117TH CONGRESS
*1st Session*
HOUSE OF REPRESENTATIVES
REPORT
117–156

# INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2022

OCTOBER 28, 2021.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SCHIFF, from the Permanent Select Committee on Intelligence, submitted the following

# R E P O R T

together with

## MINORITY VIEWS

[To accompany H.R. 5412]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 5412) to authorize appropriations for fiscal year 2022 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

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

(a) SHORT TITLE.—This Act may be cited as the "Intelligence Authorization Act for Fiscal Year 2022".

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

# TITLE I—INTELLIGENCE ACTIVITIES

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

Funds are hereby authorized to be appropriated for fiscal year 2022 for the conduct of the intelligence and intelligence-related activities of the following elements of the United States Government:

(1) The Office of the Director of National Intelligence.
(2) The Central Intelligence Agency.
(3) The Department of Defense.
(4) The Defense Intelligence Agency.
(5) The National Security Agency.
(6) The Department of the Army, the Department of the Navy, and the Department of the Air Force.
(7) The Coast Guard.
(8) The Department of State.
(9) The Department of the Treasury.
(10) The Department of Energy.
(11) The Department of Justice.
(12) The Federal Bureau of Investigation.
(13) The Drug Enforcement Administration.
(14) The National Reconnaissance Office.
(15) The National Geospatial-Intelligence Agency.
(16) The Department of Homeland Security.

**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 elements listed in paragraphs (1) through (16) of section 101, 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.

(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 2022 the sum of $619,000,000.

(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 2022 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a).

# 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 2022.

# TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

**SEC. 301. RESTRICTION ON CONDUCT OF INTELLIGENCE ACTIVITIES.**

The authorization of appropriations by this Act shall not be deemed to constitute authority for the conduct of any intelligence activity which is not otherwise authorized by the Constitution or the laws of the United States.

**SEC. 302. 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.

**SEC. 303. TEMPORARY AUTHORITY FOR PAID LEAVE FOR A SERIOUS HEALTH CONDITION.**

(a) AUTHORIZATION OF PAID LEAVE FOR A SERIOUS HEALTH CONDITION FOR EMPLOYEES OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.—

(1) 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. 305. TEMPORARY AUTHORITY FOR PAID LEAVE FOR A SERIOUS HEALTH CONDITION.**

"(a) DEFINITIONS.—In this section:

"(1) PAID SERIOUS HEALTH CONDITION LEAVE.—The term 'paid serious health condition leave' means paid leave taken under subsection (b).

"(2) SERIOUS HEALTH CONDITION.—The term 'serious health condition' has the meaning given the term in section 6381 of title 5, United States Code.

"(3) SON OR DAUGHTER.—The term 'son or daughter' has the meaning given the term in section 6381 of title 5, United States Code.

"(b) PAID SERIOUS HEALTH CONDITION LEAVE.—During the period specified in subsection (f), and notwithstanding any other provision of law, a civilian employee of an element of the intelligence community shall have available a total of 12 administrative workweeks of paid leave during any 12-month period for one or more of the following:

"(1) In order to care for the spouse, or a son, daughter, or parent, of the employee, if such spouse, son, daughter, or parent has a serious health condition.

"(2) Because of a serious health condition that makes the employee unable to perform the functions of the employee's position.

"(c) TREATMENT OF SERIOUS HEALTH CONDITION LEAVE REQUEST.—Notwithstanding any other provision of law, an element of the intelligence community shall accommodate an employee's leave schedule request under subsection (b), including a request to use such leave intermittently or on a reduced leave schedule, to the extent that the requested leave schedule does not unduly disrupt agency operations.

"(d) RULES RELATING TO PAID LEAVE.—During the period specified in subsection (f), and notwithstanding any other provision of law—

"(1) an employee of an element of the intelligence community—

"(A) shall be required to first use all accrued or accumulated paid sick leave before being allowed to use paid serious health condition leave; and

"(B) may not be required to first use all or any portion of any unpaid leave available to the employee before being allowed to use paid serious health condition leave; and

"(2) paid serious health condition leave—

"(A) shall be payable from any appropriation or fund available for salaries or expenses for positions within the employing element;

"(B) may not be considered to be annual or vacation leave for purposes of section 5551 or 5552 of title 5, United States Code, or for any other purpose;

"(C) if not used by the employee before the end of the 12-month period described in subsection (b) to which the leave relates, may not be available for any subsequent use and may not be converted into a cash payment;

"(D) may be granted only to the extent that the employee does not receive a total of more than 12 weeks of paid serious health condition leave in any 12-month period;

"(E) shall be used in increments of hours (or fractions thereof), with 12 administrative workweeks equal to 480 hours for employees of elements of the intelligence community with a regular full-time work schedule and converted to a proportional number of hours for employees of such elements with part-time, seasonal, or uncommon tours of duty; and

"(F) may not be used during off-season (nonpay status) periods for employees of such elements with seasonal work schedules.

"(e) IMPLEMENTATION.—

"(1) CONSISTENCY WITH SERIOUS HEALTH CONDITION LEAVE UNDER TITLE 5.—The Director of National Intelligence shall carry out this section in a manner consistent, to the extent appropriate, with the administration of leave taken under section 6382 of title 5, United States Code, for a reason described in subparagraph (C) or (D) of subsection (a)(1) of that section, including with respect to the authority to require a certification described in section 6383 of such title.

"(2) IMPLEMENTATION PLAN.—Not later than 1 year after the date of enactment of this section, the Director of National Intelligence shall submit to the congressional intelligence committees an implementation plan that includes—

"(A) processes and procedures for implementing the paid serious health condition leave policies under subsections (b) through (d) during the period specified in subsection (f);

"(B) an explanation of how such implementation will be reconciled with policies of other elements of the Federal Government, including the impact on elements funded by the National Intelligence Program that are housed within agencies outside the intelligence community;

"(C) the projected impact of such implementation on the workforce of the intelligence community, including take rates, retention, recruiting, and morale, broken down by each element of the intelligence community; and

"(D) all costs or operational expenses associated with such implementation.

"(3) DIRECTIVE.—Not later than 90 days after the Director of National Intelligence submits the implementation plan under paragraph (2), the Director of National Intelligence shall issue a written directive to implement this section, which directive shall take effect on the date of issuance.

"(f) DURATION OF AUTHORITY.—The authority and requirements under subsections (b) through (d) shall only apply during the 3-year period beginning on the date on which the Director of National Intelligence issues the written directive under subsection (e)(3).

"(g) ANNUAL REPORT.—During the period specified in subsection (f), the Director of National Intelligence shall submit to the congressional intelligence committees an annual report that—

"(1) details the number of employees of each element of the intelligence community who applied for and took paid serious health condition leave during the year covered by the report;

"(2) includes updates on major implementation challenges or costs associated with paid serious health condition leave; and

"(3) includes a recommendation of the Director with respect to whether to extend the period specified in subsection (f).".

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

"Sec. 305. Temporary authority for paid leave for a serious health condition.".

(b) APPLICABILITY.—Section 305 of the National Security Act of 1947, as added by subsection (b), shall apply with respect to leave taken in connection with a serious health condition (as defined in subsection (a) of such section 305) that occurs or continues to exist during the period specified in subsection (f) of such section.

**SEC. 304. HARMONIZATION OF WHISTLEBLOWER PROTECTIONS.**

(a) PROHIBITED PERSONNEL PRACTICES IN THE INTELLIGENCE COMMUNITY.—

(1) THREATS RELATING TO PERSONNEL ACTIONS.—

(A) AGENCY EMPLOYEES.—Section 1104(b) of the National Security Act of 1947 (50 U.S.C. 3234(b)) is amended, in the matter preceding paragraph (1)—

(i) by striking "Any employee of an agency" and inserting "Any employee of a covered intelligence community element or an agency"; and

(ii) by inserting ", or threaten to take or fail to take," after "take or fail to take".

(B) CONTRACTOR EMPLOYEES.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)) is amended, in the matter preceding subparagraph (A), by inserting ", or threaten to take or fail to take," after "take or fail to take".

