report or other information relating to
18 expenditures by an element of the intelligence community,
19 a covered official may modify or omit information relating
20 to such expenditures in a manner necessary to ensure the
21 protection of classified information.

22 “(d) DEFINITIONS.—In this section:

23 “(1) COVERED OFFICIAL.—The term ‘covered
24 official’ means the following:

25 “(A) The Secretary of the Treasury.

1 “(B) The Director of the Office of Man-
2 agement and Budget.

3 “(C) Each head of an element of the intel-
4 ligence community.

5 “(D) Any other head of a department or
6 agency of the Federal Government carrying out
7 a function specified in paragraph (1), (2), or
8 (3) of subsection (a).

9 “(2) FEDERAL FINANCIAL MANAGEMENT SERV-
10 ICE FUNCTIONS.—In this section, the term ‘Federal
11 financial management service functions’ means
12 standard functions, as determined by the Secretary
13 of the Treasury, that departments and agencies of
14 the Federal Government perform relating to Federal
15 financial management, including budget execution,
16 financial asset information management, payable
17 management, revenue management, reimbursable
18 management, receivable management, delinquent
19 debt management, cost management, general ledger
20 management, financial reconciliation, and financial
21 and performance reporting.

22 “(3) INTELLIGENCE COMMUNITY TERMS.—The
23 terms ‘congressional intelligence committees’, ‘intel-
24 ligence community’, and ‘National Intelligence Pro-
25 gram’ have the meaning given those terms in section

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

3 (2) CLERICAL AMENDMENT.—The table of sec-
4 tions at the beginning of chapter 11 of title 31,
5 United States Code, is amended by inserting after
6 the item relating to section 1126 the following new
7 item:

“1127. Protection of classified information relating to budget functions.”.

8 (b) FUNDING NEEDED TO IMPLEMENT SPECIFIED
9 REQUIREMENTS.—

10 (1) REIMBURSEMENT.—Notwithstanding any
11 other provision of law, of the amounts authorized to
12 be appropriated or otherwise made available to the
13 Director of National Intelligence under the Intel-
14 ligence Community Management Account that are
15 available until September 30, 2028, the Director
16 may reimburse a covered official for amounts that
17 the official incurred to implement section 1127(a) of
18 title 31, United States Code, as added by subsection
19 (a).

20 (2) REPORT.—Not later than 180 days after
21 the date of the enactment of this Act, the Director
22 of National Intelligence, the Secretary of the Treas-
23 ury, and the heads of the elements of the intelligence
24 community shall jointly submit to the congressional
25 intelligence committees a detailed cost estimate asso-

1 ciated with the implementation of the requirements
2 under section 1127(a) of title 31, United States
3 Code, as added by subsection (a).

4 (3) COVERED OFFICIAL DEFINED.—In this sub-
5 section, the term “covered official” has the meaning
6 given that term in section 1127(d) of title 31,
7 United States Code, as added by subsection (a).

8 (c) FEDERAL FUNDING ACCOUNTABILITY AND
9 TRANSPARENCY ACT OF 2006.—Section 7 of the Federal
10 Funding Accountability and Transparency Act of 2006
11 (Public Law 109–282; 31 U.S.C. 6101 note) is amend-
12 ed—

13 (1) in paragraph (1), by striking “or” at the
14 end;

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

17 (3) by adding at the end the following new
18 paragraph:

19 “(3) information that the Director of National
20 Intelligence, in consultation with the Director of the
21 Office of Management and Budget, determines
22 would result in the exposure of classified programs
23 or activities, including such information that could,
24 when combined with other publicly available infor-
25 mation, reveal classified programs or activities.”.

