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.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Intelligence Authorization Act for Fiscal Year 2027".

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

SEC. 2. DEFINITIONS.

In this Act:

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

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

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 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.

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

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

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

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2027 the sum of $568,000,000.

(b) CLASSIFIED AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2027 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a).

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

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

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund $514,000,000 for fiscal year 2027.

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.

(a) REDESIGNATION OF PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE AS DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE.—

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

(A) in the subsection heading, by striking ''PRINCIPAL''; and

(B) by striking ''Principal'' each place it appears.

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

(A) in the subsection heading, by striking ''PRINCIPAL''; and

(B) in paragraph (2)(B), by striking ''Principal''.

(3) ADDITIONAL CONFORMING AMENDMENT.—

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

(i) in section 103(c)(2) (50 U.S.C. 3025(c)(2)), by striking ''Principal'';

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

(iii) in section 106(a)(2)(A) (50 U.S.C. 3041(a)(2)(A)), by striking ''Principal''; and

(iv) in section 116(b) (50 U.S.C. 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

NATIONAL INTELLIGENCE'' and inserting ''DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE AND ASSISTANT DIRECTORS OF NATIONAL INTELLIGENCE''.

(2) TABLE OF CONTENTS.—The table of contents for such Act, in the matter preceding section 2 of such Act, is amended by striking the item relating to section 103A and inserting the following:

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

SEC. 302. REPEAL OF NATIONAL INTELLIGENCE MANAGEMENT COUNCIL.

(a) IN GENERAL.—Section 103M of the National Security Act of 1947 (50 U.S.C. 3034d) is repealed.

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

SEC. 303. REPEAL OF VARIOUS POSITIONS, UNITS, CENTERS, COUNCILS, AND OFFICES.

(a) INTELLIGENCE COMMUNITY CHIEF DATA OFFICER.—

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

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

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

(b) INTELLIGENCE COMMUNITY INNOVATION UNIT.—

(1) TERMINATION.—The Director of National Intelligence shall take such actions as may be necessary to terminate and wind down the operations of the Intelligence Community Innovation Unit before the date specified in paragraph (3).

(2) REPEAL.—

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

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

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

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

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

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

''(2) The term 'climate security' means the effects of climate change on the following:

''(A) The national security of the United States, including national security infrastructure.

''(B) Subnational, national, and regional political stability.

''(C) The security of allies and partners of the United States.

''(D) Ongoing or potential political violence, including unrest, rioting, guerrilla warfare, insurgency, terrorism, rebellion, revolution, civil war, and interstate war.''.

(3) CLERICAL AMENDMENT.—The table of contents for such Act, in the matter preceding section

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

(d) FRAMEWORK FOR CROSS-DISCIPLINARY EDUCATION AND TRAINING.—

(1) REPEAL.—Subtitle A of title X of the National Security Act of 1947 (50 U.S.C. 3191 et seq.) is amended by striking section 1002 (50 U.S.C. 3192).

(2) CLERICAL AMENDMENT.—The table of contents for such Act, in the matter preceding section 2 of such Act, is further amended by striking the item relating to section 1002.

(e) FOREIGN LANGUAGES PROGRAM.—

(1) TERMINATION.—The Director of National Intelligence shall take such actions as may be necessary to terminate and wind down the operations of the Foreign Languages Program before the date specified in paragraph (5).

(2) REPEALS.—Subtitle B of such title (50 U.S.C. 3201 et seq.) is amended by striking sections 1011 (50 U.S.C. 3201, relating to program on advancement of foreign languages critical to the intelligence community), 1012 (50 U.S.C. 3202, relating to education partnerships), and 1013 (50 U.S.C. 3203, relating to voluntary services).

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

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

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

(f) JOINT INTELLIGENCE COMMUNITY COUNCIL.—

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

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

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

striking ", as appropriate, after obtaining the advice of the Joint Intelligence Community Council,".

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

SEC. 304. TRANSFER OF NATIONAL INTELLIGENCE UNIVERSITY.

(a) TRANSFER.—The Director of National Intelligence shall transfer the functions of the National Intelligence University to the National Defense University described in section 2165 of title 10, United States Code.

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

(c) CONFORMING AMENDMENTS.—

(1) TITLE 10.—Section 2151(b) of title 10, United States Code, is amended by striking paragraph (3).

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

(A) by striking subparagraph (M); and

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

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

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

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

(a) DOMESTIC COUNTERTERRORISM INTELLIGENCE.—Subsection (e) of section 119 of the National Security Act of 1947 (50 U.S.C. 3056) is amended to read as follows:

''(e) LIMITATION ON DOMESTIC ACTIVITIES.—The Center may, consistent with applicable law, the direction of the President, and the guidelines referred to in section 102A(b), receive and retain intelligence pertaining to domestic terrorism (as defined in section 2331 of title 18, United States Code) to enable the Center to collect, retain,

and disseminate intelligence pertaining only to international terrorism (as defined in section 2331 of title 18, United States Code).''.

SEC. 306. TIMELY PROVISION OF SECURITY DIRECTION TO INTELLIGENCE COMMUNITY WHISTLEBLOWERS.

(a) INTELLIGENCE COMMUNITY EMPLOYEES.—Section 103H(k)(5)(D)(ii)(II) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)(D)(ii)(II)) is amended by inserting '', unless the Director does not provide such direction not later than 7 calendar days after the date on which the employee furnishes the statement required by subclause (I)'' after ''practices''.

(b) CENTRAL INTELLIGENCE AGENCY EMPLOYEES.—Section 17(d)(5)(D)(ii)(II) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)(D)(ii)(II)) is amended by inserting '', unless the Director does not provide such direction not later than 7 calendar days after the date on which the employee furnishes the statement required by subclause (I)'' after ''practices''.

SEC. 307. NOTIFICATION OF CERTAIN DECLASSIFICATIONS.

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

"SEC. 806. NOTIFICATION OF CERTAIN DECLASSIFICATIONS.

"(a) NOTIFICATION TO CONGRESS BY DIRECTOR OF NATIONAL INTELLIGENCE.—

"(1) IN GENERAL.—Immediately upon declassifying, downgrading, or directing the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities pursuant to section 3.1(c) of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or any successor order, the Director of National Intelligence, or the Principal Deputy Director of National Intelligence, as delegated by the Director of National Intelligence, shall notify the congressional intelligence committees and the Archivist of the United States in writing of such declassification, downgrading, or direction.

"(2) CONTENTS.—Each notification required by paragraph (1) shall include a copy of the information that has been, or has been directed to be, declassified or downgraded.

"(b) NOTIFICATION TO CONGRESS BY AGENCY HEAD.—

"(1) IN GENERAL.—Immediately upon the declassification of information pursuant to section 3.1(d) of Executive Order 13526, or any successor

order, the head, or senior official, of a relevant element of the intelligence community shall notify the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, and the Archivist of the United States in writing of such declassification.

''(2) CONTENTS.—Each notification required by paragraph (1) shall include a copy of the information that has been declassified.''.

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

''Sec. 806. Notification of certain declassifications.''.

SEC. 308. NO POLICE, SUBPOENA, OR LAW ENFORCEMENT POWERS OR INTERNAL SECURITY FUNCTIONS FOR DIRECTOR OF NATIONAL INTELLIGENCE.

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

''(z) NO POLICE, SUBPOENA, OR LAW ENFORCEMENT POWERS OR INTERNAL SECURITY FUNCTIONS.—The Director of National Intelligence shall have no police,

subpoena, or law enforcement powers or internal security functions.''.

TITLE IV—MATTERS RELATING TO THE CENTRAL INTELLIGENCE AGENCY

SEC. 401. EXTENSION OF CENTRAL INTELLIGENCE AGENCY AUTHORITY REGARDING UNMANNED AIRCRAFT SYSTEMS.

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

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

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

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

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

''(c) SPECIAL RULE.—With respect to a member of a qualifying Federal service who is an officer or employee of an element of the intelligence community, the term 'permanent duty station', as used in this section, shall exclude

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

SEC. 403. MODIFICATION RELATING TO SECURITY PERSONNEL AT CERTAIN INSTALLATIONS.

Section 15(a)(1)(D) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3515(a)(1)(D)) is amended by inserting ''or the National Reconnaissance Office'' after ''Office of the Director of National Intelligence''.

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.

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

''SEC. 23. AUTHORITY TO CORRELATE, EVALUATE, AND DISSEMINATE CERTAIN INTELLIGENCE.

''The Director of the National Security Agency may—

''(1) correlate and evaluate intelligence related to national security; and

''(2) disseminate such intelligence to legislative and executive branch customers as the Director considers appropriate.''.

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

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

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

(a) IN GENERAL.—Subchapter I of chapter 21 of title 10, United States Code, is amended by inserting after section 421 the following:

''§ 421a. Funds for foreign intelligence activities conducted with and by the National Reconnaissance Office

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

priated funds available to the National Reconnaissance Office for intelligence and communications purposes to pay for the expenses of arrangements with foreign countries for intelligence activities conducted with and by the National Reconnaissance Office.

''(b) USE OF FUNDS OTHER THAN APPROPRIATED FUNDS.—The Director of the National Reconnaissance Office may use funds other than appropriated funds to pay for the expenses of arrangements with foreign countries for intelligence activities conducted with and by the National Reconnaissance Office without regard for the provisions of law relating to the expenditure of United States Government funds, except that—

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

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

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

''(c) REPORTS.—

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

''(A) the Select Committee on Intelligence, the Committee on Armed Services, and the Subcommittee on Defense of the Committee on Appropriations of the Senate; and

''(B) the Permanent Select Committee on Intelligence, the Committee on Armed Services, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives.

''(2) USE OF FUNDS OTHER THAN APPROPRIATED FUNDS.—Funds expended under the authority of subsection (b) shall be reported to the committees described in paragraph (1) pursuant to procedures jointly agreed upon by such committees and the Director of the National Reconnaissance Office.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such subchapter is amended by inserting after the item relating to section 421 the following:

''421a. 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.

Section 512A(b)(6) of the National Security Act of 1947 (50 U.S.C. 3111a(b)(6)) is amended by striking ''country affiliation'' and inserting ''terrorist organization''.

SEC. 505. ESTABLISHMENT OF OFFICE OF COUNTERINTELLIGENCE.

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

(1) in subsection (a)—

(A) in paragraph (2), by striking ''; and'' and inserting a semicolon;

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

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

''(3) identify and mitigate counterintelligence threats to the Department of the Treasury; and''; and

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

''(c) OFFICE OF COUNTERINTELLIGENCE.—There is established, within the Office of Intelligence and Analysis, the Office of Counterintelligence, which shall be responsible for implementing the policies and procedures across

the bureaus of the Department of the Treasury required to carry out the counterintelligence responsibilities described in subsection (a).''.

SEC. 506. MODIFICATION OF RESPONSIBILITIES OF OFFICE OF INTELLIGENCE AND ANALYSIS.

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

(1) in subsection (d)—

(A) in paragraph (1), by striking ''in support'' and all that follows through ''of the homeland.'' and inserting ''pertaining to foreign threats to the homeland, as determined by the Secretary.'';

(B) in paragraph (2)—

(i) by striking ''terrorist attacks within'' and inserting ''foreign threats to''; and

(ii) by striking ''attacks'' each place it appears and inserting ''threats'';

(C) in paragraph (3)(A), by striking ''terrorist and other'' and inserting ''foreign'';

(D) in paragraph (6), by striking ''terrorist attacks against'' and inserting ''foreign threats to'';

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

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

(F) in paragraph (7), as so redesignated, by striking ''threats of terrorism'' and inserting ''foreign threats'';

(G) in paragraph (9), as so redesignated, by striking ''threats of terrorism in'' and inserting ''foreign threats to''; and

(H) in paragraph (12), as so redesignated, by striking '', other agencies'' and all that follows through ''by the Department,''; and

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

''(h) COLLECTION OF INTELLIGENCE AND INFORMATION.—In carrying out the duties and responsibilities of the Secretary pursuant to this section, the personnel of the Office of Intelligence and Analysis shall liaise and share intelligence and other information between federal agencies (including the components of the Department), State, local, or tribal governments, and the private sector.

''(i) PROHIBITION.—

''(1) UNITED STATES PERSON DEFINED.—In this subsection, the term 'United States person' means—

''(A) a United States citizen;

''(B) an alien known by the Office of Intelligence and Analysis to be a permanent resident alien;

''(C) an unincorporated association substantially composed of United States citizens or permanent resident aliens; or

''(D) a corporation incorporated in the United States, except for a corporation directed and controlled by 1 or more foreign governments.

''(2) IN GENERAL.—Notwithstanding any other provision of law, the Office of Intelligence and Analysis may not engage in the collection of information or intelligence targeting any United States person, or any clandestine collection.

''(j) INTELLIGENCE DEFINED.—In this section, the term 'intelligence' has the meaning given the terms foreign intelligence and counterintelligence, as defined paragraphs (2) and (3) of the National Security Act of 1947 (50 U.S.C. 3003(2),(3)).''.

SEC. 507. ROLE OF NATIONAL SECURITY AGENCY IN COLLECTION AND ANALYSIS OF SIGNALS INTELLIGENCE.

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

"SEC. 23. SIGNALS INTELLIGENCE.

''The Director of the National Security Agency shall—

''(1) provide overall direction for and coordination of the collection and analysis of signals intelligence by elements of the intelligence community authorized to undertake such collection and analysis; and

''(2) in coordination with other departments, agencies, and elements of the United States Government that are authorized to undertake such collection, ensure that—

''(A) the most effective use is made of resources; and

''(B) appropriate account is taken of the risks to the United States and those involved in such collection.''.

TITLE VI—GENERAL INTELLIGENCE COMMUNITY MATTERS

SEC. 601. AMENDMENTS TO PRESIDENTIAL APPOINTMENTS FOR INTELLIGENCE COMMUNITY POSITIONS.

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

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

"(c) There is a Deputy Director of the National Security Agency, who shall be appointed by the President, by and with the advice and consent of the Senate.".

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

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

"(c) DIRECTOR.—

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

Counterintelligence, who shall be appointed by the President, by and with the advice and consent of the Senate. The Director of the Office shall report directly to the Secretary.

''(2) TERM.—

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

''(B) REAPPOINTMENT.—The Director shall be eligible for reappointment for 1 or more terms.

''(3) QUALIFICATIONS.—The Director shall—

''(A) be an employee in the Senior Executive Service, the Senior Intelligence Service, the Senior National Intelligence Service, or any other Service that the Secretary, in coordination with the Director of National Intelligence, considers appropriate; and

''(B) have substantial expertise in matters relating to the intelligence community, including foreign intelligence and counterintelligence.''.

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

(d) APPOINTMENT OF DIRECTOR OF THE NATIONAL COUNTERTERRORISM CENTER.—Section 119(b)(1) of the National Security Act of 1947 (50 U.S.C. 3056(b)(1)) is amended by striking ''President, by and with the advice and consent of the Senate'' and inserting ''Director of National Intelligence''.

(e) APPOINTMENT OF DIRECTOR THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER.—Section 902(a) of the Intelligence Authorization Act for Fiscal Year 2003 (50 U.S.C. 3382(a)) is amended by striking ''President, by and with the advice and consent of the Senate'' and inserting ''Director of National Intelligence''.

(f) APPOINTMENT OF GENERAL COUNSEL OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.—Section 103C(a) of the National Security Act of 1947 (50 U.S.C. 3028(a)) is amended by striking ''by the President, by and with the advice and consent of the Senate'' and inserting ''by the Director of National Intelligence''.

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

SEC. 602. PROCEDURES REGARDING DISSEMINATION OF NONPUBLICLY AVAILABLE INFORMATION CONCERNING UNITED STATES PERSONS.

(a) PROCEDURES.—

(1) IN GENERAL.—Title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) is amended by adding at the end the following new section:

"SEC. 519. PROCEDURES REGARDING DISSEMINATION OF NONPUBLICLY AVAILABLE INFORMATION CONCERNING UNITED STATES PERSONS.