(2) PROTECTION FOR CONTRACTOR EMPLOYEES AGAINST REPRISAL FROM AGENCY EMPLOYEES.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)), as amended by paragraph (1)(B) of this subsection, is further amended, in the matter preceding subparagraph (A), by inserting "of an agency or" after "Any employee".

(3) ENFORCEMENT.—Subsection (d) of section 1104 of such Act (50 U.S.C. 3234) is amended to read as follows:

"(d) ENFORCEMENT.—The President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.".

(b) RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.—

(1) ENFORCEMENT.—Section 3001(j) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)) is amended—

(A) by redesignating paragraph (8) as paragraph (9); and

(B) by inserting after paragraph (7) the following:

"(8) ENFORCEMENT.—Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.".

(2) TOLLING OF DEADLINE FOR APPEAL OF PROHIBITED REPRISAL.—Section 3001(j)(4) of such Act (50 U.S.C. 3341(j)(4)) is amended—

(A) in subparagraph (A), by inserting "(except as provided by subparagraph (D))" after "within 90 days"; and

(B) by adding at the end the following new subparagraph:

"(D) TOLLING.—The time requirement established by subparagraph (A) for an employee or former employee to appeal the decision of an agency may be tolled if the employee or former employee presents substantial credible evidence showing why the employee or former employee did not timely initiate the appeal and why the enforcement of the time requirement would be unfair, such as evidence showing that the employee or former employee—

"(i) did not receive notice of the decision; or

"(ii) could not timely initiate the appeal because of factors beyond the control of the employee or former employee.".

(c) CORRECTION OF DEFINITION OF AGENCY.—Section 3001(a)(1)(B) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(a)(1)(B)) is amended by striking "and" and inserting "or".

(d) ESTABLISHING CONSISTENCY WITH RESPECT TO PROTECTIONS FOR DISCLOSURES OF MISMANAGEMENT.—

(1) SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—Section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)) is amended—

(A) in subparagraph (A)(ii), by striking "gross mismanagement" and inserting "mismanagement"; and

(B) in subparagraph (B)(ii), by striking "gross mismanagement" and inserting "mismanagement".

(2) PERSONNEL ACTIONS AGAINST CONTRACTOR EMPLOYEES.—Section 1104(c)(1)(B) of the National Security Act of 1947 (50 U.S.C. 3234(c)(1)(B)) is amended by striking "gross mismanagement" and inserting "mismanagement".

(e) PROTECTED DISCLOSURES TO SUPERVISORS.—

(1) PERSONNEL ACTIONS.—

(A) DISCLOSURES BY AGENCY EMPLOYEES TO SUPERVISORS.—Section 1104(b) of the National Security Act of 1947 (50 U.S.C. 3234(b)), as amended by subsection (a)(1)(A), is further amended, in the matter preceding paragraph (1), by inserting "a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including" before "the head of the employing agency".

(B) DISCLOSURES BY CONTRACTOR EMPLOYEES TO SUPERVISORS.—Section 1104(c)(1) of such Act (50 U.S.C. 3234(c)(1)), as amended by subsection (a), is further amended, in the matter preceding subparagraph (A), by inserting "a supervisor in the contractor employee's direct chain of command, or a supervisor of the contracting agency with responsibility for the subject matter of the disclosure, up to and including" before "the head of the contracting agency".

(2) SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—Section 3001(j)(1)(A) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)(A)) is amended, in the matter preceding clause (i), by inserting "a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including" before "the head of the employing agency".

(f) ESTABLISHING PARITY FOR PROTECTED DISCLOSURES.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is further amended—

(1) in subsection (b), as amended by subsections (a)(1)(A) and (e)(1)(A)—

(A) by redesignating paragraphs (1) and (2) as subparagraphs (A) and (B), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the right;

(B) in the matter preceding subparagraph (A), as redesignated and moved by subparagraph (A) of this paragraph, by striking "for a lawful disclosure" and inserting the following: "for—

"(1) any lawful disclosure"; and

(C) by adding at the end the following:

"(2) any lawful disclosure that complies with—

"(A) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

"(B) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or

"(C) subparagraphs (A), (D), and (I) of section 103H(k)(5); or

"(3) if the actions do not result in the employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

"(A) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

"(B) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in subparagraph (A); or

"(C) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General."; and

(2) in subsection (c)(1), as amended by subsections (a) and (e)(1)(B)—

(A) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and moving such clauses, as so redesignated, 2 ems to the right;

(B) in the matter preceding clause (i), as redesignated and moved by subparagraph (A) of this paragraph, by striking "for a lawful disclosure" and inserting the following: "for—

"(A) any lawful disclosure"; and

(C) by adding at the end the following:

"(B) any lawful disclosure that complies with—

"(i) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

"(ii) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or

"(iii) subparagraphs (A), (D), and (I) of section 103H(k)(5); or

"(C) if the actions do not result in the contractor employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

"(i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

"(ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or

"(iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.".

(g) CLARIFICATION RELATING TO PROTECTED DISCLOSURES.—Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is further amended—

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

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

"(d) RULE OF CONSTRUCTION.—Consistent with the protection of sources and methods, nothing in subsection (b) or (c) shall be construed to authorize—

"(1) the withholding of information from Congress; or

"(2) the taking of any personnel action against an employee who lawfully discloses information to Congress.

"(e) DISCLOSURES.—A disclosure shall not be excluded from this section because—

"(1) the disclosure was made to an individual, including a supervisor, who participated in an activity that the employee reasonably believed to be covered under subsection (b)(1)(B) or the contractor employee reasonably believed to be covered under subsection (c)(1)(A)(ii);

"(2) the disclosure revealed information that had been previously disclosed;

"(3) the disclosure was not made in writing;

"(4) the disclosure was made while the employee was off duty;

"(5) of the amount of time which has passed since the occurrence of the events described in the disclosure; or

"(6) the disclosure was made during the normal course of duties of an employee or contractor employee.".

(h) CORRECTION RELATING TO NORMAL COURSE DISCLOSURES.—Section 3001(j)(3) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(3)) is amended—

(1) by striking "DISCLOSURES.—" and all that follows through "because—" and inserting "DISCLOSURES.—A disclosure shall not be excluded from paragraph (1) because—";

(2) by striking subparagraph (B);

(3) by redesignating clauses (i) through (v) as subparagraphs (A) through (E), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the left;

(4) in subparagraph (D), as so redesignated, by striking "or" at the end;

(5) in subparagraph (E), as redesignated by paragraph (3), by striking the period at the end and inserting "; or"; and

(6) by adding at the end the following:

"(F) the disclosure was made during the normal course of duties of an employee.".

(i) CLARIFICATION RELATING TO RULE OF CONSTRUCTION.—Section 3001(j)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(2)) is amended by inserting "or clearance action" after "personnel action".

(j) CLARIFICATION RELATING TO PROHIBITED PRACTICES.—Section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)), as amended by this section, is further amended by striking "over" and inserting "to take, direct others to take, recommend, or approve".

(k) TECHNICAL CORRECTION.—Section 3001(j)(1)(C)(i) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)(C)(i)) is amended by striking "(h)" and inserting "(g)".

(l) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community shall submit to the congressional intelligence committees a report assessing the extent to which protections provided under Presidential Policy Directive 19 (relating to protecting whistleblowers with access to classified information) have been codified in statutes.

**SEC. 305. CONGRESSIONAL OVERSIGHT OF CERTAIN SPECIAL ACCESS PROGRAMS.**

(a) IN GENERAL.—Title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) is amended by inserting after section 501 the following new section (and conforming the table of contents at the beginning of such Act accordingly):

**"SEC. 501A. CONGRESSIONAL OVERSIGHT OF CERTAIN SPECIAL ACCESS PROGRAMS.**

"(a) REPORTS AND NOTIFICATIONS.—At the same time that the Secretary of Defense submits any report or notification under section 119 of title 10, United States Code, that relates to a covered special access program or a new covered special access program, the Secretary shall also submit such report or notification to the congressional intelligence committees.

"(b) BRIEFINGS.—On a periodic basis, but not less frequently than semiannually, the Secretary of Defense shall provide to the chairmen and ranking minority members of the congressional intelligence committees, and to any staff of such a committee designated by either the chair or ranking member for purposes of this subsection, a briefing on covered special access programs. Each such briefing shall include, at a minimum—

"(1) a description of the activity of the program during the period covered by the briefing; and

"(2) documentation with respect to how the program has achieved outcomes consistent with requirements documented by the Director of National Intelligence and the Secretary of Defense.