1 **SEC. 804. REVIEW BY COMMITTEE ON FOREIGN INVEST-**
 2 **MENT IN THE UNITED STATES OF TRANS-**
 3 **ACTIONS IN REAL ESTATE NEAR INTEL-**
 4 **LIGENCE COMMUNITY FACILITIES.**

5 (a) IN GENERAL.—Section 721(a)(4) of the Defense
 6 Production Act of 1950 (50 U.S.C. 4565(a)(4)) is amend-
 7 ed—

8 (1) in subparagraph (B)(ii)(II)(bb)(AA), by in-
 9 serting “, facility owned or operated by an element
 10 of the intelligence community,” after “military in-
 11 stallation”; and

12 (2) in subparagraph (C)(ii), by inserting “, fa-
 13 cility owned or operated by an element of the intel-
 14 ligence community,” after “military installation”.

15 (b) APPLICABILITY.—The amendments made by sub-
 16 section (a) apply with respect to transactions proposed or
 17 pending on or after the date of the enactment of this Act.

18 **SEC. 805. INTELLIGENCE SUPPORT TO THE U.S. INTER-**
 19 **NATIONAL DEVELOPMENT FINANCE COR-**
 20 **PORATION.**

21 The Director of National Intelligence, in coordination
 22 with the heads of the other elements of the intelligence
 23 community, shall provide intelligence and analytic support
 24 to the U.S. International Development Finance Corpora-
 25 tion to ensure all projects of the Corporation are appro-
 26 priately informed and strategically executed in accordance

1 with the purpose of the Corporation as described in section
2 1412(b) of the BUILD Act of 2018 (22 U.S.C. 9612(b)).

3 **SEC. 806. ESTABLISHING PROCESSES AND PROCEDURES**
4 **FOR PROTECTING FEDERAL RESERVE INFOR-**
5 **MATION.**

6 (a) IN GENERAL.—The Director of National Intel-
7 ligence, in coordination with the Director of the Federal
8 Bureau of Investigation, and in consultation with the rel-
9 evant heads of the elements of the intelligence community,
10 as determined by the Directors, shall—

11 (1) brief the Board of Governors of the Federal
12 Reserve System on foreign threats to the Federal
13 Reserve System; and

14 (2) work with the Chair of the Board of Gov-
15 ernors of the Federal Reserve System to create and
16 implement standardized security and classification
17 measures for protecting information collected, gen-
18 erated, and stored by the Federal Reserve System.

19 (b) REPORT.—Not later than 180 days after the date
20 of the enactment of this Act, the Director of National In-
21 telligence, the Director of the Federal Bureau of Inves-
22 tigation, and the Chair of the Board of Governors of the
23 Federal Reserve System shall jointly submit to the appro-
24 priate congressional committees a report detailing the sta-

1 tus of implementing the security measures described in
 2 subsection (a).

3 (c) APPROPRIATE CONGRESSIONAL COMMITTEES DE-
 4 FINED.—In this section, the term “appropriate congres-
 5 sional committees” means—

6 (1) the congressional intelligence committees;

7 (2) the Committee on the Judiciary and the
 8 Committee on Banking, Housing, and Urban Affairs
 9 of the Senate; and

10 (3) the Committee on the Judiciary and the
 11 Committee on Financial Services of the House of
 12 Representatives.

13 **SEC. 807. AMENDMENTS TO PROHIBIT PAYMENTS TO OB-**
 14 **TAIN NATIONAL SECURITY INFORMATION OR**
 15 **APPROVALS.**

16 (a) EXPORT CONTROL REFORM ACT OF 2018.—Sec-
 17 tion 1756(c) of the Export Control Reform Act of 2018
 18 (50 U.S.C. 4815(c)) is amended—

19 (1) by inserting “, collected, or paid” after
 20 “charged”; and

21 (2) by inserting “or for the award of such li-
 22 cense or other authorization” after “this part”.

23 (b) PROTECTING AMERICANS FROM FOREIGN AD-
 24 VERSARY CONTROLLED APPLICATIONS ACT.—Section
 25 2(c) of the Protecting Americans from Foreign Adversary

1 Controlled Applications Act (15 U.S.C. 9901 note; Public
2 Law 118–50) is amended—

3 (1) in the subsection heading, by inserting “;
4 PROHIBITION” after “EXEMPTIONS”; and

5 (2) by adding at the end the following new
6 paragraph:

7 “(3) PROHIBITION.—No fee may be charged,
8 collected, or paid in connection with the execution of
9 a qualified divestiture.”.