''(a) PROCEDURES.—The head of each element of the intelligence community, in consultation with the Director of National Intelligence, shall develop and maintain procedures for that element to respond to unmasking requests.

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

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

''(A) information that identifies the disseminated intelligence report containing the United States person identifying information requested;

''(B) the date the unmasking request was submitted to the disseminating element;

''(C) the name, title, and organization of the individual who submitted the unmasking request in an official capacity;

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

''(E) a fact-based justification describing why such United States person identifying information is required by each individual who will receive the information to carry out the duties of the individual.

''(2) An unmasking request may only be approved by the head of the disseminating element or by officers or employees of such element to whom the head has specifically delegated such authority. When the disseminating element is not the originating element of the United States person identifying information, the head of the disseminating element shall obtain the concurrence of the head or designee of the originating element before approving the unmasking request.

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

cluding the disposition of such requests, for not less than 10 years.

''(4) The records described in paragraph (3) shall include, with respect to each approved unmasking request—

''(A) the name and title of the individual of the disseminating element who approved the request; and

''(B) the fact-based justification for the request.

''(5) The procedures shall include an exception that—

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

''(B) requires that promptly after such disclosure, the recipient of the United States person identifying information make a written unmasking request with respect to such information.

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

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

"(A) the documentation required by paragraph (1) shall include whether—

"(i) the requesting entity knows or reasonably believes that any United States person identifying information sought is of an individual who is a member of the transition team as identified by an apparent successful candidate for the office of President or Vice President; or

"(ii) based on the intelligence report to which the unmasking request pertains, the disseminating element or the originating element knows or reasonably believes that any United States person identifying information sought is of an individual who is a member of the transition team as identified by an apparent successful candidate for the office of President or Vice President;

"(B) the approval made pursuant to paragraph (2) of an unmasking request that contains United States person identifying information described in subparagraph (A) shall be

subject to the concurrence of the general counsel of the disseminating element (or, in the absence of the general counsel, the principal deputy general counsel, or, as applicable, the senior Departmental legal officer supporting the disseminating element) that the dissemination of such United States person identifying information is in accordance with the procedures required by subsection (a); and

''(C) consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the head of the disseminating element shall notify the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, and the majority leader and minority leader of the Senate of an approval described in subparagraph (B) not later than 14 days after the date of such approval.

''(7) If an unmasking request concerns a nominee for or the holder of a Federal office, a member of a transition team as identified by an eligible can-

didate for the office of the President, a Justice of the Supreme Court of the United States, or an individual nominated by the President to be a Justice of the Supreme Court of the United States, and such unmasking request is approved, the head of the disseminating element shall submit the documentation for the request to the congressional intelligence committees not later than 14 days after the date of such approval.

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

''(1) the total number of unmasking requests received by that element;

''(2) of such total number, the number of requests approved;

''(3) of such total number, the number of requests denied; and

''(4) for each number calculated under paragraphs (1) through (3), the number disaggregated by requesting entity.

''(d) CERTAIN PROCEDURES REGARDING CONGRESSIONAL IDENTITY INFORMATION.—With respect to the

dissemination of congressional identity information, the head of each element of the intelligence community shall carry out this section in accordance with annex A of Intelligence Community Directive 112, or successor annex or directive.

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

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

''(2) any procedures governing the collection, retention, or dissemination of information concerning United States persons established under Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities) or successor order; and

''(3) any other provision of statute or Executive order the Director of National Intelligence considers relevant.

''(f) DEFINITIONS .—In this section:

''(1) APPARENT SUCCESSFUL CANDIDATE.—The term 'apparent successful candidate' means any apparent successful candidate for the office of President or Vice President as determined pursuant to

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

''(2) CANDIDATE; FEDERAL OFFICE.—The terms 'candidate' and 'Federal office' have the meanings given those terms in section 301 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101).

''(3) CONGRESSIONAL IDENTITY INFORMATION.—The term 'congressional identity information' means information that identifies, by name or by individually identifying titles or characteristics—

''(A) any current Member of the Senate or the House of Representatives;

''(B) any current staff officer for any Senator or Representative, whether paid or unpaid; or

''(C) any current staff officer of any committee of the Senate or the House of Representatives, whether paid or unpaid.

''(4) DISSEMINATING ELEMENT.—The term 'disseminating element' means an element of the intelligence community that disseminated an intelligence report subject to an unmasking request.

''(5) ELIGIBLE CANDIDATE.—The term 'eligible 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')—

''(i) means information that is reasonably likely to identify one or more specific United States persons; and

''(ii) includes a single item of information and information that, when combined with other information, is reasonably likely to identify one or more specific United States persons.

''(B) DETERMINATION.—The determination of whether information is reasonably likely to identify one or more specific United States persons may require assessment by a trained intelligence professional on a case-by-case basis.

''(10) UNMASKING REQUEST.—The term 'unmasking request' means a request to gain access to nonpublic United States person identifying information concerning a known unconsenting United States person that was omitted from a disseminated intelligence report by the originating element.''.

(2) CLERICAL AMENDMENT.—The table of contents preceding section 2 of such Act is amended by inserting after the item relating to section 518 the following new item:

''Sec. 519. Procedures regarding dissemination of nonpublicly available information concerning United States persons.''.

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

(c) PUBLIC RELEASE.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall make publicly available the procedures for each element of the intelligence community required by section 519(a) of the National Security Act of 1947, as added by subsection (a)(1).

SEC. 603. ANALYTIC STANDARDS FOR ALL-SOURCE INTELLIGENCE PRODUCTS.

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

"SEC. 1115. ANALYTIC STANDARDS FOR ALL-SOURCE INTELLIGENCE PRODUCTS.

''(a) DEFINITIONS.—In this section:

''(1) ALL-SOURCE INTELLIGENCE PRODUCT.—The term 'all-source intelligence product'—

''(A) means any intelligence product published by an element of the intelligence community using multiple types of intelligence for pur-

poses of providing an analytic assessment or situational update; and

"(B) does not include a product containing purely law enforcement information.

"(2) ASSUMPTION.—The term 'assumption' means a supposition used to frame or support an argument.

"(3) JUDGMENT.—The term 'judgment' means a conclusion based on underlying intelligence information, analysis, and assumptions.

"(b) ESTABLISHMENT.—

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

"(A) the analytic standards described in subsection (c); and

"(B) any guidance or policy issued under paragraph (2).

"(2) GUIDANCE AND POLICY.—The Director of National Intelligence or any other head of an element of the intelligence community may issue guidance or policy that expands upon the standards described in subsection (c) as such head considers appropriate, except that any such guidance or policy shall not contradict or otherwise circumvent such standards.

''(c) ANALYTIC STANDARDS.—The standards described in this subsection are the following:

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

''(A) shall—

''(i) perform the analyst's functions with objectivity and with awareness of their own assumptions and reasoning;

''(ii) employ reasoning techniques and practical mechanisms that reveal and mitigate bias;

''(iii) be alert to influence by existing analytic positions or judgments; and

''(iv) consider alternative perspectives and contrary information; and

''(B) shall not be unduly constrained by previous judgments when new developments indicate a modification is necessary.

''(2) INDEPENDENT OF POLITICAL CONSIDERATION.—Any all-source intelligence product shall not be—

''(A) distorted by, or shaped for, advocacy of a particular audience, agenda, or policy viewpoint; or

''(B) influenced by the force of preference for a particular policy.

''(3) TIMELY.—Any all-source intelligence product shall be disseminated in time for the product to be actionable by customers.

''(4) BASED ON ALL RELEVANT INFORMATION AVAILABLE.—Any all-source intelligence product shall be informed by all relevant information available.

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

''(A) SOURCING.—Any all-source intelligence product shall—

''(i) identify and properly describe the quality and credibility of underlying sources, data, and methodologies upon which judgments are based; and

''(ii) use source descriptors in accordance with sourcing guidance prescribed by the Director of National Intelligence.

''(B) UNCERTAINTY.—Any all-source intelligence product shall—

''(i) indicate and explain the basis for the uncertainties associated with major

analytic judgments, specifically the likelihood of occurrence of an event or development, and the analyst's confidence in the basis for the judgment;

"(ii) note causes of uncertainty, including assumptions and gaps, and explain how uncertainties affect analysis; and

"(iii) for expressions of likelihood or probability, use one of the sets of terms defined in Intelligence Community Directive 203.

"(C) DISTINGUISHING.—Any all-source intelligence product shall—

"(i) clearly distinguish statements that convey underlying intelligence information used in analysis from statements that convey assumptions or judgments;

"(ii) state an assumption explicitly when the assumption serves as the linchpin of an argument or when the assumption bridges key information gaps;

"(iii) explain the implications for judgments if assumptions prove to be incorrect; and

"(iv) as appropriate, identify indicators that, if detected, would alter judgments.

"(D) INCORPORATE ANALYSIS OF ALTERNATIVES.—Any all-source intelligence product shall—

"(i) identify and assess plausible alternative hypotheses;

"(ii) in discussing alternatives, address factors such as associated assumptions, likelihood, or implications related to United States interests; and

"(iii) identify indicators that, if detected, would affect the likelihood of identified alternatives.

"(E) RELEVANCE.—Any all-source intelligence product shall provide information and insight on United States national security issues.

"(F) ARGUMENTATION.—Any all-source intelligence product shall—

"(i) present a clear main analytic message up front;

"(ii) in the case of a product containing multiple judgments, have a main

analytic message that is drawn collectively from those judgments; and

''(iii) be effectively supported by relevant intelligence information and coherent reasoning.

''(G) ANALYTIC LINE.—Any all-source intelligence product shall—

''(i) state how its major judgments on a topic are consistent with or represent a change from major judgments in previously published analysis, or that it represent initial coverage of a topic; and

''(ii) fully consider and bring to the attention of customers significant differences in analytic judgment, such as between two analytic elements of the intelligence community.

''(H) ACCURACY.—Any all-source intelligence product shall—

''(i) apply expertise and logic to make the most accurate judgments and assessments possible, based on the information available and known information gaps; and

''(ii) express judgments as clearly and precisely as possible, reducing ambiguity

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

''(I) VISUALS.—Any all-source intelligence product shall incorporate effective visual information as appropriate. Any content of any all-source intelligence product depicted visually shall adhere to the analytic standards described in this subsection.

''(d) REQUIRED INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), any all-source intelligence product shall include a section dedicated to explaining the tradecraft related to the analytic tradecraft standards described in subparagraphs (A), (B), (C), (D), and (G) of subsection (c)(5).

''(2) EXCEPTIONS.—The requirement of paragraph (1) shall not apply to—

''(A) any all source-intelligence product less than 300 words; or

''(B) any all-source intelligence product produced for the President's Daily Brief.

''(e) TRACKING ADHERENCE TO ANALYTIC STANDARDS.—The Director of National Intelligence and each other head of an element of the intelligence community shall—

''(1) develop metrics for evaluating the performance of their respective element in adhering to the analytic standards described in subsection (c); and

''(2) use such metrics to evaluate individual performance, develop analytic workforce training, and inform Congress on matters related to analytic performance.''.

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

''Sec. 1115. Analytic standards for all-source intelligence products.''.

SEC. 604. LIMITATION ON USE OF INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT FUNDS FOR CERTAIN ENTITIES.

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

''SEC. 314. LIMITATION ON USE OF INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT FUNDS FOR CERTAIN ENTITIES.

''Amounts appropriated for the Intelligence Community Management Account may not be obligated or expended to provide financial or in-kind support for the purposes of analytic collaboration, including for any study, research, or assessment, to—

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

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

''(2) an entity that is organized for research or for engaging in advocacy in areas such as public policy or political strategy that has received or expects to receive any financial or in-kind support from a government, or an entity affiliated with the military or intelligence services, of—

''(A) the People's Republic of China;

''(B) the Russian Federation;

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

''(D) the Islamic Republic of Iran;

''(E) the Bolivarian Republic of Venezuela; or

''(F) the Republic of Cuba.''.

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

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

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

SEC. 605. BEN SASSE INTELLIGENCE COMMUNITY TECHNOLOGY FELLOWSHIP PROGRAM.

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

"SEC. 1003. BEN SASSE INTELLIGENCE COMMUNITY TECHNOLOGY FELLOWSHIP PROGRAM.

"(a) IN GENERAL.—There is established a program (in this section referred to as the 'Program') under which selected employees of the intelligence community may train at certain nongovernmental entities as technology fellows.

"(b) DESIGNATION.—The program shall be known as the 'Ben Sasse Intelligence Community Technology Fellowship Program'.

"(c) AGREEMENTS.—

"(1) NONGOVERNMENTAL ENTITIES.—Each head of an element of the intelligence community described in paragraph (3) shall seek to enter into agreements with nongovernmental entities with expe-

rience in cutting-edge technology under which such entities may host technology fellows under the Program.

''(2) SELECTED EMPLOYEES.—For each employee of an element of the intelligence community selected for participation in the Program in accordance with subsection (e), the head of the element of the intelligence community that selected the employee shall provide for a written agreement among that element of the intelligence community, the nongovernmental entity concerned, and the employee. The agreement shall—

''(A) require that the employee of the element of the intelligence community, upon completion of the fellowship, serve in that element, or elsewhere in the intelligence community if approved by the head of the element that selected the employee, for a period equal to twice the length of the fellowship;

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

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

''(C) contain language ensuring that the employee of the element of the intelligence community does not improperly use information that the employee knows relates to an acquisition or procurement of the element of the intelligence community for the benefit or advantage of the nongovernmental entity.

''(3) ELEMENTS DESCRIBED.—The elements of the intelligence community described in this paragraph are the following:

''(A) The Central Intelligence Agency.

''(B) The National Security Agency.

''(C) The National Geospatial-Intelligence Agency.

''(D) The National Reconnaissance Office.

''(E) The Defense Intelligence Agency.

''(d) BOARD.—

''(1) IN GENERAL.—There is established a board for the Program (in this section referred to as the 'Board').

''(2) MEMBERSHIP.—The Board shall be composed of the directors of science and technology, or

equivalents, of the elements of the intelligence community described in subsection (c)(3).

''(3) CO-CHAIRS.—The members of the Board shall serve as co-chairs of the Board.

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

''(e) SELECTION.—Each year, each head of an element of the intelligence community described in subsection (c)(3) shall select two employees of such element to participate in the Program.

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

(b) CLERICAL AMENDMENT.—The table of contents of such Act is amended by inserting after the item relating to section 1002 the following:

''Sec. 1003. Ben Sasse Intelligence Community Technology Fellowship Program.''.

SEC. 606. INTELLIGENCE COMMUNITY COUNTERINTELLIGENCE OFFICE AT THE DEPARTMENT OF COMMERCE.

(a) DEFINITIONS.—In this section:

(1) DEPARTMENT.—The term ''Department'' means the Department of Commerce.

(2) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

(b) ESTABLISHMENT OF INTELLIGENCE COMMUNITY COUNTERINTELLIGENCE OFFICE.—

(1) AGREEMENT WITH SECRETARY OF COMMERCE.—The Director of National Intelligence, acting through the Director of the National Counterintelligence and Security Center, shall seek to enter into an agreement with the Secretary under which the Director of National Intelligence and the Secretary shall establish within the Department, within the Office of Secretary, an office, which shall be known as the ''Intelligence Community Counterintelligence Office'', in accordance with this section.

(2) LOCATION.—The Intelligence Community Counterintelligence Office established pursuant to this section shall be physically located within the headquarters of the Department and within reasonable proximity to the offices of the leadership of the Department.

(3) SECURITY.—The Director of the National Counterintelligence and Security Center shall be responsible for the protection of classified information

and for the establishment and enforcement of all security-related controls within the Intelligence Community Counterintelligence Office.