"(c) NOTIFICATIONS ON COMPARTMENTS AND SUBCOMPARTMENTS.—

"(1) REQUIREMENT.—Except as provided by paragraph (2), a head of an element of the intelligence community may not establish a compartment or a subcompartment under a covered special access program until the head notifies the congressional intelligence committees of such compartment or subcompartment, as the case may be.

"(2) WAIVER.—

"(A) DETERMINATION.—On a case-by-case basis, the Director of National Intelligence may waive the requirement under paragraph (1). Not later than two days after making such a waiver, the Director shall notify the con-

gressional intelligence committees of the waiver, including a justification for the waiver.

"(B) SUBMISSION.—Not later than 30 days after the date on which the Director makes a waiver under subparagraph (A), the head of the element of the intelligence community for whom the waiver was made shall submit to the congressional intelligence committees the notification required under paragraph (1) relating to such waiver.

"(d) ANNUAL REPORTS.—

"(1) REQUIREMENT.—On an annual basis, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report on covered special access programs administered by the head.

"(2) MATTERS INCLUDED.—Each report shall include, with respect to the period covered by the report, the following:

"(A) A list of all compartments and subcompartments of covered special access programs active as of the date of the report.

"(B) A list of all compartments and subcompartments of covered special access programs terminated during the period covered by the report.

"(C) With respect to the report submitted by the Director of National Intelligence, in addition to the matters specified in subparagraphs (A) and (B)—

"(i) a certification regarding whether the creation, validation, or substantial modification, including termination, for all existing and proposed covered special access programs, and the compartments and subcompartments within each, are substantiated and justified based on the information required by clause (ii); and

"(ii) for each certification—

"(I) the rationale for the revalidation, validation, or substantial modification, including termination, of each covered special access program, compartment, and subcompartment;

"(II) the identification of a control officer for each covered special access program; and

"(III) a statement of protection requirements for each covered special access program.

"(e) COVERED SPECIAL ACCESS PROGRAM DEFINED.—In this section, the term 'covered special access program' means a special access program that receives funding under the National Intelligence Program or the Military Intelligence Program, relates to an intelligence or intelligence-related activity, or both.".

(b) FIRST REPORT.—Not later than 30 days after the date of the enactment of this Act, the head of each element of the intelligence community shall submit to the congressional intelligence committees the first report required under section 501A(d)(1) of the National Security Act of 1947, as added by subsection (a).

(c) CONFORMING REPEAL.—Section 608 of the Intelligence Authorization Act for Fiscal Year 2017 (division N of Public Law 115–31; 131 Stat. 833; 50 U.S.C. 3315) is amended by striking subsection (b).

**SEC. 306. CLARIFICATION OF REQUIREMENT FOR AUTHORIZATION OF FUNDING FOR INTELLIGENCE ACTIVITIES.**

Paragraph (1) of section 504(a) of the National Security Act of 1947 (50 U.S.C. 3094(a)) is amended to read as follows:

"(1) those funds were specifically authorized by Congress for use for such intelligence or intelligence-related activities; or".

**SEC. 307. AUTHORIZATION OF SUPPORT BY DIRECTOR OF NATIONAL INTELLIGENCE FOR CERTAIN ACTIVITIES RELATING TO INTELLIGENCE COMMUNITY WORKFORCE.**

Title X of the National Security Act of 1947 (50 U.S.C. 3191 et seq.) is amended by inserting after section 1024 the following new section (and conforming the table of contents at the beginning of such Act accordingly):

**"SEC. 1025. AUTHORIZATION OF SUPPORT BY DIRECTOR OF NATIONAL INTELLIGENCE FOR CERTAIN WORKFORCE ACTIVITIES.**

"(a) AUTHORIZATION.—The Director may, with or without reimbursement, obligate or expend amounts authorized to be appropriated or otherwise made available for the Office of the Director of National Intelligence for covered workforce activities for the purpose of supporting a covered workforce activity of an element of the intelligence community.

"(b) COVERED WORKFORCE ACTIVITY DEFINED.—In this section, the term 'covered workforce activity' means an activity relating to—

"(1) recruitment or retention of the intelligence community workforce; or

"(2) diversity, equality, inclusion, or accessibility, with respect to such workforce.".

**SEC. 308. REQUIREMENTS FOR CERTAIN EMPLOYMENT ACTIVITIES BY FORMER INTELLIGENCE OFFICERS AND EMPLOYEES.**

(a) MODIFICATIONS TO REQUIREMENT.—

(1) IN GENERAL.—Section 304 of the National Security Act of 1947 (50 U.S.C. 3073a) is amended to read as follows:

**"SEC. 304. REQUIREMENTS FOR CERTAIN EMPLOYMENT ACTIVITIES BY FORMER INTELLIGENCE OFFICERS AND EMPLOYEES.**

"(a) TEMPORARY RESTRICTION.—An employee of an element of the intelligence community who occupies a covered intelligence position may not occupy a covered post-service position during the 30-month period following the date on which the employee ceases to occupy a covered intelligence position.

"(b) COVERED POST-SERVICE EMPLOYMENT REPORTING.—

"(1) REQUIREMENT.—During the 5-year period beginning on the date on which an employee ceases to occupy a covered intelligence position, the employee shall—

"(A) report covered post-service employment to the head of the element of the intelligence community that employed such employee in such covered intelligence position upon accepting such covered post-service employment; and

"(B) annually (or more frequently if the head of such element considers it appropriate) report covered post-service employment to the head of such element.

"(2) REGULATIONS.—The head of each element of the intelligence community shall issue regulations requiring, as a condition of employment, each employee of such element occupying a covered intelligence position to sign a written agreement requiring the regular reporting of covered post-service employment to the head of such element pursuant to paragraph (1).

"(c) PENALTIES.—

"(1) CRIMINAL PENALTIES.—A former employee who knowingly and willfully violates subsection (a) or who knowingly and willfully fails to make a required report under subsection (b) shall be fined under title 18, United States Code, or imprisoned for not more than 5 years, or both. Each report under subsection (b) shall be subject to section 1001 of title 18, United States Code.

"(2) SECURITY CLEARANCES.—The head of an element of the intelligence community shall revoke the security clearance of a former employee if the former employee knowingly and willfully fails to make a required report under subsection (b) or knowingly and willfully makes a false report under such subsection.

"(d) PROVISION OF INFORMATION.—

"(1) TRAINING.—The head of each element of the intelligence community shall regularly provide training on the reporting requirements under subsection (b) to employees of that element who occupy a covered intelligence position.

"(2) WRITTEN NOTICE.—The head of each element of the intelligence community shall provide written notice of the reporting requirements under subsection (b) to an employee when the employee ceases to occupy a covered intelligence position.

"(e) ANNUAL REPORTS.—

"(1) REQUIREMENT.—Not later than March 31 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report on covered post-service employment occurring during the year covered by the report.

"(2) ELEMENTS.—Each report under paragraph (1) shall include the following:

"(A) The number of former employees who occupy a covered post-service position, broken down by—

"(i) the name of the employer;

"(ii) the foreign government, including by the specific foreign individual, agency, or entity, for whom the covered post-service employment is being performed; and

"(iii) the nature of the services provided as part of the covered post-service employment.

"(B) A certification by the Director that—

"(i) each element of the intelligence community maintains adequate systems and processes for ensuring that former employees are submitting reports required under subsection (b);

"(ii) to the knowledge of the heads of the elements of the intelligence community, all former employees who occupy a covered post-service position are in compliance with this section;

"(iii) the services provided by former employees who occupy a covered post-service position do not—

"(I) pose a current or future threat to the national security of the United States; or

"(II) pose a counterintelligence risk; and

"(iv) the Director and the heads of such elements are not aware of any credible information or reporting that any former employee who occupies a covered post-service position has engaged in activities that violate Federal law, infringe upon the privacy rights of United States persons, or constitute abuses of human rights.