10 (c) NATIONAL SECURITY ACT OF 1947.—Section 801
11 of the National Security Act of 1947 (50 U.S.C. 3161)
12 is amended by adding at the end the following new sub-
13 section:

14 “(c) No fee may be charged, collected, or paid in con-
15 nection access to classified information.”.

16 **SEC. 808. OFFENSES INVOLVING ESPIONAGE.**

17 (a) IN GENERAL.—Chapter 213 of title 18, United
18 States Code, is amended by adding at the end the fol-
19 lowing:

20 **“§ 3302. Espionage offenses**

21 “Notwithstanding any other provision of law, an in-
22 dictment may be found or an information may be insti-
23 tuted at any time without limitation for a violation of sec-
24 tion 794 or a conspiracy to violate such section.”.

1 (b) CLERICAL AMENDMENT.—The table of sections
 2 for chapter 213 of title 18, United States Code, is amend-
 3 ed by adding at the end the following:

“3302. Espionage offenses.”.

4 (c) CONFORMING AMENDMENT.—Section 19 of the
 5 Internal Security Act of 1950 (18 U.S.C. 792 note; 64
 6 Stat. 1005) is amended by striking “, 793, or 794” and
 7 inserting “or 793”.

8 **SEC. 809. PARENTAL BEREAVEMENT LEAVE.**

9 Section 6329d(b)(1) of title 5, United States Code,
 10 is amended by inserting “, including any instance of the
 11 natural or spontaneous loss of an unborn child (as defined
 12 in section 1841(d) of title 18), such as through mis-
 13 carriage, stillbirth, or a loss that occurs due to a medical
 14 intervention for a pregnancy emergency, such as the treat-
 15 ment of an ectopic pregnancy” after “of the employee”.

16 **SEC. 810. DEFINITION OF FOREIGN INSTRUMENTALITY FOR**
 17 **PURPOSES OF ECONOMIC ESPIONAGE PROHI-**
 18 **BITION.**

19 Section 1839(1) of title 18, United States Code, is
 20 amended—

21 (1) by striking “that is substantially owned”
 22 and inserting the following: “that is—

23 “(A) substantially owned”; and

24 (2) by adding at the end the following: “or

1 “(B) domiciled in a covered nation, as de-
2 fined in section 4872 of title 10;”.

3 **SEC. 811. PROTECTION OF TRADE SECRETS.**

4 (a) **REQUIRING ADVANTAGE TO FOREIGN ENTITY OR**
5 **INJURY TO UNITED STATES UNDER ECONOMIC ESPIO-**
6 **NAGE STATUTE.**—Section 1831(a) of title 18, United
7 States Code, is amended, in the matter preceding para-
8 graph (1), by striking “benefit any foreign government,
9 foreign instrumentality, or foreign agent” and inserting
10 “provide any advantage to a foreign government, foreign
11 instrumentality, or foreign agent, or injure or disadvan-
12 tage in any way the United States, an instrumentality of
13 the United States, or an agent of the United States”.

14 (b) **EXTENDING JURISDICTION OVER ECONOMIC ES-**
15 **PIONAGE AND TRADE SECRET OFFENSES.**—Section 1837
16 of title 18, United States Code, is amended—

17 (1) in paragraph (1), by striking “or” at the
18 end;

19 (2) in paragraph (2), by striking the period at
20 the end and inserting a semicolon; and

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

22 “(3) the victim is—

23 “(A) a natural person who is a citizen or
24 permanent resident alien of the United States;

25 or

1 “(B) a person, including an organization,
2 headquartered or incorporated in the United
3 States; or

4 “(4) an act committed in furtherance of the of-
5 fense used or took place through—

6 “(A) communications in interstate or for-
7 eign commerce; or

8 “(B) financial infrastructure in the United
9 States.”.