(c) PERSONNEL.—

(1) DIRECTOR.—

(A) APPOINTMENT.—There shall be at the head of the Intelligence Community Counterintelligence Office a Director who is appointed by the Director of National Intelligence. The Director of the Intelligence Community Counterintelligence Office shall—

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

(ii) be an employee of the intelligence community with significant counterintelligence experience; and

(iii) serve for a period of 3 years.

(B) RESPONSIBILITIES.—The Director of the Intelligence Community Counterintelligence Office shall carry out the following responsibilities:

(i) Serving as the head of the Intelligence Community Counterintelligence Office, with supervisory responsibility for the Intelligence Community Counterintelligence Office and any other personnel assigned to the Intelligence Community Counterintelligence Office.

(ii) Advising the Secretary on counterintelligence and intelligence information.

(iii) Ensuring that counterintelligence threat information and, as appropriate, finished intelligence on topics related to the functions of the Department, are provided to appropriate personnel of the department or agency without delay.

(iv) Ensuring critical intelligence relevant to the Secretary is requested and disseminated in a timely manner.

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

(vi) Correlating and evaluating counterintelligence threats identified within intelligence community reporting, in coordination with the National Counterintelligence and Security Center, and providing appropriate dissemination of such intelligence to officials of the Department with a need-to-know.

(vii) Advising the Secretary on methods to improve the counterintelligence posture of the Department.

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

(ix) In coordination with the National Counterintelligence and Security Center, establishing counterintelligence partnerships to improve the counterintelligence defense of the Department.

(2) DEPUTY DIRECTOR.—There shall be within the Intelligence Community Counterintelligence Office a Deputy Director who is appointed by the Secretary, in coordination with the Director of National 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,

including employees assigned by program elements of the intelligence community and other Federal departments and agencies, as appropriate.

(C) JOINT DUTY OR ASSIGNED PERSONNEL REIMBURSEMENT.—The Director of National Intelligence shall reimburse a program element of the intelligence community or a Federal department or agency for any permanent change of station employee assigned to the Intelligence Community Counterintelligence Office from amounts authorized to be appropriated for the Office of the Director of National Intelligence.

(D) OPERATION UNDER AUTHORITY OF DIRECTOR OF NATIONAL INTELLIGENCE.—Employees assigned to the Intelligence Community Counterintelligence Office under this paragraph shall operate under the authorities of the Director of National Intelligence for the duration of their assignment or period of employment within the Intelligence Community Counterintelligence Office, except for temporary duty assignment employees.

(E) INCENTIVE PAY.—

(i) IN GENERAL.—An employee who accepts employment at the Intelligence Community Counterintelligence Office during the 120-day period after the date of the establishment of the Intelligence Community Counterintelligence Office shall receive an incentive payment, which shall be payable by the Director of National Intelligence, in an amount equal to 10 percent of the base annual pay of the employee. Such an employee who completes 2 years of service in the Intelligence Community Counterintelligence Office may receive an incentive payment in an amount equal to 10 percent of the base annual pay of the employee if the Director of the Intelligence Community Counterintelligence Office determines the performance of the employee is exceptional.

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

ligence Community Counterintelligence Office for a period of at least 2 years.

(d) FUNDING.—To the extent and in such amounts as specifically provided in advance in appropriations Acts for the purposes detailed in this subsection, the Director of National Intelligence may expend such sums as are authorized within the National Intelligence Program of the Office of the Director of National Intelligence for—

(1) the renovation, furnishing, and equipping of a Federal building, as necessary, to meet the security and operational requirements of the Intelligence Community Counterintelligence Office;

(2) the provision of connectivity to the Intelligence Community Counterintelligence Office to enable briefings, secure audio and video communications, and collaboration between employees of the Department and the intelligence community at the unclassified, secret, and top secret levels;

(3) the provision of other information technology systems and devices, such as computers, printers, and phones, for use by employees of the Intelligence Community Counterintelligence Office;

(4) the assignment of employees of the intelligence community to support the operation of the

Intelligence Community Counterintelligence Office; and

(5) the provision of other personal services necessary for the operation of the Intelligence Community Counterintelligence Office.

(e) DEADLINE FOR ESTABLISHMENT OF THE INTELLIGENCE COMMUNITY COUNTERINTELLIGENCE OFFICE.—

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

(2) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a report on the plan to establish the Intelligence Community Counterintelligence Office required under paragraph (1). Such report shall include the costs and schedule associated with establishing the Intelligence Community Counterintelligence Office.

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

(a) FINDINGS.—Congress finds the following:

(1) In 2025, foreign malicious cybercriminal organizations, such as foreign scam centers that engage in sophisticated investment fraud, cyber-enabled extortion activity, and impersonation-based fraud, stole at least $7,566,000,000 from Americans according to the Federal Bureau of Investigation's Internet Crime Complaint Center, which has emphasized that these estimates are conservative and only includes losses reported to the Federal Bureau of Investigation.

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

(3) Investigative reporting, Federal indictments, and sanctions designations issued by the Department of the Treasury have revealed the extent to which foreign malicious cybercriminal organizations collaborate with foreign governments, illicit finance actors, and foreign militia groups whose activities present a threat to the economic and national security of the United States.

(4) Foreign malicious cybercriminal organizations rely extensively on communications and finan-

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

(5) Financial insecurity generated by foreign malicious cybercriminal organizations presents a counterintelligence threat to the United States intelligence community.

(b) SENSE OF CONGRESS.—

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

(A) foreign malicious cybercriminal organizations, and foreign affiliates associated with those organizations, constitute hostile foreign cyber actors and are valid targets for intelligence operations under existing intelligence authorities; and

(B) the Director of National Intelligence should treat collection, analysis, and disruption toward hostile foreign cyber actors as a national intelligence priority as part of the National Intelligence Priorities Framework.

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

(A) Prince Group.

(B) Huione Group.

(C) L.Y.P. Group.

(D) Jin Bei Group.

(E) Funnull Technology Inc.

(F) TransAsia International holding Group Thailand Company Limited.

(G) The Democratic Karen Benevolent Army.

(H) HH Bank Cambodia PLC.

(c) REPORT.—

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

(2) CONTENTS.—The report required by paragraph (1) shall include the following:

(A) An identification of the individuals and entities operating as hostile foreign cyber actors, including foreign scam centers, that pose the most significant threat.

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

(C) A description of the infrastructure, tactics, and techniques hostile foreign cyber actors, including foreign scam centers, commonly use, including reliance on any products or services subject to the jurisdiction of the United States.

(D) A description of any relationships between the individuals and entities that operate as hostile foreign cyber actors, including foreign scam centers, and their governments or countries of origin that could impede the ability to counter threats from such centers.

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

(F) A description of any relationships that the individuals and entities identified under subparagraph (A) have with transnational organized crime groups.

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

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

SEC. 608. NOTIFICATION OF CRIMINAL REFERRALS REGARDING CURRENT OR FORMER INTELLIGENCE COMMUNITY EMPLOYEES.

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

"SEC. 519. NOTIFICATION OF CRIMINAL REFERRALS REGARDING CURRENT OR FORMER INTELLIGENCE COMMUNITY EMPLOYEES.

''If an element of the intelligence community makes a criminal referral to the Department of Justice regarding a current or former employee of any element of the intelligence community, the general counsel of the element of the intelligence community that made the referral shall notify the congressional intelligence committees of the referral on the date such referral is made and provide to the congressional intelligence committees a summary of the referral.''.

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

''Sec. 519. 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.

(a) DEFINITIONS.—Section 3 of the National Security Act of 1947 (50 U.S.C. 3003) is amended—

(1) in paragraph (1), by striking ''includes'' and inserting ''means''; and

(2) in paragraph (5)—

(A) in the matter before subparagraph (A), by striking ''refer to all'' and inserting ''means'';

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

''(B) involves foreign threats to the United States, its people, property, or interests.''.

(b) SCOPE OF INTELLIGENCE SHARING RESPONSIBILITIES.—Section 102A(f)(1) of such Act (50 U.S.C. 3024(f)(1)) is amended, in the first sentence, by inserting '', and other Federal agencies as the Director considers appropriate,'' after ''community''.

SEC. 610. PROHIBITION ON INTELLIGENCE COMMUNITY USE OF ADVERSARY UNMANNED GROUND VEHICLES.

(a) DEFINITIONS.—In this section:

(1) COVERED FOREIGN COUNTRY.—The term ''covered foreign country'' means any of the following:

(A) The People's Republic of China.

(B) The Russian Federation.

(C) The Islamic Republic of Iran.

(D) The Democratic People's Republic of Korea.

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

(3) COVERED UNMANNED GROUND VEHICLE SYSTEM.—The term ''covered unmanned ground vehicle system''—

(A) means a mechanical device that—

(i) is capable of locomotion, navigation, or movement on the ground; and

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

(B) includes—

(i) remote surveillance vehicles, autonomous patrol technologies, mobile robotics, and humanoid robots; and

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

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

(1) IN GENERAL.—Except as provided under paragraph (2), the head of an element of the intelligence community may not procure any covered unmanned ground vehicle system that is manufactured or assembled by a covered foreign entity.

(2) EXEMPTION.—The heads of elements of the intelligence community are exempt from the restriction under paragraph (1) if the procurement is required in the national interest of the United States and—

(A) is for the sole purposes of research, evaluation, training, testing, or analysis for electronic warfare, information warfare operations, cybersecurity, or development of unmanned ground vehicle system or counter-unmanned 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-

cle system manufactured or assembled by a covered foreign entity.

(B) APPLICABILITY TO CONTRACTED SERVICES.—The prohibition under subparagraph (A) applies to any covered unmanned ground vehicle systems that are being used by any element of the intelligence community through the method of contracting for the services of covered unmanned ground vehicle systems.

(2) EXEMPTION.—The heads of the elements of the intelligence community are exempt from the restriction under paragraph (1) if the operation is required in the national interest of the United States and—

(A) is for the sole purposes of research, evaluation, training, testing, or analysis for electronic warfare, information warfare operations, cybersecurity, or development of unmanned ground vehicle system or counter-unmanned 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 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—

(A) to procure a covered unmanned ground vehicle system that is manufactured or assembled by a covered foreign entity; or

(B) in connection with the operation of such a robot or unmanned ground vehicle system.

(2) EXEMPTION.—The heads of elements of the intelligence community are exempt from the restriction under paragraph (1) if the procurement or operation is required in the national interest of the United States and—

(A) is for the sole purposes of research, evaluation, training, testing, or analysis for electronic warfare, information warfare operations, cybersecurity, or development of unmanned ground vehicle system or counter-unmanned 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 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.

SEC. 611. CHINA-TAIWAN STRATEGIC WARNING TASK FORCE.

(a) ESTABLISHMENT.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence and the Undersecretary of Defense for Intelligence and Security shall establish a task force to be known as the China-Taiwan Strategic Warning Task Force (referred to in this section as the ''Task Force'') to lead the efforts of the intelligence community with respect to providing indications and warning of any military aggression by the People's Republic of China against Taiwan.

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

(1) The synchronization of all intelligence community efforts related to China-Taiwan indications

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

(2) The coordination of analysis related to China-Taiwan indications and warning and the development of analytic methodologies for use across the intelligence community in conducting analysis related to China-Taiwan indications and warning.

(3) The development and implementation of information technology solutions to synchronize the access of the intelligence community to information relating to indications and warning.

(c) MEMBERSHIP.—The Task Force shall be composed of the following members (or their designees):

(1) The Director of National Intelligence.

(2) The Undersecretary of Defense for Intelligence and Security.

(3) The Director of the Defense Intelligence Agency.

(4) The Director of the Central Intelligence Agency.

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

(6) The Director of the National-Geospatial Intelligence Agency.

(7) The Director of the National Security Agency.

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

(9) The Assistant Secretary of State for Intelligence and Research.

(10) Such other heads of the elements of the intelligence community that the Director of National Intelligence and the Undersecretary of Defense for Intelligence and Security determine appropriate.

(d) LEADERSHIP; ORGANIZATION; MEETINGS.—

(1) CO-CHAIRS.—The Director of National Intelligence (or a designee of the Director) and the Undersecretary of Defense for Intelligence and Security (or a designee of the Undersecretary) shall be co-chairs of the Task Force.

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

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

(e) STAFFING.—

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

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

(2) AGENCY LIAISON.—Each member listed in subsection (b) shall appoint a senior intelligence officer from the agency concerned to serve as a liaison to the Task Force. Such liaison shall be responsible for coordinating the participation and support of the agency concerned to the Task Force.

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

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

(2) a summary of efforts by the Task Force to develop a common set of indicators and organize collection efforts by the intelligence community against such indicators;

(3) a description of the resources provided by each Task Force member towards efforts with respect to China-Taiwan indications and warning, disaggregated by—

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

(B) total full-time equivalent personnel; and

(4) recommendations to improve the collection and analysis of the intelligence community with respect to China-Taiwan indications and warning.

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

SEC. 612. LIMITATIONS RELATING TO CHINESE PRODUCTS AND SERVICES.

(a) PROHIBITION ON USE BY INTELLIGENCE COMMUNITY.—

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

''(1) COVERED APPLICATION.—The term 'covered application' means—

''(A) the DeepSeek application or any successor application or service; or

"(B) any product or service from any entity of the People's Republic of China that is included on—

"(i) the Entity List maintained by the Bureau of Industry and Security of the Department of Commerce;

"(ii) the list (sometimes known as the 'Non-SDN Chinese Military-Industrial Complex Companies List') maintained by the Office of Foreign Assets Control of the Department of the Treasury under Executive Order 13959, as amended by Executive Order 14032 (50 U.S.C. 1701 note; relating to addressing the threat from securities investments that finance certain companies of the People's Republic of China), or any successor order; or

"(iii) the list of Chinese military companies required under section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (10 U.S.C. 113 note; Public Law 116–283) and maintained by the Department of Defense.".

(2) CONFORMING AMENDMENT.—The heading for such section is amended by striking ''**DEEPSEEK**'' and inserting ''**PRODUCTS AND SERVICES FROM PEOPLE'S REPUBLIC OF CHINA**''.

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

(1) in the section heading, by striking ''**BY FEDERAL BUREAU OF INVESTIGATION**'';

(2) in subsection (a)—

(A) in the matter before paragraph (1), by striking ''Director of the Federal Bureau of Investigation'' and inserting ''head of an element of the intelligence community'';

(B) in paragraph (1), by striking ''Federal Bureau of Investigation'' and inserting ''element''; and

(C) in paragraph (3), by striking ''Director (or a designee of the Director)'' and inserting ''head'';

(3) in subsection (b), by striking ''the Director (or a designee of the Director, as applicable) approves a recommendation pursuant to subsection

(a)(3), the Director shall'' and inserting ''the head of an element of the intelligence community approves a recommendation pursuant to subsection (a)(3), the head shall'';

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

''(2) PEOPLE'S REPUBLIC OF CHINA PRODUCT OR SERVICE.—The term 'People's Republic of China product or service' means—

''(A) an information or communication technology product manufactured in China, Hong Kong, or Macau and designed, developed, or maintained by a firm that is domiciled in China, Hong Kong, or Macau; or

''(B) an information or communication technology product or service provided or manufactured by—

''(i) an entity that is fully or partially owned or controlled by, or otherwise connected to, the government of China; or

''(ii) an entity included on the list submitted by the Director of National Intelligence under section 6706(c) of the Intelligence Authorization Act for Fiscal

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

SEC. 613. LIMITATION ON INTELLIGENCE COMMUNITY SUPPORT FOR OFFENSIVE CYBER OPERATIONS CONDUCTED BY NONGOVERNMENTAL ENTITIES.

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

''SEC. 1115. LIMITATION ON INTELLIGENCE COMMUNITY SUPPORT FOR OFFENSIVE CYBER OPERATIONS CONDUCTED BY NONGOVERNMENTAL ENTITIES.

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

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

''(2) is otherwise authorized by the President of the United States to conduct the offensive cyber operation.