"(3) FORM.—Each report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

"(f) NOTIFICATION.—In addition to the annual reports under subsection (e), if a head of an element of the intelligence community determines that the services provided by a former employee who occupies a covered post-service position pose a threat or risk described in clause (iii) of paragraph (2)(B) of such subsection, or include activities described in clause (iv) of such paragraph, the head shall notify the congressional intelligence committees of such determination by not later than 7 days after making such determination. The notification shall include the following:

"(1) The name of the former employee.

"(2) The name of the employer.

"(3) The foreign government, including the specific foreign individual, agency, or entity, for whom the covered post-service employment is being performed.

"(4) As applicable, a description of—

"(A) the risk to national security, the counterintelligence risk, or both; and

"(B) the activities that may violate Federal law, infringe upon the privacy rights of United States persons, or constitute abuses of human rights.

"(g) DEFINITIONS.—In this section:

"(1) COVERED INTELLIGENCE POSITION.—The term 'covered intelligence position' means a position within an element of the intelligence community that, based on the level of access of a person occupying such position to information regarding sensitive intelligence sources or methods or other exceptionally sensitive matters, the head of such element determines should be subject to the requirements of this section.

"(2) COVERED POST-SERVICE EMPLOYMENT.—The term 'covered post-service employment' means direct or indirect employment by, representation of, or any provision of advice or services relating to national security, intelligence, the military, or internal security to, the government of a foreign country or any company, entity, or other person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized, in whole or in major part, by any government of a foreign country.

"(3) COVERED POST-SERVICE POSITION.—The term 'covered post-service position' means a position of employment described in paragraph (2).

"(4) EMPLOYEE.—The term 'employee', with respect to an employee occupying a covered intelligence position, includes an officer or official of an element of the intelligence community, a contractor of such an element, a detailee to such an element, or a member of the Armed Forces assigned to such an element.

"(5) FORMER EMPLOYEE.—The term 'former employee' means an individual—

"(A) who was an employee occupying a covered intelligence position; and

"(B) who is subject to the requirements under subsection (a) or (b).

"(6) GOVERNMENT OF A FOREIGN COUNTRY.—The term 'government of a foreign country' has the meaning given the term in section 1(e) of the Foreign Agents Registration Act of 1938 (22 U.S.C. 611(e)).".

(2) APPLICATION.—Such section 304, as amended by paragraph (1), shall apply with respect to employees who occupy covered intelligence positions (as defined in such section) on or after the date of the enactment of this Act.

(3) REVISED REGULATIONS.—

(A) SUBMISSION.—Not later than 90 days after the date of the enactment of this Act, the head of each element of the intelligence community shall submit to the congressional intelligence committees new or updated regulations issued under such section 304, as amended by paragraph (1).

(B) CERTIFICATION.—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—

(i) a written certification for each head of an element of the intelligence community who has issued the updated regulations under such section 304, as amended by paragraph (1); and

(ii) for each head of an element of the intelligence community who has not issued such updated regulations, an explanation for the failure to issue such updated regulations.

(4) INITIAL REPORT.—In the first report submitted by the Director of National Intelligence under subsection (e) of such section 304, as amended by paragraph (1), the Director shall include an assessment of the licensing requirements under the Arms Export Control Act (22 U.S.C. 2751 et seq.) and recommendations with respect to strengthening the activities regulated under such section 304.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such Act is amended by striking the item relating to section 304 and inserting the following new item:

"Sec. 304. Requirements for certain employment activities by former intelligence officers and employees.".

**SEC. 309. NON-REIMBURSABLE DETAIL OF INTELLIGENCE COMMUNITY PERSONNEL TO ASSIST WITH PROCESSING AND RESETTLEMENT OF REFUGEES, PAROLEES, AND OTHER ALIENS FROM AFGHANISTAN.**

Section 113A of the National Security Act of 1947 (50 U.S.C. 3049) is amended—

(1) by striking "An officer" and inserting "(a) IN GENERAL.—An officer";

(2) by striking "section" both places it appears and inserting "subsection"; and

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

"(b) PROCESSING AND RESETTLEMENT OF REFUGEES, PAROLEES, AND OTHER ALIENS FROM AFGHANISTAN.—An officer or employee of an element of the intelligence community may be detailed to another element of the United States Government on a non-reimbursable basis for the purpose of providing assistance with the processing and resettlement of refugees, parolees, and other aliens, from Afghanistan, as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed 1 year. This subsection does not limit any other source of authority for reimbursable or non-reimbursable details. A non-reimbursable detail made under this subsection shall not be considered an augmentation of the appropriations of the receiving element of the United States Government.".

**SEC. 310. AUTHORITY FOR TRANSPORT OF CERTAIN CANINES ASSOCIATED WITH FORCE PROTECTION DUTIES OF INTELLIGENCE COMMUNITY.**

Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by inserting after section 116 the following new section (and conforming the table of contents at the beginning of such Act accordingly):

**"SEC. 116A. AUTHORITY FOR TRANSPORTATION OF CERTAIN CANINES ASSOCIATED WITH FORCE PROTECTION DUTIES OF INTELLIGENCE COMMUNITY.**

"(a) TRANSPORTATION.—For purposes of section 1344 of title 31, United States Code, the transportation of federally owned canines associated with force protection duties of an element of the intelligence community between the residence of an officer or employee of the element and various locations that is essential for the performance of the force protection duty shall be deemed essential for the safe and efficient performance of intelligence duties.

"(b) OFFICERS AND EMPLOYEES COVERED.—In the administration of section 1344 of title 31, United States Code, an officer or employee of an element of the intelligence community shall be treated as being listed in subsection (b).".

**SEC. 311. DEVELOPMENT OF DEFINITIONS FOR CERTAIN TERMS RELATING TO INTELLIGENCE.**

(a) DEVELOPMENT.—Not later than September 30, 2023, the Director of National Intelligence and the Under Secretary of Defense for Intelligence and Security, in consultation with the heads of the elements of the intelligence community, shall jointly develop and publish definitions for the following terms:

(1) Acoustic intelligence.
(2) All-source intelligence.
(3) Communications intelligence.
(4) Critical intelligence.
(5) Cyber-threat intelligence.
(6) Electronic intelligence.
(7) Explosive ordnance intelligence.
(8) General military intelligence.
(9) Imagery intelligence.
(10) Instrumentation signals intelligence.
(11) Intelligence-related activity.
(12) Joint intelligence.
(13) Measurement and signature intelligence.
(14) Medical intelligence.
(15) Open-source intelligence.
(16) Operational intelligence.
(17) Scientific and technical intelligence.
(18) Signals intelligence.

(19) Strategic intelligence.
(20) Tactical intelligence.
(21) Target intelligence.
(22) Technical intelligence.
(23) Such others terms as may be jointly determined necessary by the Director of National Intelligence and the Under Secretary of Defense for Intelligence and Security.

(b) APPLICATION TO ACTIVITIES OF INTELLIGENCE COMMUNITY.—The Director of National Intelligence shall ensure that the definitions developed under subsection (a) are used uniformly across activities of the intelligence community with respect to the corresponding terms specified in such subsection.

(c) NOTICE OF MODIFICATIONS.—The Director of National Intelligence and the Under Secretary of Defense for Intelligence shall submit to the congressional intelligence committees notification of any modification by the Director and Under Secretary to a definition of a term specified in subsection (a) following the initial publication of the definition under such subsection.

(d) DEFINITIONS.—In this section, the terms "congressional intelligence committees" and "intelligence community" have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

**SEC. 312. SUPPORT FOR AND OVERSIGHT OF UNIDENTIFIED AERIAL PHENOMENA TASK FORCE.**

(a) AVAILABILITY OF DATA ON UNIDENTIFIED AERIAL PHENOMENA.—The Director of National Intelligence shall ensure that each element of the intelligence community with data relating to unidentified aerial phenomena makes such data available immediately to the Unidentified Aerial Phenomena Task Force, or successor entity, and to the National Air and Space Intelligence Center.

(b) QUARTERLY REPORTS.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, and not less frequently than quarterly thereafter, the Unidentified Aerial Phenomena Task Force, or successor entity, shall submit to the appropriate congressional committees a report on the findings of the Unidentified Aerial Phenomena Task Force, or successor entity.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, at a minimum, the following:

(A) All reported unidentified aerial phenomena-related events that occurred during the period covered by the report.