10 (c) CRIMINALIZING UNAUTHORIZED TRANSMISSION
11 OF TRADE SECRETS OUTSIDE THE UNITED STATES.—
12 Section 1832 of title 18, United States Code, is amended
13 by adding at the end the following:

14 “(c) TRANSMISSION OF TRADE SECRETS OUTSIDE
15 THE UNITED STATES.—

16 “(1) OFFENSE.—It shall be unlawful for a per-
17 son to, without authorization, knowingly—

18 “(A) transmit a trade secret outside the
19 United States;

20 “(B) attempt to commit an offense de-
21 scribed in subparagraph (A); or

22 “(C) conspire with one or more other per-
23 sons to commit an offense described in subpara-
24 graph (A).

25 “(2) PENALTIES.—

1 “(A) IN GENERAL.—Except as provided in
 2 subparagraph (B), any person who violates
 3 paragraph (1) shall be fined not more than
 4 \$5,000,000, imprisoned not more than 5 years,
 5 or both.

6 “(B) ORGANIZATIONS.—Any organization
 7 that commits an offense described in paragraph
 8 (1) shall be fined not less than 3 times the
 9 value of the stolen trade secret to the victim, in-
 10 cluding expenses for research and design and
 11 other costs of reproducing the trade secret that
 12 the organization has thus avoided.”.

13 (d) CRIMINALIZING INCITING ECONOMIC ESPIONAGE
 14 AND THEFT OF TRADE SECRETS.—Chapter 90 of title 18,
 15 United States Code, is amended—

16 (1) in section 1831, by adding at the end the
 17 following:

18 “(c) INCITEMENT OR SOLICITATION OF ECONOMIC
 19 ESPIONAGE.—

20 “(1) IN GENERAL.—It shall be unlawful for a
 21 person to solicit, command, induce, or otherwise en-
 22 deavor to persuade another person to engage in an
 23 offense described in subsection (a).

1 “(2) PENALTIES.—Any person who violates
2 paragraph (1) shall be fined under this title or im-
3 prisoned not more than 10 years, or both.”; and

4 (2) in section 1832, as amended by subsection
5 (c), by adding at the end the following:

6 “(d) INCITEMENT OR SOLICITATION OF THEFT OF
7 TRADE SECRETS.—

8 “(1) IN GENERAL.—It shall be unlawful for a
9 person to solicit, command, induce, or otherwise en-
10 deavor to persuade another person to engage in an
11 offense described in subsection (a) or (c).

12 “(2) PENALTIES.—Any person who violates
13 paragraph (1) shall be fined under this title or im-
14 prisoned not more than 10 years, or both.”.

15 (e) DEFINITION OF FOREIGN INSTRUMENTALITY FOR
16 PURPOSES OF ECONOMIC ESPIONAGE PROHIBITION.—
17 Section 1839(1) of title 18, United States Code, is amend-
18 ed—

19 (1) by striking “that is substantially owned”
20 and inserting the following: “that is—

21 “(A) substantially owned”; and

22 (2) by adding at the end the following: “or

23 “(B) domiciled in a covered nation, as de-
24 fined in section 4872 of title 10;”.

1 **SEC. 812. TECHNICAL AMENDMENTS.**

2 (a) DEFINITION OF ARMED FORCES IN NATIONAL
3 SECURITY ACT OF 1947.—Section 605(8) of the National
4 Security Act of 1947 (50 U.S.C. 3126(8)) is amended by
5 inserting “Space Force,” after “Marine Corps,”.

6 (b) NATIONAL INTELLIGENCE UNIVERSITY.—Section
7 6801(a)(4) of the Intelligence Authorization Act for Fiscal
8 Year 2026 (Public Law 119–60) is amended in the matter
9 preceding subparagraph (A) by striking “3327” and in-
10 serting “3227”.

Calendar No. 420

119TH CONGRESS
2^D Session

S. 4615

A BILL

To authorize appropriations for fiscal year 2027 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.

MAY 20, 2026

Read twice and placed on the calendar