''(b) DEFINITIONS.—In this section:

''(1) NONGOVERNMENTAL ENTITY.—The term 'nongovernmental entity' means any entity that is not an entity of the United States Government.

''(2) OFFENSIVE CYBER OPERATION.—The term 'offensive cyber operation' means any activity carried out in cyberspace, or any associated preparatory action, that affects an information system, network, or any other computer infrastructure that is not owned or lawfully operated by the entity carrying out the activity or action.''.

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

''Sec. 1115. Limitation on intelligence community support for offensive cyber operations conducted by nongovernmental entities.''.

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

(a) IN GENERAL.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by adding at the end the following:

''SEC. 124. BIOLOGICAL INTELLIGENCE ACTIVITIES OF THE INTELLIGENCE COMMUNITY.

''(a) DEFINITIONS.—In this section:

''(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

biological system, that is measured, collected, or aggregated for analysis, including information from humans, animals, plants, or microbes.

''(2) BIOLOGICAL INTELLIGENCE.—The term 'biological intelligence' includes the information collected or disseminated by the intelligence community concerning biological threats through genomic surveillance, immunological monitoring, environmental sampling, multiomic analysis, and other scientific methodologies.

''(3) BIOLOGICAL THREAT.—The term 'biological threat' includes any naturally occurring infectious disease, engineered pathogen, toxin, or other biological agent that poses a risk to human, animal, or plant health or to the national security of the United States.

''(b) DETERMINATION; DISSEMINATION.—The Director of National Intelligence, in such coordination with the Secretary of Defense as the Director considers appropriate, shall, consistent with applicable Federal law and Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities)—

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

tion, characterization, and attribution of foreign biological threats; and

''(2) disseminate such anonymized biological data and biological intelligence to agencies identified under paragraph (1).

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

''(1) ensure standards for the collection and data formats of anonymized biological data and biological intelligence are, to the extent possible, consistent with standards used by other United States agencies, including by—

''(A) providing for standardized data categorization and tagging of biological data;

''(B) considering standardized scientific and laboratory equipment and data collection methodologies; and

''(C) minimizing collection of any biological data that is likely to contain biological or genomic information specific to any United States person, including any derived data that is specific to any United States person; and

''(2) facilitate the establishment and maintenance of streamlined and unified accesses to databases of biological intelligence collected by the intelligence community or the Department of Defense.

''(d) PRIORITY.—In carrying out subsections (b) and (c), the Director of National Intelligence shall prioritize supporting capabilities, including the development of technical tools, that enable the early detection, characterization, and attribution of naturally occurring, novel, or engineered pathogens that could threaten the United States.''.

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

''Sec. 124. Biological intelligence activities of the intelligence community.''.

SEC. 615. PROHIBITION ON PARTICIPATION IN PREDICTION MARKETS.

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

''SEC. 304A. PROHIBITION ON PARTICIPATION IN PREDICTION MARKETS.

''(a) IN GENERAL.—Except as may be necessary to conduct authorized intelligence activities, a covered individual may not participate in a prediction market on any topic relating to nonpublic information to which the cov-

ered individual has access by virtue of being a covered individual, during—

''(1) the period during which the covered individual is employed or contracted by an element of the intelligence community; or

''(2) the two-year period beginning on the date on which the covered individual ceases to be employed or contracted by such an element.

''(b) POLICY.—Not later than 45 days after the date of the enactment of this section, the Director of National Intelligence shall issue a policy implementing the prohibition in subsection (a), including—

''(1) establishing appropriate penalties for violating the prohibition; and

''(2) providing notice to all covered individuals.

''(c) DEFINITIONS.—In this section:

''(1) COVERED INDIVIDUAL.—The term 'covered individual' means an employee or contractor, or a former employee or contractor, of an element of the intelligence community who holds a security clearance.

''(2) PREDICTION MARKET.—The term 'prediction market' means a platform, company, or service that allows agreements, contracts, transactions, or swaps between users over the outcome of non-fi-

nancial future events, such as sports, military actions, and elections.''.

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

''Sec. 304A. Prohibition on participation in prediction markets.''.

SEC. 616. REPEAL OF CERTAIN REPORT AND BRIEFING REQUIREMENTS.

(a) OVERSIGHT OF FOREIGN INFLUENCE IN ACADEMIA.—Section 5713 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3369b) is repealed.

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

(c) MONITORING MINERAL INVESTMENTS UNDER BELT AND ROAD INITIATIVE OF THE PEOPLE'S REPUBLIC OF CHINA.—Section 7003 of the Energy Act of 2020 (50 U.S.C. 3372) is amended by striking subsection (d).

(d) BRIEFING ON PROTOCOLS FOR CERTAIN INTELLIGENCE COMMUNITY EMPLOYEES AND DEPENDENTS.—Section 605(g) of the Intelligence Authorization Act for

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

(e) PROGRAM ON USE OF INTELLIGENCE RESOURCES IN EFFORTS TO SANCTION FOREIGN OPIOID TRAFFICKERS.—Section 7231 of the Fentanyl Sanctions Act (21 U.S.C. 2331) is amended—

(1) by striking subsection (c); and

(2) by redesignating subsection (d) as subsection (c).

(f) PERIODIC REPORT ON POSITIONS IN THE INTELLIGENCE COMMUNITY THAT CAN BE CONDUCTED WITHOUT ACCESS TO CLASSIFIED INFORMATION, NETWORKS, OR FACILITIES.—Section 6610 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3352e) is repealed.

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

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

and 2020 (50 U.S.C. 3370) is amended by striking subsection (e).

(i) REPORT ON BEST PRACTICES TO PROTECT PRIVACY, CIVIL LIBERTIES, AND CIVIL RIGHTS OF CHINESE AMERICANS.—Section 620 of the Intelligence Authorization Act for Fiscal Year 2021 (50 U.S.C. 3240) is repealed.

(j) ENFORCEMENT OF CYBERSECURITY REQUIREMENTS FOR NATIONAL SECURITY SYSTEMS; REPORT ON EXEMPTIONS.—Section 6309(f) of the Intelligence Authorization Act for Fiscal Year 2023 (44 U.S.C. 3557 note; division F of Public Law 117–263) is amended by striking paragraph (3).

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

(l) TIMELINESS STANDARD FOR RENDERING DETERMINATIONS OF TRUST FOR PERSONNEL VETTING; REVIEWS.—Section 7702(a) of the Intelligence Authorization Act for Fiscal Year 2024 (50 U.S.C. 3352h(a)) is amended by striking paragraph (2).

(m) BRIEFINGS ON STATUS OF INTELLIGENCE COMMUNITY INNOVATION UNIT.—Subsections (c) and (d) of section 7502 of the Intelligence Authorization Act for Fiscal Year 2024 (Public Law 118–31; 137 Stat. 1082) are repealed.

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

(1) by striking subsections (c) and (d); and

(2) by redesignating subsections (e) and (f) as subsections (c) and (d), respectively.

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

(p) SOFTWARE LICENSING.—Section 109 of the National Security Act of 1947 (50 U.S.C. 3044) is amended—

(1) by striking subsection (c); and

(2) by redesignating subsection (d) as subsection (c).

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

(1) by striking subsection (c); and

(2) by redesignating subsection (d) as subsection (c).

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

(1) by striking subsection (c); and

(2) by redesignating subsection (d) as subsection (c).

SEC. 617. INTELLIGENCE COMMUNITY PERSONNEL TRAVEL, ALLOWANCES, AND RELATED EXPENSES REGULATIONS.

(a) CENTRAL INTELLIGENCE AGENCY.—Section 4 of the Central Intelligence Act of 1949 (50 U.S.C. 3505) is amended by adding at the end the following new subsection:

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

''(1) review the regulations covered by this section; and

''(2) not later than 10 days after completing a review under paragraph (1), submit to the congressional intelligence committees the findings of the Director with respect to the review, including identification of any changes to the regulations or personnel coverage thereof that the Director determines to be necessary for the performance of intelligence functions.''.

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

''(z) BIENNIAL REVIEWS AND REPORTS REGARDING INTELLIGENCE COMMUNITY PERSONNEL TRAVEL, ALLOWANCES, AND RELATED EXPENSES REGULATIONS.—Not later than September 30, 2027, and not less frequently than once every 2 years thereafter, in order to reflect the requirements of the Office of the Director of National Intelligence not taken into account in the formulation of Government-wide travel procedures covered by this section, the Director shall—

''(1) review such requirements; and

''(2) not later than 10 days after completing a review under paragraph (1), submit to the congressional intelligence committees the findings of the Director with respect to the review, including any regulations that the Director determines to be necessary for the performance of intelligence functions.''.

SEC. 618. PROHIBITION ON SENDING AND RECEIVING OBJECTS USING ENTITIES OWNED OR CONTROLLED BY PERSONS OR GOVERNMENTS OF CERTAIN COUNTRIES.

(a) DEFINITION OF COVERED NATION.—In this section, the term ''covered nation'' has the meaning given such term in section 4872(f) of title 10, United States Code.

(b) IN GENERAL.—

(1) LIST REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, shall develop a list of products, intellectual property, technology, and any other objects that the Directors determine—

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

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

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

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

(d) WAIVER.—The head of an element of the intelligence community—

(1) may waive the prohibition in subsection (c) for the element on a case by case basis if the head determines that in the particular case, sending or receiving any product, intellectual property, technology, or other object by an entity identified pursuant to subsection (b) is necessary for the national security of the United States; and

(2) not later than 3 days after issuing such waiver, shall notify the Director of National Intelligence of the waiver.

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

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

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

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

(a) DEFINITION OF INTELLIGENCE COOPERATION.—In this section, the term ''intelligence cooperation'' means activities authorized under the provisions of law administered by the heads of the elements of the intelligence community, including the collection, analysis, production, and dissemination of information, intelligence, and imagery.

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

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

(c) REQUIREMENTS.—

(1) IN GENERAL.—The Director of National Intelligence shall, acting in close coordination with such heads of elements of the intelligence community as the Director considers relevant and the members of the Five Eyes intelligence-sharing alliance, undertake efforts to bolster and improve—

(A) the intelligence foundations of alliances between the United States and Australia, Japan, New Zealand, the Philippines, the Republic of Korea, and Thailand; and

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

(2) PRIORITY AREAS FOR ENHANCED COOPERATION.—Efforts undertaken pursuant to paragraph (1) shall include efforts—

(A) to address the speed and complexity of potential strategic and operational contingencies in the Indo-Pacific region, including any scenarios involving adversarial efforts to limit the

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

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

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

(D) to inform collective defense planning and response by further integrating intelligence cooperation into joint and combined operational planning activities, exercises, and wargames focused on regional contingencies, including the Rim of the Pacific;

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

(F) to promote multilateral intelligence sharing and collaboration among allies and partners of the United States, such as through the United States–Japan–Republic of Korea trilateral mechanism and the United States–Japan–Philippines trilateral mechanism.

SEC. 620. INTELLIGENCE ACTIVITIES RELATED TO UKRAINE.

(a) STATEMENT OF POLICY.—

(1) IN GENERAL.—Section 3 of the Support for the Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 (22 U.S.C. 8902) is amended—

(A) in paragraph (16), by striking ''; and'' and inserting a semicolon;

(B) in paragraph (17), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(18) to assist Ukraine in maintaining a credible defense and deterrence capability, including through the provision of intelligence support, as a means of advancing the national security of the United States, regional stability, and the protection of United States interests in Europe.''.

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

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

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

''(3) CREDIBLE DEFENSE AND DETERRENCE CAPABILITY.—The term 'credible defense and deter-

rence capability' means the ability to defend against and deter any credible conventional military threat from the Russian Federation acting unilaterally or in concert with partners, through the use of conventional military means, possessed in sufficient quantity, including weapons platforms and munitions, and command, control, communication, intelligence, surveillance, and reconnaissance capabilities.

''(4) INTELLIGENCE SUPPORT.—The term 'intelligence support' means activities authorized under the provisions of law governing the heads of the elements of the intelligence community, including the collection, analysis, production, and dissemination of information, intelligence, and imagery.''.

(b) REQUIREMENT RELATING TO INTELLIGENCE SUPPORT ABSENT AN ARMISTICE OR COMPREHENSIVE POLITICAL SETTLEMENT.—Until Ukraine and the Russian Federation voluntarily and freely enter into an armistice or comprehensive political settlement of the conflict, the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the Defense Intelligence Agency, and the heads of any other relevant element of the intelligence community, shall continue to ensure the provision of intelligence sup-

port to the Government of Ukraine for purposes of advancing United States policy goals in Ukraine.

(c) PAUSES IN INTELLIGENCE SUPPORT.—

(1) IN GENERAL.—Intelligence support to Ukraine required under this section shall not be suspended or limited unless the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency and the Director of the Defense Intelligence Agency, identifies a specific and identifiable national security concern.

(2) NOTIFICATION.—Not later than 15 days after making the decision to pause, terminate, restrict, or otherwise materially downgrade intelligence support to Ukraine, the Director of National Intelligence, in coordination with the heads of the elements of the intelligence community, shall submit to the congressional intelligence committees a notification that includes—

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

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

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

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

(d) REQUIREMENT RELATING TO INTELLIGENCE SUPPORT IN THE EVENT OF ARMISTICE OR COMPREHENSIVE POLITICAL SETTLEMENT.—

(1) IN GENERAL.—If Ukraine and the Russian Federation voluntarily and freely enter into an armistice or a comprehensive political settlement, the Director of National Intelligence, in coordination with the heads of the other relevant elements of the intelligence community, shall adjust the intelligence support to Ukraine to support implementation of the armistice or the comprehensive political settlement and, consistent with the national security interests of the United States, support building and sustaining the capacity of Ukraine to detect, deter, and repel any future Russian attack against the territory of Ukraine.

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

ical settlement is entered into force, the Director of the Central Intelligence Agency, in coordination with the heads of the other relevant elements of the intelligence community, including the Director of the Defense Intelligence Agency, the Director of the National Security Agency, and the Director of the National Geospatial-Intelligence Agency, shall submit to the congressional intelligence committees a report that includes—

(A) a description of the details of the armistice or the comprehensive political settlement of the conflict in Ukraine, including a description of the role of the intelligence community in monitoring the adherence by the parties to specific elements of the agreement;

(B) an assessment of the vulnerabilities that Ukraine will face under the terms of the agreement and potential measures that the intelligence community or other parties could take to help mitigate such vulnerabilities;

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

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

(D) an assessment of the implications of the armistice or comprehensive political settlement for the national security interests of the United States in Europe, including the capacity of the United States and the North Atlantic Treaty Organization to deter future aggression by the Russian Federation; and

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

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

(4) EARLY WARNING.—The Director of National Intelligence, in coordination with the heads of any other relevant elements of the intelligence community, shall provide to Ukraine and member coun-

tries of the North Atlantic Treaty Organization intelligence and early warning to allow for an appropriate and timely response with respect to any potential attack or act of aggression against Ukraine by the Russian Federation.

(5) NOTIFICATION.—

(A) IN GENERAL.—The Director of National Intelligence shall promptly notify each Member of the congressional intelligence committees not later than 5 days after any intelligence element provides Ukraine any intelligence pursuant to paragraph (4).

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

(i) a description of the specific threatened attack or act of aggression shared with Ukraine;

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

(iii) details of the channel through which the intelligence was shared, including the names and titles of the relevant intelligence community officers and Ukrainian government officials;

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

(v) an assessment produced by the Defense Intelligence Agency, in coordination with other relevant elements of intelligence community, as to what support Ukraine might require in order to deter or repel the threatened attack or act of aggression; and

(vi) a summary of subsequent actions that the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the Defense Intelligence Agency, and other heads of relevant elements of the intelligence community, directed be taken to support Ukraine in defending against or otherwise responding to the threatened attack or act of aggression.

(C) FORM.—A notification submitted pursuant to subparagraph (A) shall be in unclassified form, but may include a classified annex.