(B) All reported unidentified aerial phenomena-related events that occurred during a period other than the period covered by the report but were not included in an earlier report.

(3) FORM.—Each report submitted under paragraph (1) shall be submitted in classified form, consistent with the protection of intelligence sources and methods.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means the following:

(A) The congressional intelligence committees.

(B) The Committees on Armed Services of the House of Representatives and the Senate.

(2) UNIDENTIFIED AERIAL PHENOMENA TASK FORCE.—The term "Unidentified Aerial Phenomena Task Force" means the task force established by the Department of Defense on August 4, 2020, to be led by the Department of the Navy, under the Office of the Under Secretary of Defense for Intelligence and Security.

# TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

## Subtitle A—Office of the Director of National Intelligence

**SEC. 401. NATIONAL COUNTERPROLIFERATION AND BIOSECURITY CENTER.**

(a) REDESIGNATION OF CENTER.—Section 119A of the National Security Act of 1947 (50 U.S.C. 3057) is amended by striking "National Counter Proliferation Center" each place it appears and inserting "National Counterproliferation and Biosecurity Center".

(b) ESTABLISHMENT AND HEAD.—Subsection (a) of such section is amended—

(1) in paragraph (1)—

(A) by striking "government tools to prevent" and inserting "government tools to—

"(A) prevent";

(B) by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new subparagraph:

"(B) lead integration and mission management of all intelligence activities pertaining to biosecurity and foreign biological threats."; and

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

"(4) The Director of the National Counterproliferation and Biosecurity Center shall serve as the principal coordinator for the intelligence community, and as the principal advisor to the Director of National Intelligence, with respect to biosecurity and foreign biological threats.".

(c) MISSIONS AND OBJECTIVES.—Subsection (b) of such section is amended—

(1) by redesignating paragraphs (1) through (7) as subparagraphs (A) through (G), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the right;

(2) in the matter preceding subparagraph (A), as so redesignated, by striking "In establishing" and inserting the following:

"(1) COUNTERPROLIFERATION.—In establishing"; and

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

"(2) BIOSECURITY.—In establishing the National Counterproliferation and Biosecurity Center, the President shall address the following missions and objectives to ensure that the Center serves as the lead for the intelligence community for the integration, mission management, and coordination of intelligence activities pertaining to biosecurity and foreign biological threats, regardless of origin:

"(A) Ensuring that the elements of the intelligence community provide timely and effective warnings to the President and the Director of National Intelligence regarding emerging foreign biological threats, including diseases with pandemic potential.

"(B) Overseeing and coordinating the collection and analysis of intelligence on biosecurity and foreign biological threats in support of the intelligence needs of the Federal departments and agencies responsible for public health, including by conveying collection priorities to elements of the intelligence community.

"(C) Coordinating intelligence support to the Federal departments and agencies responsible for public health, including by ensuring that intelligence pertaining to biosecurity and foreign biological threats is disseminated among appropriately cleared personnel of such departments and agencies.

"(D) Coordinating with the Federal departments and agencies responsible for public health to encourage information sharing with the intelligence community.

"(E) Identifying gaps in the capabilities of the intelligence community regarding biosecurity and countering foreign biological threats and providing to the Director of National Intelligence recommended solutions for such gaps, including by encouraging research and development of new capabilities to counter foreign biological threats.".

(d) CONFORMING AMENDMENTS.—Such section is further amended—

(1) by striking "counter proliferation" each place it appears and inserting "counterproliferation"; and

(2) in the section heading, by striking "COUNTER PROLIFERATION" and inserting "COUNTERPROLIFERATION AND BIOSECURITY" (and conforming the table of sections at the beginning of such Act accordingly).

(e) REFERENCES.—Any reference in any law, regulation, guidance, instruction, or other document of the United States Government to the National Counter Proliferation Center shall be deemed to refer to the National Counterproliferation and Biosecurity Center.

**SEC. 402. CLARIFICATION OF CERTAIN RESPONSIBILITIES OF DIRECTOR OF NATIONAL INTELLIGENCE.**

Section 102A(f)(8) of the National Security Act of 1947 (50 U.S.C. 3024(f)(8)) is amended by striking "such other functions" and inserting "such other intelligence-related functions".

**SEC. 403. RESPONSIBILITY OF DIRECTOR OF NATIONAL INTELLIGENCE REGARDING NATIONAL INTELLIGENCE PROGRAM BUDGET CONCERNING FEDERAL BUREAU OF INVESTIGATION.**

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:

"(aa) RESPONSIBILITY OF DIRECTOR OF NATIONAL INTELLIGENCE REGARDING NATIONAL INTELLIGENCE PROGRAM BUDGET CONCERNING FEDERAL BUREAU OF INVESTIGATION.—(1) Consistent with subsection (c)(5)(C), the Director of National Intelligence shall, after consultation with the Director of the Federal Bureau of Investigation, ensure that the programs and activities of the Federal Bureau of Investigation that are part of the National Intelligence Program are executed in a manner that conforms with the requirements of the national intelligence strategy under section 108A and the National Intelligence Priorities Framework of the Office of the Director of National Intelligence (or any successor mechanism established for the prioritization of such programs and activities).

"(2) Consistent with subsection (c)(5)(C), the Director of National Intelligence shall ensure that the programs and activities that are part of the National Intelligence Program, including those of the Federal Bureau of Investigation, are structured and executed in a manner than enables budget traceability.".

**SEC. 404. CLIMATE SECURITY ADVISORY COUNCIL.**

(a) REPORTS.—Subsection (d) of section 120 of the National Security Act of 1947 (50 U.S.C. 3060) is amended—

(1) by striking "Not later" and inserting the following:

"(1) REQUIREMENT.—Not later"; and

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

"(2) MATTERS INCLUDED.—Each report under paragraph (1) shall include a description of any obstacles or gaps relating to—

"(A) the Council fulfilling its duties and responsibilities under subsection (c); or

"(B) the responsiveness of the intelligence community to the climate security needs and priorities of the policymaking elements of the Federal Government.".

(b) EXTENSION OF SUNSET; TECHNICAL AMENDMENTS.—Such section 120 is amended—

(1) in subsection (b)(1)(B)(v), by inserting "and Security" after "for Intelligence";

(2) by redesignating the second subsection (e) as subsection (f); and

(3) in subsection (e), by striking "the date that is 4 years after the date of the enactment of this section" and inserting "December 31, 2025".

# Subtitle B—Other Elements

**SEC. 411. PROTECTION OF CERTAIN FACILITIES AND ASSETS OF CENTRAL INTELLIGENCE AGENCY FROM UNMANNED AIRCRAFT.**

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

**"SEC. 15A. PROTECTION OF CERTAIN FACILITIES AND ASSETS OF CENTRAL INTELLIGENCE AGENCY FROM UNMANNED AIRCRAFT.**

"(a) AUTHORITY.—In accordance with subsection (b), the Director shall have the same authority for the Agency as is available to the Secretary of Homeland Security for the Department of Homeland Security and the Attorney General for the Department of Justice under section 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n), and shall be subject to the same limitations and requirements under such section.

"(b) ADMINISTRATION.—For purposes of subsection (a)—

"(1) the reference in subsection (i) of section 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n) to 'the date that is 4 years after the date of enactment of this section' shall be deemed to be a reference to 'October 5, 2026';

"(2) the term 'appropriate congressional committees' as defined in paragraph (1) of subsection (k) of such section shall be deemed to mean the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate; and

"(3) the term 'covered facility or asset' as defined in paragraph (3) of such subsection (k) shall be deemed to mean installations, property, and persons—

"(A) that are located in the United States;

"(B) for which the Director may provide protection pursuant to section 5(a)(4) or 15(a)(1) of this Act; and

"(C) that the Director identifies as high-risk and a potential target for unlawful unmanned aircraft activity.".

**SEC. 412. MODIFICATION OF NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY PERSONNEL MANAGEMENT AUTHORITY TO ATTRACT EXPERTS IN SCIENCE AND ENGINEERING.**

Section 1599h(b)(2)(A) of title 10, United States Code, is amended—

(1) by striking "paragraph (1)(B)" and inserting "subparagraph (B) of paragraph (1)"; and

(2) by inserting "or employees appointed pursuant to the first subparagraph (G) of such paragraph to any of 2 positions of administration or management designated by the Director of the National Geospatial-Intelligence Agency for purposes of this subparagraph" after "this subparagraph".

**SEC. 413. REQUIREMENTS FOR TERMINATION OF DUAL-HAT ARRANGEMENT FOR COMMANDER OF THE UNITED STATES CYBER COMMAND.**

Section 1642 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 130 Stat. 2601), as amended by section 1636 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1748), is further amended—

(1) by striking subsections (a), (b), and (c), and inserting the following new subsections:

"(a) LIMITATION ON TERMINATION OF DUAL-HAT ARRANGEMENT.—The Secretary of Defense may not terminate the dual-hat arrangement until the date on which the Secretary submits to the appropriate committees of Congress the certification under subsection (b)(1). The Secretary shall implement such termination by not later than the first day of the fiscal year following the fiscal year in which the Secretary submits such certification.

"(b) ANNUAL SUBMISSION OF INFORMATION.—Together with the defense budget materials for fiscal year 2023, and annually thereafter until the termination of the dual-hat arrangement, the Secretary of Defense, in coordination with the Director of National Intelligence, shall submit to the appropriate committees of Congress a report containing either of the following:

"(1) A certification that the United States Cyber Command has met each of the following conditions:

"(A) Sufficient operational infrastructure has been deployed to meet the unique cyber mission needs of the United States Cyber Command.

"(B) Sufficient command and control systems and processes have been established for planning, deconflicting, and executing military cyber operations.

"(C) Capabilities have been established to enable intelligence collection and operational preparation of the environment for cyber operations consistent with the United States Cyber Command reaching full operational status.

"(D) Mechanisms have been established to train cyber operations personnel, test cyber capabilities, and rehearse cyber missions.

"(E) The United States Cyber Command has achieved full operational capability.

"(2) If the Secretary, in coordination with the Director, is not able to make the certification under paragraph (1)—

"(A) an identification of the items contained in the defense budget materials that are related to meeting the conditions specified in such paragraph; and

"(B) an assessment of the funding required to meet such conditions during the period covered by the future-years defense program under section 221 of title 10, United States Code.";

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

(3) in subsection (c), as so redesignated, by adding at the end the following new paragraph:

"(3) DEFENSE BUDGET MATERIALS.—The term 'defense budget materials' has the meaning given that term in section 231(f) of title 10, United States Code.".

**SEC. 414. NATIONAL SPACE INTELLIGENCE CENTER.**

(a) FINDINGS.—Congress finds the following:

(1) Section 9081 of title 10, United States Code, establishes the United States Space Force as an Armed Force within the Department of the Air Force to, as stated in subsection (c) of such section—

(A) provide freedom of operation for the United States in, from, and to space;

(B) conduct space operations; and

(C) protect the interests of the United States in space.

(2) The National Air and Space Intelligence Center, headquartered at Wright-Patterson Air Force Base, Ohio, is the primary source for foreign air and space threat analysis within the intelligence enterprise of the Air Force.

(3) Section 8041 of the Department of Defense Appropriations Act, 2020 (division A of Public Law 116–93; 133 Stat. 2345) prohibits the establishment of a new field operating agency using funds made available under that Act, although the Secretary of Defense or the Secretary of a military department may waive the prohibition in cases where the relevant Secretary determines that the establishment will reduce the personnel or financial requirements of the relevant department.

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

(1) space has become increasingly contested, congested, and competitive, mandating an expanded need for space intelligence;

(2) to support this increasingly complex operational environment, the Space Force should have its own intelligence organization dedicated to providing the Joint Combat forces with the required intelligence and analysis to support operations;

(3) a prominent factor in the basing decision should consider that co-locating the National Space Intelligence Center with the National Air and Space Intelligence Center at Wright-Patterson Air Force Base will provide an operational and geographic synergy, which will greatly benefit combat operations across the air and space operational environments;

(4) the Air Force has requested authority to establish the National Space Intelligence Center as a field operating agency to ensure the appropriate prioritization of analytic effort for the space domain, enhance responsiveness to national-level customers, and align command relationships with the Director of Intelligence, Surveillance, and Reconnaissance of the Space Force; and

(5) establishing the National Space Intelligence Center as a field operating agency would be a resource-neutral administrative realignment of billets, and would facilitate a lean and agile space intelligence enterprise.

(c) EXCEPTION.—Notwithstanding section 8041 of the Department of Defense Appropriations Act, 2020 (division A of Public Law 116–93; 133 Stat. 2345), or any other provision of law prohibiting the establishment of a field operating agency, the Secretary of the Air Force may establish the National Space Intelligence Center as a field operating agency of the Space Force to perform the analysis and production of scientific and technical intelligence on foreign space and counter-space threat capabilities in the support of the Space Force.

**SEC. 415. PROCUREMENT BY FEDERAL BUREAU OF INVESTIGATION OF CHINESE PRODUCTS AND SERVICES.**

(a) SECURITY ASSESSMENT.—The Director of the Federal Bureau of Investigation may not procure a Chinese product or service unless, before such procurement, the Counterintelligence Division of the Federal Bureau of Investigation—

(1) conducts a security assessment of such product or service, including with respect to any physical or cyber vulnerabilities; and

(2) makes a recommendation to the Director regarding such proposed procurement.

(b) SUBMISSION.—Not later than 30 days after the date on which the Counterintelligence Division of the Bureau conducts a security assessment under subsection (a), the Director shall submit to the congressional intelligence committees a copy of such assessment and the recommendation under paragraph (2) of such subsection.

(c) CHINESE PRODUCT OR SERVICE DEFINED.—In this section, the term "Chinese product or service" means a product or service provided by an entity that is owned or controlled by, or otherwise connected to, the government of China.

**SEC. 416. COUNTERINTELLIGENCE UNITS AT NON-INTELLIGENCE COMMUNITY FEDERAL DEPARTMENTS AND AGENCIES.**

(a) ESTABLISHMENT.—The Director of the Federal Bureau of Investigation shall establish counterintelligence units in the departments and agencies described in subsection (b). Such units shall be composed of officers of the Counterintelligence Division of the Federal Bureau of Investigation.

(b) DEPARTMENTS AND AGENCIES DESCRIBED.—The departments and agencies described in this subsection are the following departments and agencies of the United States Government:

(1) The Department of Agriculture.

(2) Any other department or agency that the Director, in coordination with the Director of National Intelligence, determines appropriate.

(c) DUTIES.—The Director of the Federal Bureau of Investigation shall ensure that each counterintelligence unit established under subsection (a) in a department or agency described in subsection (b) carries out the following duties:

(1) Conducts assessments, in coordination with the leadership of the department or agency, to determine the counterintelligence posture of the department or agency, including any components thereof.

(2) Informs and consults with the leadership of the department or agency, including any components thereof, and provides recommendations with respect to any counterintelligence threats identified by the intelligence community.

(3) Provides such administrative and technical support as is necessary to develop, in coordination with the leadership of the department or agency, a plan to eliminate or reduce the threats described in paragraph (2).

(4) Serves as the primary point of contact for the department or agency with respect to counterintelligence for the intelligence community.

(d) INTELLIGENCE COMMUNITY SUPPORT.—The heads of the elements of the intelligence community shall ensure that relevant counterintelligence information is provided to counterintelligence units established under subsection (a) in a manner that is consistent with the need to protect sources and methods.

**SEC. 417. DETECTION AND MONITORING OF WILDFIRES.**

(a) SENSE OF CONGRESS.—It is the sense of Congress that the Director of the National Geospatial-Intelligence Agency, in accordance with relevant provisions of law, should continue to manage the systems of the National Geospatial-Intelligence Agency that enable the FireGuard program of the Department of Defense.

(b) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Director of the National Geospatial-Intelligence Agency, in consultation with the Secretary of Defense and the heads of the departments and agencies of the United States Government and other organizations that constitute the National Interagency Fire Center, and any other relevant organization the Director determines appropriate, shall submit to the appropriate congressional committees a coordinated interagency report that—

(1) explains how to leverage existing resources to improve processes and organization alignment;

(2) identifies future opportunities to improve the ability to detect and track wildfires and support firefighting efforts; and

(3) includes an explication of the relevant authorities with respect to the matters under paragraphs (1) and (2).