(e) REQUIREMENT RELATING TO INTELLIGENCE SUPPORT IN THE EVENT OF AN ARMED ATTACK ON

UKRAINE IN VIOLATION OF AN ARMISTICE OR COMPREHENSIVE POLITICAL SETTLEMENT.—

(1) IN GENERAL.—In the event of an armed attack by the Russian Federation on Ukraine that violates an armistice or a comprehensive political settlement, the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the Defense Intelligence Agency, and the heads of other relevant elements of the intelligence community, shall immediately resume the provision of intelligence support to the Government of Ukraine at a level the Directors deem necessary to support military operations of the Government of Ukraine that are intended, or reasonably expected, to help the Armed Forces of Ukraine defend or liberate the territory of Ukraine and prevent such territory of Ukraine from being occupied or attacked by the Russian Federation.

(2) NOTIFICATION.—

(A) IN GENERAL.—The Director of National Intelligence shall promptly notify the congressional intelligence committees not later than 5 days after resuming intelligence support pursuant to paragraph (1).

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

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

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

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

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

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

(C) FORM.—A notification submitted pursuant to subparagraph (A) shall be in unclassified form, but may include a classified annex.

(3) SUNSET.—

(A) IN GENERAL.—The provision of intelligence support for Ukraine under this subsection shall cease on the date that is 120 days after the date on which the Government of Ukraine and the Government of the Russian

Federation agree to reinstate the armistice or comprehensive political settlement that was violated or a new armistice or comprehensive political settlement is entered into force.

(B) RECOMMENCEMENT.—Upon the cessation of the provision of intelligence support under subparagraph (A), the Director of the Central Intelligence Agency, in coordination with the heads of any other relevant elements of the intelligence community, shall resume the provision of intelligence support to Ukraine pursuant to subsection (d).

(f) DEFINITIONS.—In this section:

(1) ARMISTICE; COMPREHENSIVE POLITICAL SETTLEMENT.—The terms ''armistice'' and ''comprehensive political settlement'' mean a formal written agreement between the Government of Ukraine and the Government of the Russian Federation that has the effect of permanently ending the armed conflict between both nations.

(2) INTELLIGENCE SUPPORT.—The term ''intelligence support'' means activities authorized under the provisions of law governing the heads of the elements of the intelligence community, including the

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

(3) SPECIFIC AND IDENTIFIABLE NATIONAL SECURITY CONCERN.—The term ''specific and identifiable national security concern'' includes the following:

(A) Credible intelligence that an element of the Government of Ukraine has been compromised by the Russian Federation or another foreign adversary.

(B) Protection of sources and methods.

(C) A voluntary request from the Government of Ukraine to pause intelligence support.

(D) Credible intelligence that an element of the Government of Ukraine receiving United States intelligence support engaged in a pattern of human rights violations, atrocities, or violations of the law of armed conflict.

(4) TERRITORY OF UKRAINE.—The term ''territory of Ukraine'' means all territory internationally recognized to be the sovereign territory of Ukraine on February 19, 2014, including Crimea and the territory that the Russian Federation claims to have annexed in Kherson and Zaporizhzia.

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

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

(1) by striking ''Under the direction'' and inserting the following:

''(1) IN GENERAL.—Under the direction''; and

(2) by adding at the end the following:

''(2) NOTIFICATION REQUIRED.—

''(A) IN GENERAL.—Not later than 48 hours after a decision to pause, terminate, or otherwise restrict or materially downgrade intelligence support or intelligence activities (as defined in section 501(f)), including information, intelligence, and imagery collection authorized under Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), to the government of a country of significant concern to the United States, the Director of National Intelligence shall submit to the congressional intelligence committees a notification of such decision.

''(B) ELEMENTS.—The notification required in subsection (a) shall include—

''(i) a detailed description of the reason for the pause, termination, restriction, or material downgrade of intelligence support;

''(ii) a description of the change in intelligence sharing;

''(iii) the categories of information affected;

''(iv) the expected duration of the pause, termination, restriction, or material downgrade; and

''(v) the anticipated impact of such decision on regional security and the national security objectives of the United States.

''(C) COUNTRY OF SIGNIFICANT CONCERN TO THE UNITED STATES DEFINED.—In this subsection, the term 'country of significant concern to the United States' means—

''(i) Israel;

''(ii) Ukraine;

''(iii) Taiwan; and

''(iv) any other country designated as such by the President.''.

SEC. 622. UNITED STATES-ISRAEL INTELLIGENCE SHARING ENHANCEMENT.

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

(1) to maintain and strengthen the strategic security partnership with Israel as a means of advancing the national defense of the United States, regional stability, and the protection of United States personnel and interests in the Middle East;

(2) to enhance intelligence collaboration through robust intelligence sharing and analytic partnership with Israel to counter terrorism, proliferation networks, cyber threats, state and nonstate aggressors, terror financing, sanctions evasion, and other transnational security challenges that threaten both Israel and the United States;

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

(4) to ensure that security assistance and defense cooperation are structured to help Israel maintain its qualitative military edge, consistent with United States law and broader regional security considerations;

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

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

(b) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) Israel remains a critical United States security partner whose defense and intelligence capabilities provide a strategic advantage that contributes to enhanced operational effectiveness and technological superiority;

(2) timely and actionable intelligence sharing between the United States and Israel has saved United States personnel and property in the region and should remain a central pillar of the bilateral security relationship;

(3) the evolving threat environment in the Middle East—including missile proliferation, unmanned systems, cyber operations, terror financing, and

proxy warfare—requires sustained and adaptive cooperation between the United States and Israel;

(4) the United States-Israel security partnership has historically benefitted from bipartisan support, which strengthens the partnership's credibility, durability, and deterrent value; and

(5) expanding normalization and practical security cooperation between Israel and regional states can serve as a force multiplier for collective deterrence and integrated defense.

(c) REQUIREMENTS RELATING TO INTELLIGENCE SHARING.—

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

"SEC. 1115. REQUIREMENTS RELATING TO INTELLIGENCE SHARING.

''(a) INTELLIGENCE SHARING WITH ISRAEL.—

''(1) IN GENERAL.—The President, acting through the Director of National Intelligence and, as necessary, the Secretary of Defense, shall, subject to applicable law and the protection of intelligence sources and methods, expand and enhance intelligence sharing with the Government of Israel.

''(2) SCOPE OF INTELLIGENCE SHARING.—Intelligence sharing carried out under this subsection shall include the sharing of information relating to cybersecurity threats, terrorism, sanctions evasion, plans and intentions of state and nonstate actors, adversarial technology proliferation, missile threats, unmanned aerial systems, cruise missiles, ballistic missiles, air and space domain awareness, and other aerial threats relevant to the defense of Israel, United States forces and interests in the region, and regional security partners.

''(3) LIMITATIONS ON REDUCTION OF INTELLIGENCE SHARING.—

''(A) IN GENERAL.—Intelligence sharing and related security information exchanges with the Government of Israel shall not be suspended, reduced, or otherwise materially limited except on the basis of a specific and identifiable national security concern determined by the President, such as the protection of intelligence sources and methods, counterintelligence risk, or another significant security consideration.

''(B) DOCUMENTATION REQUIREMENT.—The President shall document any determination to suspend, reduce, or otherwise materially

limit intelligence sharing or related security information exchanges with the Government of Israel, including a description of the national security rationale supporting the change.

''(4) CONGRESSIONAL NOTIFICATION.—

''(A) IN GENERAL.—Not later than 15 days after the date of any decision to materially increase, suspend, reduce, or otherwise alter intelligence sharing or related security information exchanges with the Government of Israel, the President shall notify the congressional intelligence committees of such decision.

''(B) ELEMENTS.—Each notification required by subparagraph (A) shall include the following:

''(i) A description of the change in intelligence sharing or security information exchange.

''(ii) The categories of information affected.

''(iii) The national security objectives served by the change.

''(iv) In the case of a suspension or reduction, the specific national security concern supporting the change.

"(v) An assessment of the anticipated impact on regional security, United States forces, and integrated air and missile defense cooperation.

"(b) INTELLIGENCE SHARING AND ANALYTIC COOPERATION WITH ABRAHAM ACCORDS COUNTRIES.—

"(1) IN GENERAL.—The President, acting through the Director of National Intelligence and, as necessary, the Secretary of Defense, shall, consistent with applicable law and security agreements, expand and enhance intelligence sharing and analytic cooperation with countries that have normalized relations with Israel pursuant to the Abraham Accords (as defined in section 64(k) of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2735a(k)) in order to strengthen regional security integration.

"(2) PRIORITY AREAS.—In carrying out paragraph (1), the President shall prioritize the sharing of appropriate intelligence and information relating to—

"(A) counterterrorism threats and networks, including state and nonstate aggressors, and terror financing;

"(B) cybersecurity threats, vulnerabilities, and defensive best practices;

''(C) air and missile defense early warning and threat tracking;

''(D) geospatial, overhead, and other imaging intelligence relevant to shared security concerns; and

''(E) maritime security threats, including threats to freedom of navigation, commercial shipping, sanctions evasion, and regional maritime stability.

''(3) SAFEGUARDS.—

''(A) ADOPTION OF GUIDELINES.—The Director of National Intelligence, in coordination with the Secretary of Defense, shall adopt guidelines for intelligence sharing and analytic cooperation carried out under this subsection that ensure appropriate safeguards—

''(i) to protect intelligence sources and methods; and

''(ii) to ensure that recipients maintain adequate security protections consistent with United States requirements.

''(B) RESTRICTIONS ON ACCESS.—If the Director of National Intelligence determines that a recipient of intelligence sharing or analytic cooperation carried out under this sub-

section has any intelligence, defense, or technological information sharing relationship with an adversarial nation, the Director shall restrict all access of such recipient to such intelligence sharing and analytic cooperation.

''(c) REPORT REQUIRED.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, and annually thereafter for 5 years, the President shall submit to the appropriate congressional committees a report on the status of United States intelligence sharing with the Government Israel and, as appropriate, regional partners.

''(2) MATTERS TO BE INCLUDED.—Each report required by paragraph (1) shall include, to the extent consistent with the protection of intelligence sources and methods, the following:

''(A) A description of the categories of intelligence and security information shared by the United States Government with the Government of Israel.

''(B) An assessment of progress toward seamlessly integrating Israel into regional air and missile defense and early warning architectures with partner countries, including those

that have normalized relations with Israel pursuant to the Abraham Accords.

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

''(i) improved detection, tracking, warning, interception, or deterrence of aerial threats, including missiles and unmanned systems, for Israel, United States forces, or regional partners; and

''(ii) the overall stability and coordination of security in the region.

''(D) An assessment of progress in improving interoperability among technology networks of the United States, Israel, and partner countries.

''(E) A description of efforts to secure technology networks and data from cyber threats and unauthorized access.

''(F) An identification of any legal, policy, technical, counterintelligence, or security barriers limiting deeper intelligence integration, including risks to intelligence sources and methods.

''(G) A summary of any significant increases or reductions in intelligence sharing

during the reporting period and the national security rationale for such changes.

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

''(4) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this subsection, the term 'appropriate congressional committees' means—

''(A) the congressional intelligence committees; and

''(B) to the extent Department of Defense information is implicated, the congressional defense committees (as defined in section 101(a) of title 10, United States Code).''.

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

''Sec. 1115. Requirements relating to intelligence sharing.''.

TITLE VII—ARTIFICIAL INTELLIGENCE MATTERS RELATING TO THE INTELLIGENCE COMMUNITY

SEC. 701. ARTIFICIAL INTELLIGENCE EXPLOITATION GUARD AND INTELLIGENCE SHARING.

(a) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE MODEL.—The term ''artificial intelligence model'' means a capability or series of capabilities combined that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions without human intervention or input.

(2) CENTER.—The term ''Center'' means the Artificial Intelligence Security Center of the National Security Agency.

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

(4) CLEARED INDUSTRY PERSONNEL.—The term ''cleared industry personnel'' means employees or representatives of a covered person who hold an appropriate security clearance and have a demonstrated need to know.

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

(6) COVERED PERSON.—The term ''covered person'' means a non-Federal person who—

(A) is a United States citizen;

(B) develops, deploys, or operates artificial intelligence models or critical enabling infrastructure; and

(C) provides the services described in subparagraph (B) to an element of the intelligence community or Department of Defense.

(7) DIRECTOR.—The term ''Director'' means the Director of the National Security Agency.

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

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

(10) SECURITY CLEARANCE.—The term ''security clearance'' means an authorization to access classified information.

(11) THREAT INFORMATION.—The term ''threat information'' means information on—

(A) efforts by foreign adversary countries to use products or research of covered persons or other entities or individuals to generate synthetic media for foreign-directed influence cam-

paigns, develop and manage computer network exploitation campaigns, design or develop weapons systems, or enhance surveillance capabilities in ways that undermine the privacy or threaten the security of citizens of the United States;

(B) threats posed by foreign adversary countries, including indications of compromise to networks associated with covered persons and other entities and individuals, or other technical indicators, indicating a compromise to the confidentiality, integrity, or availability of an artificial intelligence system, or to the supply chain of an artificial intelligence system, including training or test data, frameworks or software libraries, training or inference computing environments, or other components necessary for the training, management, or maintenance of an artificial intelligence system;

(C) activity of foreign entities of concern to clandestinely, fraudulently, or otherwise maliciously access the systems of covered persons for purposes of illicit technology transfer or otherwise gaining unfair economic advantage, including through techniques to extract a model's technical capabilities to replicate, develop, or

improve a foreign artificial intelligence model without authorization by the covered person;

(D) activity of foreign entities of concern to sabotage or otherwise clandestinely degrade artificial intelligence systems or the supply chain of an artificial intelligence system, including training or test data, frameworks or software libraries, training or inference computing environments, or other components necessary for the training, management, or maintenance of an artificial intelligence system; and

(E) observations, emerging concerns, or other inputs from vendors or researchers regarding relevant malicious or clandestine activity of foreign entities of concern toward an artificial intelligence system, its supply chain, or other necessary components.

(b) ESTABLISHMENT OF PILOT PROGRAM ON SHARING OF INTELLIGENCE AND THREAT INFORMATION WITH COVERED PERSONS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director shall, acting through the Center, establish a pilot program to assess the feasibility and advisability of facilitating the secure sharing with covered

persons of intelligence and threat information germane to the exploitation of access to United States artificial intelligence systems and enabling infrastructure to engage in intelligence collection, intellectual property theft, and other malicious activities.

(2) PARTICIPATION.—The Director may not select covered persons to participate in the pilot in a manner that provides a competitive advantage or procurement preference to any covered person, to the detriment of another covered person.

(3) DURATION.—The Director shall carry out the pilot program established pursuant to paragraph (1) during the 3-year period beginning on the date of the establishment of the pilot program.

(c) PARTICIPATION REQUIREMENTS.—

(1) CRITERIA.—The Director shall establish criteria governing engagement with covered persons under the pilot program required by subsection (b), which may include criteria relating to the following:

(A) Relevance to national security.

(B) The ability to protect classified or sensitive intelligence information.

(C) Cybersecurity and information security maturity.

(D) Agreement to comply with intelligence handling, use, and nondisclosure requirements.

(E) The availability of cleared personnel of covered persons or willingness of covered persons to increase the number of cleared personnel.

(2) NATURE OF PARTICIPATION.—Participation in the pilot program shall not be construed as a certification, endorsement, or regulatory approval by the United States Government of any artificial intelligence system or commercial activity and the Director may not exclude a covered person from participating on the basis of political or ideological viewpoints of the covered person or its employees.

(d) INTELLIGENCE SHARING STRUCTURE.—

(1) AUTHORIZED MODES.—Under the pilot program required by subsection (b), the Director may, acting through the Center, authorize the sharing of intelligence and threat information as described in paragraph (1) of such subsection through—

(A) bilateral exchanges between elements of the intelligence community and a covered person;

(B) multilateral exchanges among covered persons, as determined appropriate by the Director; or

(C) another designated intelligence-sharing mechanism operated or overseen by the Director.