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term "appropriate congressional committees" means—

(1) the congressional intelligence committees; and

(2) the congressional defense committees (as defined in section 101(a)(16) of title 10, United States Code).

# TITLE V—ANOMALOUS HEALTH INCIDENTS AND OTHER HEALTH CARE MATTERS

**SEC. 501. COMPENSATION AND PROFESSIONAL STANDARDS FOR CERTAIN MEDICAL OFFICERS OF CENTRAL INTELLIGENCE AGENCY.**

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

**"SEC. 26. COMPENSATION AND PROFESSIONAL STANDARDS FOR CERTAIN MEDICAL OFFICERS.**

"(a) OFFICE OF MEDICAL SERVICES.—There is in the Agency an Office of Medical Services.

"(b) COMPENSATION.—Beginning not later than 1 year after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, each medical officer of the Office of Medical Services who meets the qualifications under subsection (c) shall be compensated during a pay period pursuant to a pay range that is equal to the pay range published in the Federal Register pursuant to section 7431(e)(1)(C) of title 38, United States Code (for the corresponding pay period), for a physician in the Veterans Health Administration in the District of Columbia region with a medical subspecialty that is the equivalent of the medical subspecialty of the officer.

"(c) CLINICAL PRACTICE QUALIFICATIONS.—A medical officer meets the qualifications under this subsection if the officer provides direct care services to patients in connection with the official duties of the officer and—

"(1) maintains current, active, full, and unrestricted licensure or registration as a physician from a State, the District of Columbia, or a commonwealth or territory of the United States;

"(2) holds active board certification and maintains accreditation in an American Board of Medical Specialties direct care clinical specialty; and

"(3) except as provided in subsection (d), maintains a minimum of 160 hours per year of clinical practice in an accredited clinic or hospital facility that is not affiliated with the Central Intelligence Agency.

"(d) EXCEPTION FOR OVERSEAS SERVICE.—If a medical officer is a medical officer located in a duty station outside of the United States pursuant to a permanent change of station and greater than 50 percent of the official duties of the officer in such duty station involve direct patient care, the officer, in lieu of performing the minimum hours under subsection (c)(3) on an annual basis, may perform up to 480 hours of clinical practice as specified in such subsection prior to such change of station, to fulfil in advance the requirement under such subsection for up to 3 years.

"(e) CLINICAL PRACTICE HOURS.—The head of the Office of Medical Services shall make available to medical officers excused absence time to allow for the maintenance of clinical practice hours in accordance with subsection (c)(3).".

**SEC. 502. MEDICAL ADVISORY BOARD OF CENTRAL INTELLIGENCE AGENCY.**

(a) ESTABLISHMENT.—The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.), as amended by section 501, is further amended by adding at the end the following new section:

**"SEC. 27. MEDICAL ADVISORY BOARD.**

"(a) ESTABLISHMENT.—The Director shall establish within the Agency a medical advisory board (in this section referred to as the 'Board').

"(b) DUTIES.—The Board shall—

"(1) conduct a study on the Office of Medical Services of the Agency, and submit reports regarding such study, in accordance with subsection (c); and

"(2) upon request, provide advice and guidance in connection with any independent review of the Office conducted by an inspector general.

"(c) STUDY.—

"(1) OBJECTIVES.—In conducting the study under subsection (b)(1), the Board shall seek to—

"(A) contribute to the modernization and reform of the Office of Medical Services;

"(B) ensure that the activities of the Office are of the highest professional quality; and

"(C) ensure that all medical care provided by the Office is provided in accordance with the highest professional medical standards.

"(2) REPORTS.—The Board shall submit to the congressional intelligence committees, in writing—

"(A) interim reports on the study; and

"(B) a final report on the study, which shall—

"(i) set forth in detail the findings of the study and the recommendations of the Board, based on such findings and taking into consideration the objectives under paragraph (1), regarding any changes to the activities of the Office of Medical Services; and

"(ii) include, as applicable, any additional or dissenting views submitted by a member of the Board.

"(d) MEMBERSHIP.—

"(1) NUMBER AND APPOINTMENT.—The Board shall be composed of 11 members, appointed as follows:

"(A) 2 members appointed by the Chairman of the Permanent Select Committee on Intelligence of the House of Representatives.

"(B) 2 members appointed by the ranking minority member of the Permanent Select Committee on Intelligence of the House of Representatives.

"(C) 2 members appointed by the Chairman of the Select Committee on Intelligence of the Senate.

"(D) 2 members appointed by the Vice Chairman of the Select Committee on Intelligence of the Senate.

"(E) 3 members appointed by the Director of National Intelligence.

"(2) CHAIRPERSON.—During the first meeting under subsection (e)(1), the members of the Board shall elect a Chairperson of the Board. In addition to meeting the criteria under paragraph (3), the Chairperson may not be an employee, or former employee, of the Agency.

"(3) CRITERIA.—The members appointed under paragraph (1) shall meet the following criteria:

"(A) Each member shall be a recognized expert in at least 1 medical field, as demonstrated by appropriate credentials.

"(B) Each member shall possess significant and diverse medical experience, including clinical experience.

"(C) Each member shall hold a security clearance at the top secret level and be able to access sensitive compartmented information.

"(4) TERMS.—

"(A) IN GENERAL.—Each member, including the Chairperson, shall be appointed or elected, as applicable, for the life of the Board.

"(B) VACANCIES.—Any vacancy in the Board occurring prior to the expiration of the term under subparagraph (A) shall be filled in the manner in which the original appointment or election was made.

"(5) COMPENSATION AND TRAVEL EXPENSES.—

"(A) COMPENSATION.—Except as provided in subparagraph (B), each member of the Board, including the Chairperson, may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties under subsection (b).

"(B) EXCEPTION FOR FEDERAL EMPLOYEES.—Members of the Board, including the Chairperson, who are officers or employees of the United States shall receive no additional pay by reason of the service of the member on the Board.

"(C) TRAVEL EXPENSES.—Each member of the Board, including the Chairperson, while away from the home or regular places of business of the member in the performance of services for the Board, may be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703 of title 5, United States Code.

"(6) DETAILEES.—

"(A) IN GENERAL.—Upon request of the Board, the Director of National Intelligence may detail to the Board, without reimbursement from the Board, any of the personnel of the Office of the Director of National Intelligence to assist in carrying out the duties under subsection (b). Any such detailed personnel shall retain the rights, status, and privileges of the regular employment of the personnel without interruption.

"(B) CLEARANCE.—Any personnel detailed to the Board under subparagraph (A) shall possess a security clearance in accordance with applicable laws and regulations concerning the handling of classified information.

"(e) MEETINGS.—

"(1) BOARD MEETINGS.—The Board shall meet not less frequently than on a quarterly basis.

"(2) MEETINGS WITH CONGRESS.—The Board shall meet with the congressional intelligence committees on a biannual basis.

"(f) INFORMATION ACCESS.—

"(1) IN GENERAL.—Except as provided in paragraph (2), the Board may secure directly from any department or agency of the United States Government information necessary to enable it to carry out the duties under subsection (b) and, upon request of the Chairperson of the Board, the head of that department or agency shall furnish such information to the Board.

"(2) EXCEPTION.—The Director (without delegation) may deny a request for information made by the Board pursuant to paragraph (1), regardless of the agency from which such information is requested.

"(3) NOTIFICATION REQUIREMENT.—If the Director denies a request under paragraph (2), not later than 15 days after the date of such denial, the Director shall submit to the congressional intelligence committees a written notification of such denial.

"(4) BRIEFINGS.—The Director shall ensure that the Board receives comprehensive briefings on all activities of the Office of Medical Services, including by promptly scheduling such briefings at the request of the Board.

"(g) TERMINATION.—The Board shall terminate on the date that is 5 years after the date of the first meeting of the Board.

"(h) DEFINITIONS.—In this section, the terms 'congressional intelligence committees' and 'intelligence community' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).".