(2) LIMITATION.—Any mechanism established under this section shall be limited to the dissemination of intelligence and threat information and shall not establish standards, requirements, or best practices governing artificial intelligence development or deployment.

(e) TAILORING, HANDLING, AND PROTECTION OF INTELLIGENCE.—

(1) PROCEDURES REQUIRED.—The Director shall, acting through the Center, codify procedures to tailor, sanitize, or downgrade the classification level of intelligence shared under the pilot program required by subsection (b) to ensure usability while protecting intelligence sources and methods.

(2) EXAMPLES OF PROCEDURES.—The procedures developed under paragraph (1) may include the following:

(A) The use of tear lines and segregable summaries.

(B) The preparation of classified annexes where necessary.

(C) Criteria governing the classification level of shared intelligence.

(D) The appropriate use of cleared industry personnel.

(3) HANDLING REQUIREMENTS.—The Director shall, acting through the Center, codify policies governing the handling, storage, and dissemination of intelligence shared under the pilot program required by subsection (b), including audit and compliance mechanisms.

(f) PERMISSIBLE USE AND NONDISCLOSURE.—

(1) PERMISSIBLE USE.—Intelligence shared under the pilot program required by subsection (b) may be used solely for detecting, preventing, or mitigating malicious foreign activity exploiting access to United States artificial intelligence systems and enabling infrastructure to engage in intelligence collection, intellectual property theft, and other malicious activities.

(2) NONDISCLOSURE.—A covered person may not disclose to any person who is not a covered person or an element of the intelligence community any intelligence shared with the covered person under

the pilot program required by subsection (b), except as expressly authorized by the Director acting through the Center.

(g) PRIVACY AND CIVIL LIBERTIES.—In planning and coordinating the pilot program required by subsection (b), the Director shall, acting through the Center, consult with the Civil Liberties Protection Officer of the Office of the Director of National Intelligence.

(h) EVALUATION AND REPORTING.—

(1) EVALUATION.—The Director shall, acting through the Center, continuously evaluate the effectiveness and risks of the pilot program established under subsection (b).

(2) REPORT.—

(A) IN GENERAL.—Not later than 90 days before the date on which the pilot program required by paragraph (1) of subsection (b) terminates pursuant to paragraph (2) of such subsection, the Director shall, acting through the Center, submit to the congressional intelligence committees a report assessing—

(i) the effectiveness of intelligence sharing under the pilot program;

(ii) the adequacy of safeguards for sources, methods, and privacy;

(iii) the scope of participation; and

(iv) whether the program should be modified, extended, or terminated.

(B) FORM.—The report submitted pursuant to subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

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

(1) to authorize the collection of intelligence on United States persons not authorized by another provision of law;

(2) to require the disclosure of classified information to unauthorized persons; or

(3) to establish commercial, competition, or technology policy outside the purview of the intelligence community.

(j) EXEMPTION FROM DISCLOSURE; PROTECTION.—Any information shared by a covered person or other entity or individual with the United States Government pursuant to this section—

(1) shall be exempt from disclosure and withheld, without discretion, from the public, pursuant to section 552(b)(3)(B) of title 5, United States Code, and any other provision of United States law

or law of any State, political subdivision or agency thereof, or Tribe requiring disclosure of information or records; and

(2) shall not be deemed a waiver of any applicable privilege or protection, including trade secret protection.

SEC. 702. DIRECTOR OF NATIONAL INTELLIGENCE REVIEW OF INTELLIGENCE COMMUNITY USE OF ARTIFICIAL INTELLIGENCE TO SUPPORT TARGETING.

(a) DEFINITIONS.—In this subsection:

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

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

(b) REVIEWS RELATED TO INTELLIGENCE COMMUNITY USE OF ARTIFICIAL INTELLIGENCE TO SUPPORT TARGETING.—

(1) POLICY AND PROCEDURE REVIEWS.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Director shall review and assess the policies and procedures that govern the use by the intelligence community of artificial intelligence tech-

nologies in the production, or review, of intelligence used by the United States to inform targeting decisions with lethal effects.

(B) ELEMENTS.—In carrying out the review and assessment required by subparagraph (A), the Director shall—

(i) assess whether policies and procedures of the intelligence community that were in effect on the day before the date of the enactment of this Act adequately address risks posed by the use of artificial intelligence technologies in the targeting analysis and development and civilian harm mitigation processes; and

(ii) ensure the review covers all policies of the intelligence community that regard the production or review of intelligence, regardless of which element first produced the intelligence.

(2) WORKFLOW REVIEWS.—Not later than 90 days after the date of the enactment of this Act, the Director shall review and assess all workflows of the intelligence community that incorporate artificial intelligence used by the United States to inform targeting decisions with lethal effects.

(c) ARTIFICIAL INTELLIGENCE ERRORS EXPLORATORY ANALYSIS.—In carrying out the reviews required by subsection (b), the Director shall direct the National Intelligence Council to conduct a structured, exploratory analysis that—

(1) assess ways in which frontier artificial intelligence models could exhibit bias or cause errors that undermine intelligence or other information provided by the intelligence community that informs targeting accuracy;

(2) identify the specific point and cause of error; and

(3) provide proposed process mitigations to catch and correct such mistakes.

(d) CONSULTATION.—In carrying out the review and assessments required by subsection (b), the Director shall consult with the heads of the elements of the intelligence community whose intelligence is commonly consulted to inform targeting decisions with lethal effects, such as the National Geospatial-Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, and the Central Intelligence Agency, to solicit input on potential negative consequences resulting from artificial intelligence supported analysis, and possible ways to mitigate such consequences.

(e) POLICIES AND DIRECTIVES.—The Director shall issue or adjust such policies and directives to the intelligence community as the Director considers appropriate to improve risk mitigation in light of the review carried out under subsection (b).

(f) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees a report on the reviews and assessments carried out under subsection (b) as well as a summary of any new policies and directives issued pursuant to subsection (e).

(2) CONTENTS.—The report required by paragraph (1) shall include the following:

(A) A description of contributions of the intelligence community to targeting workflows, such as identification of points of interest, pattern of life analysis, review of proposed targets, target selection, and civilian impact reviews, as well as the understanding of the intelligence community of the delineation of roles and responsibilities with the Armed Forces where applicable.

(B) Identification of any artificial intelligence tools utilized and for what tasks or purposes they are used.

(C) The level of autonomy afforded to the tools, and whether human review of artificial intelligence system outputs is required to be conducted prior to dissemination of materials.

(D) The scope of individuals expected to have access to the materials described in subparagraph (C).

(E) An explanation of whether and how the capability limitations of artificial intelligence tools available to personnel of the intelligence community are communicated to users, including the cutoff date for the tool's training data, databases to which it does or does not have access rights, and the tasks the model has been trained for or approved for use.

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

SEC. 703. IMPROVEMENTS FOR ARTIFICIAL INTELLIGENCE POLICIES, STANDARDS, AND GUIDANCE FOR INTELLIGENCE COMMUNITY.

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

(1) in subsection (b)—

(A) by redesignating paragraph (3) as paragraph (4); and

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

''(3) STUDY FOR TRACKING DATA GENERATED OR MODIFIED BY AN ARTIFICIAL INTELLIGENCE SYSTEM.—The Chief Artificial Intelligence Officer of the Intelligence Community, in coordination with the Chief Artificial Intelligence Officer of each element of the intelligence community, shall examine whether the intelligence community should identify intelligence information generated or materially modified by an artificial intelligence system, including determining what methods are necessary to preserve such information throughout the intelligence lifecycle.'';

(2) in subsection (d), by adding at the end the following:

''(3) PROCESS FOR REVIEW OF ARTIFICIAL INTELLIGENCE TESTING METHODOLOGIES AND

BENCHMARKS.—Consistent with applicable classification and access policies, the Chief Artificial Intelligence Officer of the Intelligence Community, in coordination with the Chief Artificial Intelligence Officer of each element of the intelligence community, shall—

''(A) establish a process to review artificial intelligence testing methodologies and benchmarks employed within each element; and

''(B) ensure such methodologies and benchmarks remain commensurate with the capabilities and impacts of systems being evaluated.''; and

(3) by adding at the end the following:

''(f) PROCESS TO SYSTEMATICALLY TRACK AND EVALUATE INCIDENTS.—Not later than 180 days after the date of the enactment of this subsection, the Chief Artificial Intelligence Officer of the Intelligence Community, in coordination with the National Manager for National Security Systems, shall establish a process to systematically track and evaluate incidents associated with compromises to the confidentiality, integrity, or availability of artificial intelligence systems within each element of the intelligence community.

''(g) POLICIES FOR AGENTIC ARTIFICIAL INTELLIGENCE SYSTEMS AND PROCESSES.—

''(1) DEFINITION OF AGENTIC ARTIFICIAL INTELLIGENCE SYSTEM OR PROCESS.—In this subsection, the term 'agentic artificial intelligence system or process'—

''(A) means an artificial intelligence system or process that, given an objective or instruction—

''(i) determines the action or sequence of actions to be taken to accomplish that objective; and

''(ii) is capable of executing such actions directly on information systems, data, or external services; and

''(B) does not include a system or process that solely generates informational or advisory output for a human operator to act upon.

''(2) REVIEW OF THE ADEQUACY OF EXISTING IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT SYSTEMS FOR INFORMATION WITHIN THE INTELLIGENCE COMMUNITY.—

''(A) IN GENERAL.—Consistent with authority under section 102A(g) of the National Security Act of 1947 (50 U.S.C. 3024(g)), the

Director of National Intelligence, in coordination with the National Manager for National Security Systems, shall—

''(i) not later than 1 year after the date of the enactment of this paragraph, complete a review of the adequacy of existing identity, credential, and access management systems for information within the intelligence community used by agentic artificial intelligence systems and processes; and

''(ii) not permit access to any information within the intelligence community by an external department or agency for use in an agentic artificial intelligence system or process until the review required by clause (i) is completed.

''(B) EVALUATION OF EFFECTIVENESS OF MECHANISMS FOR AGENTIC ARTIFICIAL INTELLIGENCE SYSTEMS AND PROCESSES TO AUTHENTICATE AS NON-HUMAN ACTORS.—The review required by subparagraph (A)(i) shall include an evaluation of the effectiveness of mechanisms for agentic artificial intelligence systems 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—

''(A) establishing a taxonomy of autonomy and security risks associated with agentic artificial intelligence systems and processes that operate on, or have the possibility of accessing, information within the intelligence community; and

''(B) establishing technical controls, processes, and other mitigation measures to address the risks identified under subparagraph (A), including, at a minimum—

''(i) requirements that any element of the intelligence community or external department or agency incorporating information from an intelligence community element as part of an agentic artificial intelligence system or process provide the relevant element of the intelligence community controlling such information with documentation of—

''(I) the properties of the agentic artificial intelligence system or process, including the range of additional systems or data sources it may access (whether as a system or process input or as an agent action), the permis-

sions and classification entitlements associated with such access, as well as any relevant model or system documentation, such as model and system cards;

''(II) anticipated mission use cases for any access to information within the intelligence community in the context of an agentic artificial intelligence system or process, including whether any use case constitutes a high-impact artificial intelligence use as those terms are defined under existing Federal policies;

''(III) procedures to notify relevant intelligence community elements controlling such information of any changes to the properties of the agentic artificial intelligence system or process, to permissions and classification entitlements, or to anticipated use cases of such system or process, that might significantly limit the utility, confidentiality, integrity, or availability of such information; and

''(IV) procedures for intelligence community elements to promptly notify external intelligence community elements or departments or agencies of any material changes to upstream classified data or systems that might significantly limit or impair the utility, confidentiality, integrity, or availability of any downstream agentic artificial intelligence system or process maintained by that external intelligence community element or department or agency;

''(ii) policies and procedures to log any actions, as well as associated inputs, taken by an agentic artificial intelligence system or process to information within the intelligence community, including mechanisms to reverse or negate unauthorized actions or actions that pose a risk to the user intent or confidentiality, integrity, or availability of such information;

''(iii) policies and procedures for safeguards, continuous monitoring, and the detection of security incidents or other unex-

pected behavior of an agentic artificial intelligence system or process, or failures of associated safeguards, that may pose a threat to the confidentiality, availability, or integrity of information within the intelligence community;

''(iv) policies and procedures for system-level controls of agentic artificial intelligence systems and processes, tailored to address each system or process component; and

''(v) criteria for the selection of interoperability standards for agentic artificial intelligence systems and processes, with preference, to the extent practicable, for standards that are openly specified, governed in a vendor-neutral manner, supported by multiple model providers, extensible to future requirements, and subject to ongoing independent security review.''.

SEC. 704. ADDITIONAL FUNCTIONS AND REQUIREMENTS OF ARTIFICIAL INTELLIGENCE SECURITY CENTER.

Section 6504 of the Intelligence Authorization Act for Fiscal Year 2025 (division F of Public Law 118–159) is amended—

(1) in subsection (c)—

(A) by redesignating paragraph (3) as paragraph (4); and

(B) by inserting after paragraph (2) the following new paragraph (3):

''(3) Making available a research test-bed to private sector and academic researchers, on a subsidized basis, to engage in artificial intelligence security research, including through the secure provision of access in a secure environment for pre-deployment testing of to proprietary third-party models with the consent of the vendors of the models.'';

(2) by redesignating subsection (d) as subsection (f); and

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

''(d) TEST-BED REQUIREMENTS.—

''(1) ACCESS AND TERMS OF USAGE.—

''(A) RESEARCHER ACCESS.—The Director shall establish terms of usage governing re-

searcher access to the test-bed made available under subsection (c)(3), with limitations on researcher publication only to the extent necessary to protect classified information or proprietary information concerning third-party models provided through the consent of model vendors.

''(B) AVAILABILITY TO FEDERAL AGENCIES.—The Director shall ensure that the test-bed made available under subsection (c)(3) is also made available to other Federal agencies on a cost-recovery basis.

''(2) USE OF CERTAIN INFRASTRUCTURE AND OTHER RESOURCES.—In carrying out subsection (c)(3), the Director shall leverage, to the greatest extent practicable, infrastructure and other resources provided under section 5.2 of Executive Order 14110 (88 Fed. Reg. 75191; relating to safe, secure, and trustworthy development and use of artificial intelligence).

''(3) VOLUNTARY SECURITY GUIDANCE.—In order to incentivize participation by vendors of leading commercial models and to promote the national security of the United States, the Director shall share relevant guidance, informed by pre-deployment

testing in the secure test-bed environment identified in subsection (c), to inform voluntary vendor actions to mitigate against potential security threats to such models, or the ability of foreign actors to utilize such models for computer network exploitation campaigns, the design or development of weapons systems, or to further foreign surveillance capabilities.''.

SEC. 705. REPORTS ON NOVEL USES OF ARTIFICIAL INTELLIGENCE TECHNOLOGY.

(a) DEFINITION.—In this section, the term ''novel use of artificial intelligence technology'' means—

(1) an artificial intelligence capability or series of capabilities combined that has not previously been included in an intelligence community element's inventory of artificial intelligence use cases consistent with guidance issued pursuant to section 6702(b) of the Intelligence Authorization Act for Fiscal Year 2023 (50 U.S.C. 3334m(b));

(2) a use of an artificial intelligence capability that contravenes a restriction on the use of artificial intelligence contained in such an inventory; or

(3) a use of an artificial intelligence capability that constitutes a high-impact artificial intelligence use as that term is defined under policies of the executive branch.

(b) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, and every 180 days thereafter, the Director of National Intelligence, in coordination with the heads of the other elements of the intelligence community, shall submit to the congressional intelligence committees a consolidated report detailing any novel use of artificial intelligence technology that any element of the intelligence community is considering employing within the one-year period following submission of such report.

(c) CONTENTS.—Each report submitted pursuant to subsection (b) shall describe the proposed novel use of artificial intelligence technology, including—

(1) hardware and software requirements;

(2) the proposed application of the technology;

(3) the risks and advantages assessed with respect to the proposed novel use;

(4) any specific risk mitigation measures contemplated, including measures specific to the proposed novel use;

(5) any test and evaluation activities conducted in conjunction with the proposed novel use;

(6) any additional test and evaluation activity that is still needed, and whether the intelligence

community has resources to conduct and fund such activity; and

(7) any estimated cost increases anticipated in connection with the proposed novel use.

(d) FORM.—Each report submitted pursuant to subsection (b) shall be submitted in classified form.

(e) SUNSET.—This section shall expire on October 1, 2032.

SEC. 706. CLEAR LABELING OF ARTIFICIAL INTELLIGENCE OUTPUTS FOR TARGETING WORKFLOWS.

Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence shall, in coordination with the Chief Artificial Intelligence Officers of the elements of the intelligence community, establish a policy that applies to elements of the intelligence community, which generate intelligence that could reasonably be judged useful to develop or inform targeting with lethal effects, and that requires—

(1) labeling of outputs from any artificial intelligence system used in the development of such intelligence are clearly marked to indicate—

(A) that artificial intelligence was used;

(B) the artificial intelligence system or model used;

(C) the manner in which, or task for which, the artificial intelligence was used; and

(D) a point of contact such as the relevant Chief Artificial Intelligence Officer, who can address questions about data inputs, system access, or artificial intelligence system performance; and

(2) the label or indicator that is used pursuant to paragraph (1) is attached to the resulting data or work product in a manner that remains prominent and visible to any person who subsequently interacts with that data on a system of the intelligence community, regardless of organizational affiliation of the person or the role of the person in developing the data.

SEC. 707. RESEARCH ON USE OF ARTIFICIAL INTELLIGENCE RELATING TO INADVERTENT ESCALATION.

(a) REQUIREMENT.—Not later than 90 days after the date of the enactment of this Act and subject to the availability of appropriations, the Director of the Intelligence Advanced Research Projects Activity, in coordination with the Chief Artificial Intelligence Officer of the Intelligence Community, shall commence a research campaign to deepen the understanding of the intelligence community with

respect to specific ways in which the use of artificial intelligence systems by the intelligence community could contribute to inadvertent escalation with foreign nations or actors.

(b) ELEMENTS.—The research campaign required by subsection (a) shall include—

(1) the identification of scenarios in which artificial intelligence capabilities could contribute to inadvertent escalation with foreign nations or actors, including—

(A) analytic judgments that fail to properly consider or weigh alternative explanations;

(B) automation of imagery classification or signals intelligence;

(C) distinguishing between civilians and authorized targets;

(D) operational uses of artificial intelligence, such as time-constrained uses that do not allow for independent verification; and

(E) such other scenarios as identified by the Director or participating subject matter experts;

(2) a simulation of select scenarios to discern where miscommunication or miscalculations have a higher likelihood of occurrence; and

(3)(A) an identification of potential mitigations for vulnerabilities discovered; or

(B) if no mitigation could be identified, an identification of vulnerabilities that require follow-up action by the intelligence community.

(c) BRIEFINGS.—

(1) CONGRESS.—Not later than 180 days after the date of the enactment of this Act, or 30 days after the date of completion of the research campaign required by subsection (a), whichever occurs first, the Director of the Intelligence Advanced Research Projects Activity, in coordination with the Chief Artificial Intelligence Officer of the Intelligence Community, shall brief the congressional intelligence committees on the findings and recommendations of the research campaign.

(2) INTELLIGENCE COMMUNITY.—The Director of the Intelligence Advanced Research Projects Activity, in coordination with the Chief Artificial Intelligence Officer of the Intelligence Community, shall brief the heads and Chief Artificial Intelligence Officers of the elements of the intelligence community on the findings and recommendations of the research campaign required by subsection (a), as appropriate.

SEC. 708. RESEARCH ON INTERACTION OF ADVERSARIAL ARTIFICIAL INTELLIGENCE SYSTEMS WITH INTELLIGENCE COMMUNITY SYSTEMS.

(a) REQUIREMENT.—Not later than 90 days after the date of the enactment of this Act and subject to the availability of appropriations, the Director of the Intelligence Advanced Research Projects Activity, in coordination with the Chief Artificial Intelligence Officer of the Intelligence Community, shall commence a research campaign to deepen the understanding of the intelligence community with respect to novel dynamics and vulnerabilities that may arise when an adversarial artificial intelligence system interacts directly with systems of, or contracted by, the intelligence community that include artificial intelligence components.

(b) ELEMENTS.—The research campaign required by subsection (a) shall—

(1) pursue sandbox demonstrations with frontier artificial intelligence models or leverage other tactics necessary to uncover vulnerabilities to intelligence community systems, infrastructure, or personnel that may result from—

(A) the accelerated development of artificial intelligence capabilities by foreign nations;

(B) the increasing access that non-state and criminal actors have to commercial artifi-

cial intelligence tools that can identify vulnerabilities and propose or orchestrate attacks; and

(C) the potential for artificial intelligence systems to interact directly with each other during an attack; and

(2) pursue findings, including—

(A) an identification of potential mitigations for unique vulnerabilities discovered; or

(B) if no mitigation could be identified, an identification of vulnerabilities that require follow-up action by the intelligence community.

(c) BRIEFINGS.—

(1) CONGRESS.—Not later than 180 days after the date of the enactment of this Act, or 30 days after the date of completion of the research campaign required by subsection (a), whichever occurs first, the Director of the Intelligence Advanced Research Projects Activity, in coordination with the Chief Artificial Intelligence Officer of the Intelligence Community, shall brief the congressional intelligence committees on the findings and recommendations of the research campaign.

(2) INTELLIGENCE COMMUNITY.—The Director of the Intelligence Advanced Research Projects Ac-

tivity, in coordination with the Chief Artificial Intelligence Officer of the Intelligence Community, shall brief the heads and Chief Artificial Intelligence Officers of the elements of the intelligence community on the findings and recommendations of the research campaign required by subsection (a), as appropriate.

SEC. 709. PROLIFERATION ASSESSMENTS REGARDING THE EXPORT OF ARTIFICIAL INTELLIGENCE-RELATED TECHNOLOGIES.

(a) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE TECHNOLOGY.—The term ''artificial intelligence technology'' means—

(A) any United States-origin model weights;

(B) semiconductor manufacturing equipment; and

(C) any other item classified under—

(i) Export Control Classification Number 3A090 or 4A090 of the Commerce Control List or corresponding entries in the Export Administration Regulations, as in effect on the date of the enactment of this Act; or

(ii) any subsequent revisions to the Commerce Control List as amended by the Bureau of Industry and Security to impose more restrictive parameters.

(2) COMMERCE CONTROL LIST.—The term ''Commerce Control List'' means the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations.

(3) UNITED STATES ARTIFICIAL INTELLIGENCE STACK.—The term ''United States artificial intelligence stack'' means the United States artificial intelligence integrated circuits, cloud infrastructure, and models.

(4) EXPORT CONTROL TERMS.—The terms ''export'', ''Export Administration Regulations'', ''in-country transfer'', ''reexport'', and ''United States person'' have the meanings given those terms in section 1742 of the Export Control Reform Act of 2018 (50 U.S.C. 4801).

(b) STATEMENT OF POLICY.—It shall be the policy of the United States to restrict access to the most sophisticated artificial intelligence integrated circuits and models that United States adversaries may seek to use against the United States, while also exporting the full United

States artificial intelligence stack to allies and partners who adhere to stringent national security standards.

(c) REQUIREMENT.—Not fewer than 90 days before the Secretary of Commerce grants a license for the export, reexport, or in-country transfer of artificial intelligence technology, or before the United States joins an agreement on artificial intelligence with a foreign government, the Director of National Intelligence, acting through the National Intelligence Council, and in coordination with the Director of the Central Intelligence Agency, the Assistant Secretary of State for Intelligence and Research, the Director of the National Security Agency, and the heads of other appropriate elements of the intelligence community, shall provide to the President and the congressional intelligence committees a written assessment containing a comprehensive analysis regarding the risks associated with such action.

(d) SUBSTANCE.—Each report submitted under subsection (c) shall include the assessment of the intelligence community of the consequences of the action concerned for United States national security, including assessment of—

(1) the recipient country's export control system with respect to artificial intelligence technology,

including integrated circuits, integrated circuit design software, tools, and manufacturing equipment;

(2) information on any past, present, or expected interactions, including commercial ties and cooperation, between commercial entities or government entities in the recipient country and other countries of proliferation concern, including the People's Republic of China and the Russian Federation;

(3) actual or suspected transfers of artificial intelligence technology to such countries, including the People's Republic of China and the Russian Federation;

(4) the consequences that onward proliferation of United States artificial intelligence technology from the recipient would have for United States efforts to both deny adversaries access to advanced artificial intelligence technology and maintain a significant competitive advantage in frontier artificial intelligence development, integrated design, and integrated manufacturing, especially relative to the progress of the People's Republic of China and the Russian Federation;

(5) the capacity of the intelligence community and United States commercial entities to have near

real-time awareness of the any potential technology leakage or export violations by the recipient country;

(6) potential measures that the intelligence community assesses could reasonably be taken by the recipient country to mitigate both the proliferation concerns identified by the intelligence community and the consequences of any potential onward proliferation as detailed in paragraph (4);

(7) in the case of the grant of a license, specific measures that the intelligence community will take to evaluate compliance with any associated restrictions or compliance requirements;

(8) whether export of artificial intelligence technology would reinforce United States artificial intelligence dominance;

(9) the intended and likely end-uses, including military, intelligence, and domestic surveillance applications, and whether such uses are consistent with United States national security interests; and

(10) current and planned agreements and arrangements between the United States and the government of the recipient country.

(e) FORM.—Each report submitted under subsection (c) shall be submitted in unclassified form, but may include a classified annex.

SEC. 710. REVIEW OF ARTIFICIAL INTELLIGENCE SECURITY VULNERABILITIES UNDER VULNERABILITIES EQUITIES PROCESS.

(a) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE SECURITY VULNERABILITY.—The term ''artificial intelligence security vulnerability'' means a weakness in an artificial intelligence system that could be exploited by a third party to subvert, without authorization, the privacy, integrity, or availability of an artificial intelligence system, including through techniques such as—

(A) evasion attacks;

(B) poisoning attacks;

(C) privacy-based attacks;

(D) model theft or extraction attacks; and

(E) attacks designed to circumvent or degrade the safety, alignment, or access control mechanisms of an artificial intelligence system.

(2) ARTIFICIAL INTELLIGENCE SYSTEM.—The term ''artificial intelligence system'' means a capability or series of capabilities combined that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions without human intervention or input.

(3) VULNERABILITIES EQUITIES POLICY AND PROCESS DOCUMENT.—The term ''Vulnerabilities

Equities Policy and Process document'' means the executive branch document entitled ''Vulnerabilities Equities Policy and Process for the United States Government'' dated November 15, 2017.

(4) VULNERABILITIES EQUITIES PROCESS.—The term ''Vulnerabilities Equities Process'' means the interagency review of vulnerabilities carried out pursuant to the Vulnerabilities Equities Policy and Process document or any successor document.

(b) EVALUATION; REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of the National Security Agency shall—

(1) evaluate whether the existing Vulnerabilities Equities Process sufficiently accommodates the submission and review of artificial intelligence security vulnerabilities; and

(2) submit to the congressional intelligence committees a report describing the applicability of the Vulnerabilities Equities Process to such vulnerabilities, including whether the submission and review of such vulnerabilities under the Vulnerabilities Equities Process would result in an unduly large volume of notifications to affected vendors and, if so, an assessment of mechanisms to manage the volume of such notifications.

(c) PROCESS.—In carrying out subsection (b), if the Director of the National Security Agency determines that the existing Vulnerabilities Equities Process does not sufficiently accommodate the submission and review of artificial intelligence security vulnerabilities identified by elements of the intelligence community, and that such vulnerabilities present public interest considerations meriting review under the Vulnerabilities Equities Process, the Director shall establish a process for the submission and review of such vulnerabilities under the Vulnerabilities Equities Process not later than 30 days after the date of such determination.

(d) BRIEFING ON VULNERABILITIES IDENTIFIED BY ARTIFICIAL INTELLIGENCE SYSTEMS.—Not later than 90 days after the date of the enactment of this Act, the Director of the National Security Agency shall provide the congressional intelligence committees with a briefing on—

(1) the volume of vulnerabilities of information systems identified by artificial intelligence systems;

(2) the impact of any change in such volume on the functioning of the Vulnerabilities Equities Process; and

(3) whether the increasingly rapid discovery and exploitation of such vulnerabilities by external

cyber actors using artificial intelligence systems materially alters the equity of disclosure.

(e) CONSULTATION REQUIRED.—The Director of the National Security Agency shall carry out subsections (b), (c), and (d) in consultation with—

(1) the Director of the Central Intelligence Agency;

(2) the Director of the Federal Bureau of Investigation; and

(3) other entities as the Director of the National Security Agency considers appropriate.

SEC. 711. PROHIBITION ON CERTAIN ARTIFICIAL INTELLIGENCE MODELS ON INTELLIGENCE COMMUNITY SYSTEMS.

(a) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE MODEL.—The term ''artificial intelligence model'' means a capability or series of capabilities combined that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions without human intervention or input.

(2) CHILD PORNOGRAPHY.—The term ''child pornography'' has the meaning given that term in section 2256 of title 18, United States Code.

(3) COVERED APPLICATION.—The term ''covered application'' means any specific artificial intelligence model that has been confirmed by a head of an element of the intelligence community, or their designee, as—

(A) failing to comply with the National Institute of Standard and Technology Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile with respect to ''obscene, degrading, and/or abusive content'', or a successor standard or framework, to the extent the framework applies to synthetic child sexual abuse material or non-consensual intimate images of adults;

(B) subject to a Federal court determination that such artificial intelligence model has generated content depicting child pornography; or

(C) subject to a Federal court determination that such artificial intelligence model has generated non-consensual intimate visual depictions of an identifiable adult or a minor.

(4) INTIMATE VISUAL DEPICTION.—The term ''intimate visual depiction'' has the meaning given that term in section 1309 of the Violence Against

Women Act Reauthorization Act of 2022 (15 U.S.C. 6851).

(b) PROHIBITION.—

(1) IN GENERAL.—The acquisition or use of any covered application on national security systems operated by an element of the intelligence community or by a contractor of such element is prohibited unless the appropriate safeguards described in subsection (c) can be implemented.

(2) IMPLEMENTATION.—

(A) INITIAL REMOVAL.—Not later than 180 days after the date of the enactment of this Act, any covered application shall be required to be removed from national security systems operated by an element of the intelligence community or a contractor of such element.

(B) SUBSEQUENT REMOVALS.—Beginning after the 180-day period described in subparagraph (A), any artificial intelligence model that becomes a covered application shall be required to be removed from national security systems operated by an element of the intelligence community or a contractor of such element not later than 180 days after the date that the model is confirmed by the head of an element

of the intelligence community, or their designee, to be a covered application.

(c) SAFEGUARDS.—

(1) IN GENERAL.—The head of an element of the intelligence community may implement additional safeguards that prohibit the generation of child pornography or non-consensual intimate visual depictions of an identifiable adult or a minor.

(2) CERTIFICATION REQUIRED.—The head of an element of the intelligence community shall certify to the Director of National Intelligence that safeguards implemented under paragraph (1) are sufficient to prevent misuse of covered applications to generate child pornography or intimate visual depictions of a minor.

(3) CONGRESSIONAL NOTIFICATION.—The head of an element of the intelligence community that issues a certification pursuant to paragraph (2) shall notify the congressional intelligence committees of such certification not later than 7 days after issuing such certification. Such a notification shall identify the safeguards implemented pursuant to paragraph (1).

(d) NATIONAL SECURITY AND RESEARCH WAIVER.—

(1) IN GENERAL.—The head of an element of the intelligence community may issue a waiver for any artificial intelligence model that would otherwise be subject to the prohibition under subsection (b) if the head identifies a national security or research justification for such artificial intelligence model that benefits the intelligence community.

(2) CONGRESSIONAL NOTIFICATION.—Not later than 7 days after issuing a waiver pursuant to paragraph (1), the head of the element of the intelligence community that issues such waiver shall submit to the congressional intelligence committees a notification that includes—

(A) an identification of the national security or research justification for such usage;

(B) an estimate of the approximate cost of such usage; and

(C) a plan to implement a safeguard in such a way as to allow for continued usage consistent with the general prohibition described in subsections (b)(1) and (c)(1).

(e) CURE.—If a covered application is identified for removal or is disqualified from use or acquisition pursuant to this section, the head of an element of the intelligence 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-

spectively, and adjusting the margins accordingly;

(B) by redesignating clauses (i) and (ii) as subclauses (I) and (II), respectively, and adjusting the margins accordingly;

(C) by striking ''If any of the information'' and inserting the following:

''(i) IN GENERAL.—If a portion of the information''; and

(D) by adding at the end the following:

''(ii) FULL CLASSIFICATION.—Notwithstanding paragraphs (5) and (6), if the classification of information required to be included in the transition plan of a Federal entity prohibits even the public release of a redacted transition plan, as determined by the head of the Federal entity, the Federal entity shall—

''(I) notify the NTIA that the entire transition plan must be classified and that even a redacted version cannot be made public; and

''(II) classify the transition plan in accordance with the levels of mate-

rials contained in the transition plan.''; and

(2) in subsection (l)—

(A) by striking ''For purposes of'' and inserting the following:

''(1) IN GENERAL.—For purposes of''; and

(B) by adding at the end the following:

''(2) ELEMENTS OF THE INTELLIGENCE COMMUNITY.—Notwithstanding paragraph (1) or any other provision of this part, each element of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) shall be considered a Federal entity and shall be eligible to receive payment from the Spectrum Relocation Fund for any auction-related relocation or sharing costs incurred by the element regardless of the existence of a Government station license.''.

SEC. 803. PROTECTION OF CLASSIFIED INFORMATION RELATING TO BUDGET FUNCTIONS.

(a) REQUIREMENT.—

(1) IN GENERAL.—Chapter 11 of title 31, United States Code, is amended by adding at the end the following new section:

"§ 1127. Protection of classified information relating to budget functions

"(a) PROTECTION OF CLASSIFIED INFORMATION.—Notwithstanding any other provision of law, not later than September 30, 2028, each covered official shall ensure that the department or agency of the official uses secure systems that meet the requirements to protect classified information, including with respect to the location at which the system is located or accessed, to carry out any of the following activities of the department or agency:

"(1) Formulating, developing, and submitting the budget of the department or agency (including the budget justification materials submitted to Congress) under the National Intelligence Program.

"(2) Apportioning, allotting, issuing warrants for the disbursement of, and obligating and expending funds under the National Intelligence Program.

"(3) Carrying out Federal financial management service functions or related activities of the intelligence community.

"(b) WAIVER.—The Director of National Intelligence, in consultation with the Secretary of Defense, the Secretary of the Treasury, and the Director of the Office of Management and Budget, may issue a waiver to a head of an element of the intelligence community with respect to a requirement under subsection (a) if the Director of

National Intelligence certifies to the congressional intelligence committees that—

''(1) one or more of the Federal financial management service functions or related activities of the element under the National Intelligence Program—

''(A) are appropriately carried out using a system that does not meet the requirements to protect classified information; and

''(B) such use does not represent a significant counterintelligence risk; or

''(2) complying with a specified requirement under subsection (a) would result in an increased counterintelligence threat to a classified program or activity.

''(c) DISPLAY OF INFORMATION IN PUBLIC REPORTS.—Notwithstanding any other provision of law, in making public a report or other information relating to expenditures by an element of the intelligence community, a covered official may modify or omit information relating to such expenditures in a manner necessary to ensure the protection of classified information.

''(d) DEFINITIONS.—In this section:

''(1) COVERED OFFICIAL.—The term 'covered official' means the following:

''(A) The Secretary of the Treasury.

''(B) The Director of the Office of Management and Budget.

''(C) Each head of an element of the intelligence community.

''(D) Any other head of a department or agency of the Federal Government carrying out a function specified in paragraph (1), (2), or (3) of subsection (a).

''(2) FEDERAL FINANCIAL MANAGEMENT SERVICE FUNCTIONS.—In this section, the term 'Federal financial management service functions' means standard functions, as determined by the Secretary of the Treasury, that departments and agencies of the Federal Government perform relating to Federal financial management, including budget execution, financial asset information management, payable management, revenue management, reimbursable management, receivable management, delinquent debt management, cost management, general ledger management, financial reconciliation, and financial and performance reporting.

''(3) INTELLIGENCE COMMUNITY TERMS.—The terms 'congressional intelligence committees', 'intelligence community', and 'National Intelligence Program' have the meaning given those terms in section

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

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 11 of title 31, United States Code, is amended by inserting after the item relating to section 1126 the following new item:

''1127. Protection of classified information relating to budget functions.''.

(b) FUNDING NEEDED TO IMPLEMENT SPECIFIED REQUIREMENTS.—

(1) REIMBURSEMENT.—Notwithstanding any other provision of law, of the amounts authorized to be appropriated or otherwise made available to the Director of National Intelligence under the Intelligence Community Management Account that are available until September 30, 2028, the Director may reimburse a covered official for amounts that the official incurred to implement section 1127(a) of title 31, United States Code, as added by subsection (a).

(2) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, the Secretary of the Treasury, and the heads of the elements of the intelligence community shall jointly submit to the congressional intelligence committees a detailed cost estimate asso-

ciated with the implementation of the requirements under section 1127(a) of title 31, United States Code, as added by subsection (a).

(3) COVERED OFFICIAL DEFINED.—In this subsection, the term ''covered official'' has the meaning given that term in section 1127(d) of title 31, United States Code, as added by subsection (a).

(c) FEDERAL FUNDING ACCOUNTABILITY AND TRANSPARENCY ACT OF 2006.—Section 7 of the Federal Funding Accountability and Transparency Act of 2006 (Public Law 109–282; 31 U.S.C. 6101 note) is amended—

(1) in paragraph (1), by striking ''or'' at the end;

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

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

''(3) information that the Director of National Intelligence, in consultation with the Director of the Office of Management and Budget, determines would result in the exposure of classified programs or activities, including such information that could, when combined with other publicly available information, reveal classified programs or activities.''.

SEC. 804. REVIEW BY COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES OF TRANSACTIONS IN REAL ESTATE NEAR INTELLIGENCE COMMUNITY FACILITIES.

(a) IN GENERAL.—Section 721(a)(4) of the Defense Production Act of 1950 (50 U.S.C. 4565(a)(4)) is amended—

(1) in subparagraph (B)(ii)(II)(bb)(AA), by inserting ", facility owned or operated by an element of the intelligence community," after "military installation"; and

(2) in subparagraph (C)(ii), by inserting ", facility owned or operated by an element of the intelligence community," after "military installation".

(b) APPLICABILITY.—The amendments made by subsection (a) apply with respect to transactions proposed or pending on or after the date of the enactment of this Act.

SEC. 805. INTELLIGENCE SUPPORT TO THE U.S. INTERNATIONAL DEVELOPMENT FINANCE CORPORATION.

The Director of National Intelligence, in coordination with the heads of the other elements of the intelligence community, shall provide intelligence and analytic support to the U.S. International Development Finance Corporation to ensure all projects of the Corporation are appropriately informed and strategically executed in accordance

with the purpose of the Corporation as described in section 1412(b) of the BUILD Act of 2018 (22 U.S.C. 9612(b)).

SEC. 806. ESTABLISHING PROCESSES AND PROCEDURES FOR PROTECTING FEDERAL RESERVE INFORMATION.

(a) IN GENERAL.—The Director of National Intelligence, in coordination with the Director of the Federal Bureau of Investigation, and in consultation with the relevant heads of the elements of the intelligence community, as determined by the Directors, shall—

(1) brief the Board of Governors of the Federal Reserve System on foreign threats to the Federal Reserve System; and

(2) work with the Chair of the Board of Governors of the Federal Reserve System to create and implement standardized security and classification measures for protecting information collected, generated, and stored by the Federal Reserve System.

(b) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Chair of the Board of Governors of the Federal Reserve System shall jointly submit to the appropriate congressional committees a report detailing the sta-

tus of implementing the security measures described in subsection (a).

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

(1) the congressional intelligence committees;

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

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

SEC. 807. AMENDMENTS TO PROHIBIT PAYMENTS TO OBTAIN NATIONAL SECURITY INFORMATION OR APPROVALS.

(a) EXPORT CONTROL REFORM ACT OF 2018.—Section 1756(c) of the Export Control Reform Act of 2018 (50 U.S.C. 4815(c)) is amended—

(1) by inserting '', collected, or paid'' after ''charged''; and

(2) by inserting ''or for the award of such license or other authorization'' after ''this part''.

(b) PROTECTING AMERICANS FROM FOREIGN ADVERSARY CONTROLLED APPLICATIONS ACT.—Section 2(c) of the Protecting Americans from Foreign Adversary

Controlled Applications Act (15 U.S.C. 9901 note; Public Law 118–50) is amended—

(1) in the subsection heading, by inserting ''; PROHIBITION'' after ''EXEMPTIONS''; and

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

''(3) PROHIBITION.—No fee may be charged, collected, or paid in connection with the execution of a qualified divestiture.''.

(c) NATIONAL SECURITY ACT OF 1947.—Section 801 of the National Security Act of 1947 (50 U.S.C. 3161) is amended by adding at the end the following new subsection:

''(c) No fee may be charged, collected, or paid in connection access to classified information.''.

SEC. 808. OFFENSES INVOLVING ESPIONAGE.

(a) IN GENERAL.—Chapter 213 of title 18, United States Code, is amended by adding at the end the following:

''§ 3302. Espionage offenses

''Notwithstanding any other provision of law, an indictment may be found or an information may be instituted at any time without limitation for a violation of section 794 or a conspiracy to violate such section.''.

(b) CLERICAL AMENDMENT.—The table of sections for chapter 213 of title 18, United States Code, is amended by adding at the end the following:

"3302. Espionage offenses.".

(c) CONFORMING AMENDMENT.—Section 19 of the Internal Security Act of 1950 (18 U.S.C. 792 note; 64 Stat. 1005) is amended by striking ", 793, or 794" and inserting "or 793".

SEC. 809. PARENTAL BEREAVEMENT LEAVE.

Section 6329d(b)(1) of title 5, United States Code, is amended by inserting ", including any instance of the natural or spontaneous loss of an unborn child (as defined in section 1841(d) of title 18), such as through miscarriage, stillbirth, or a loss that occurs due to a medical intervention for a pregnancy emergency, such as the treatment of an ectopic pregnancy" after "of the employee".

SEC. 810. DEFINITION OF FOREIGN INSTRUMENTALITY FOR PURPOSES OF ECONOMIC ESPIONAGE PROHIBITION.

Section 1839(1) of title 18, United States Code, is amended—

(1) by striking "that is substantially owned" and inserting the following: "that is—

"(A) substantially owned"; and

(2) by adding at the end the following: "or

''(B) domiciled in a covered nation, as defined in section 4872 of title 10;''.

SEC. 811. PROTECTION OF TRADE SECRETS.

(a) REQUIRING ADVANTAGE TO FOREIGN ENTITY OR INJURY TO UNITED STATES UNDER ECONOMIC ESPIONAGE STATUTE.—Section 1831(a) of title 18, United States Code, is amended, in the matter preceding paragraph (1), by striking ''benefit any foreign government, foreign instrumentality, or foreign agent'' and inserting ''provide any advantage to a foreign government, foreign instrumentality, or foreign agent, or injure or disadvantage in any way the United States, an instrumentality of the United States, or an agent of the United States''.

(b) EXTENDING JURISDICTION OVER ECONOMIC ESPIONAGE AND TRADE SECRET OFFENSES.—Section 1837 of title 18, United States Code, is amended—

(1) in paragraph (1), by striking ''or'' at the end;

(2) in paragraph (2), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(3) the victim is—

''(A) a natural person who is a citizen or permanent resident alien of the United States; or

''(B) a person, including an organization, headquartered or incorporated in the United States; or

''(4) an act committed in furtherance of the offense used or took place through—

''(A) communications in interstate or foreign commerce; or

''(B) financial infrastructure in the United States.''.

(c) CRIMINALIZING UNAUTHORIZED TRANSMISSION OF TRADE SECRETS OUTSIDE THE UNITED STATES.—Section 1832 of title 18, United States Code, is amended by adding at the end the following:

''(c) TRANSMISSION OF TRADE SECRETS OUTSIDE THE UNITED STATES.—

''(1) OFFENSE.—It shall be unlawful for a person to, without authorization, knowingly—

''(A) transmit a trade secret outside the United States;

''(B) attempt to commit an offense described in subparagraph (A); or

''(C) conspire with one or more other persons to commit an offense described in subparagraph (A).

''(2) PENALTIES.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), any person who violates paragraph (1) shall be fined not more than $5,000,000, imprisoned not more than 5 years, or both.

''(B) ORGANIZATIONS.—Any organization that commits an offense described in paragraph (1) shall be fined not less than 3 times the value of the stolen trade secret to the victim, including expenses for research and design and other costs of reproducing the trade secret that the organization has thus avoided.''.

(d) CRIMINALIZING INCITING ECONOMIC ESPIONAGE AND THEFT OF TRADE SECRETS.—Chapter 90 of title 18, United States Code, is amended—

(1) in section 1831, by adding at the end the following:

''(c) INCITEMENT OR SOLICITATION OF ECONOMIC ESPIONAGE.—

''(1) IN GENERAL.—It shall be unlawful for a person to solicit, command, induce, or otherwise endeavor to persuade another person to engage in an offense described in subsection (a).

''(2) PENALTIES.—Any person who violates paragraph (1) shall be fined under this title or imprisoned not more than 10 years, or both.''; and

(2) in section 1832, as amended by subsection (c), by adding at the end the following:

''(d) INCITEMENT OR SOLICITATION OF THEFT OF TRADE SECRETS.—

''(1) IN GENERAL.—It shall be unlawful for a person to solicit, command, induce, or otherwise endeavor to persuade another person to engage in an offense described in subsection (a) or (c).

''(2) PENALTIES.—Any person who violates paragraph (1) shall be fined under this title or imprisoned not more than 10 years, or both.''.

(e) DEFINITION OF FOREIGN INSTRUMENTALITY FOR PURPOSES OF ECONOMIC ESPIONAGE PROHIBITION.—Section 1839(1) of title 18, United States Code, is amended—

(1) by striking ''that is substantially owned'' and inserting the following: ''that is—

''(A) substantially owned''; and

(2) by adding at the end the following: ''or

''(B) domiciled in a covered nation, as defined in section 4872 of title 10;''.

SEC. 812. TECHNICAL AMENDMENTS.

(a) DEFINITION OF ARMED FORCES IN NATIONAL SECURITY ACT OF 1947.—Section 605(8) of the National Security Act of 1947 (50 U.S.C. 3126(8)) is amended by inserting ''Space Force,'' after ''Marine Corps,''.

(b) NATIONAL INTELLIGENCE UNIVERSITY.—Section 6801(a)(4) of the Intelligence Authorization Act for Fiscal Year 2026 (Public Law 119–60) is amended in the matter preceding subparagraph (A) by striking ''3327'' and inserting ''3227''.

Calendar No. 420

119TH CONGRESS
2D 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