(b) DEADLINE FOR APPOINTMENTS; FIRST MEETINGS.—

(1) DEADLINE FOR APPOINTMENTS.—Each member of the medical advisory board established under section 27 of the Central Intelligence Agency Act of 1949 (as added by subsection (a)), including the Chairperson, shall be appointed or elected, as applicable, in accordance with subsection (d) of such section by not later than 45 days after the date of the enactment of this Act.

(2) FIRST BOARD MEETING.—Not later than 30 days after the first date on which at least 7 members of the Board described in paragraph (1) hold the security clearance and are able to access information in accordance with subsection (d)(3)(C) of such section 27, the Board shall meet. During such meeting, the Di-

rector of the Central Intelligence Agency shall provide to the Board a comprehensive briefing on all aspects of the Office of Medical Services of the Central Intelligence Agency.

(3) FIRST MEETING WITH CONGRESS.—Not later than 30 days after the date of the briefing under paragraph (2), the Board described in such paragraph shall meet with the staff members of the congressional intelligence committees to discuss topics for the Board to examine in carrying out the duties under subsection (b) of such section 27.

**SEC. 503. REPORT ON PROTOCOLS FOR CERTAIN INTELLIGENCE COMMUNITY EMPLOYEES AND DEPENDENTS.**

(a) IN GENERAL.—Beginning not later than 180 days after the date of enactment of this Act, the President shall develop, for uniform implementation across the elements of the intelligence community, each of the protocols described in subsections (c) through (f). Such protocols shall be subject to review and revision on a periodic basis, and any implementation of such protocols shall be conducted in accordance with applicable laws and current clinical and professional practices of the interagency medical community.

(b) PRIVACY.—No data collected pursuant to any protocol under this section may be used for research or analytical purposes without the written consent of the individual from whom such data was collected with respect to such use.

(c) PROTOCOL ON BASELINE MEDICAL TESTING.—The protocol described in this subsection is a protocol for conducting baseline medical testing of covered employees, covered individuals, and the dependents of covered employees who are included on the overseas travel orders of the covered employee, with respect to anomalous health incidents. Such protocol shall set forth the required elements of such baseline medical testing, such as—

(1) standard lab collection and testing of relevant biofluids;

(2) the conduct of relevant visual and auditory examinations;

(3) the conduct of Acquired Brain Injury Tool assessments, or other relevant assessments for balance, eye motion, and cognition;

(4) the assessment of relevant medical histories; and

(5) the conduct of any other standard relevant medical or neurological examinations, testing, or assessments.

(d) PROTOCOLS ON POST-INCIDENT MEDICAL TESTING.—The protocols described in this subsection are protocols to enable voluntary medical testing and the coordination of treatment for covered employees, covered individuals, and the dependents of covered employees, following a reported anomalous health incident, such as—

(1) a protocol that sets forth elements, similar to the elements described in subsection (c), of such testing;

(2) a protocol pertaining to the voluntary testing and treatment for victims of anomalous health incidents who are children;

(3) a protocol for ensuring that all victims of anomalous health incidents receive access to prompt and consistent medical treatment, including from medical professionals holding appropriate security clearances and medical professionals with expertise in child care;

(4) a protocol for ensuring that all victims of anomalous health incidents are offered options for psychological treatment for the effects of such incidents; and

(5) a protocol for ensuring that any testing, evaluation, or collection of biofluids or other samples following a reported anomalous health incident may be compared against the baseline for the victim of the anomalous health incident, to the extent the individual participated in the baseline medical testing, consistent with subsections (b) and (c).

(e) PROTOCOL ON INFORMATION COLLECTION, STORAGE, AND SAFEGUARDING.—The protocol described in this subsection is a protocol for the collection, storage, and safeguarding of information acquired as a result of the protocols described in subsections (c) and (d).

(f) PROTOCOL ON REPORTING MECHANISMS.—The protocol described in this subsection is a protocol for the reporting of matters relating to anomalous health incidents by covered employees, covered individuals, and the dependents of covered employees, including the development of a system for the adjudication of complaints regarding medical treatment received by such covered employees, covered individuals, and dependents of covered employees.

(g) REPORT AND BRIEFINGS.—

(1) 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 a report on the protocols described in subsections (c) through (f).

(2) ELEMENTS.—Such report shall include the following elements:

(A) A copy of each protocol under this section.

(B) A description of the following:

(i) Any interagency agreements, authorities, or policies required to effectively implement the protocols under this section.

(ii) Any new facilities, medical equipment, tools, training, or other resources required to effectively implement such protocols.

(C) A timeline for the implementation of the protocols under this section, including a proposal for the prioritization of implementation with respect to various categories of covered employees and the dependents of covered employees.

(3) BRIEFING.—Not later than 60 days following the date of submission of the report under paragraph (1), and biannually thereafter, the Director shall provide to the congressional intelligence committees a briefing regarding the implementation of the protocols under this section.

(h) DEFINITIONS.—In this section:

(1) COVERED EMPLOYEE.—The term "covered employee" means an individual who is an employee, assignee, or detailee of an element of the intelligence community.

(2) COVERED INDIVIDUAL.—The term "covered individual" means a contractor to an element of the intelligence community.

(3) DEPENDENT OF A COVERED EMPLOYEE.—The term "dependent of a covered employee" means, with respect to a covered employee, a family member (including a child), as defined by the Director of National Intelligence.

(4) VICTIM OF AN ANOMALOUS HEALTH INCIDENT.—The term "victim of an anomalous health incident" means a covered employee, covered individual, or dependent of a covered employee, who is, or is suspected to have been, affected by an anomalous health incident.

**SEC. 504. INSPECTOR GENERAL OF CENTRAL INTELLIGENCE AGENCY REVIEW OF OFFICE OF MEDICAL SERVICES.**

(a) REVIEW.—Not later than one year after the date of the enactment of this Act, the Inspector General of the Central Intelligence Agency, in coordination with, and with the support of, the Inspector General of the Intelligence Community, shall submit to the congressional intelligence committees a report containing a review of the responsibilities, authorities, resources, and performance of the Office of Medical Services of the Central Intelligence Agency (in this section referred to as the "Office").

(b) MATTERS INCLUDED.—The review under subsection (a) shall include the following:

(1) A detailed description of the responsibilities and authorities of the Office, as set forth in Federal law and any applicable regulation, policy, or other document of the Central Intelligence Agency.

(2) A detailed description of the budgetary, human, and other resources available to the Office, including with respect to employees and any other personnel.

(3) An assessment of the ability of the Office to consistently discharge the responsibilities of the Office, with an emphasis on the provision of medical treatment and care by personnel of the Office, including with respect to—

(A) the roles of personnel of the Office, and of senior officials of the Agency outside of the Office, in determining what medical evaluation, treatment, and care should be provided in a particular case, including the provision of specialty care by medical personnel outside of the Office;

(B) whether personnel of the Office consistently provide appropriate and high-quality medical treatment and care in accordance with standards set independently by the professional medical community;

(C) whether the Office has sufficient human and other resources, including personnel with specialized background, qualifications, or expertise, to consistently provide high-quality medical treatment and care in accordance with standards set independently by the professional medical community;

(D) whether personnel of the Office, including personnel claiming specialized medical backgrounds and expertise, are required by the Agency to maintain current board certifications or other certifications and licenses, and the extent to which the Office verifies such certifications and licenses;

(E) the extent to which the Office makes consistent and effective use of the specialized medical background, qualifications, and expertise of the personnel of the Office in providing medical treatment and care;

(F) an assessment of whether personnel of the Office who provide medical treatment and care, or who make decisions with respect to such treatment or care, are required to have extensive clinical or other experience in directly treating patients, including in areas requiring specialized background, qualifications, or expertise;

(G) any factors that have frustrated or delayed the provision of medical treatment and care by personnel of the Office in significant cases; and

(H) any factors that have frustrated or could frustrate prompt detection, effective oversight, and swift remediation of problems within the Office, including such factors that frustrate or delay the provision of medical treatment and care in significant cases.

(c) INDEPENDENT ADVICE.—In conducting the review under subsection (a), the Inspector General may obtain the advice of the medical advisory board established under section 502.

(d) FORM.—The report under subsection (a) shall be submitted in an unclassified form to the extent practicable, consistent with the protection of intelligence sources and methods, but may include a classified annex.

**SEC. 505. CLARIFICATION OF EFFECT OF CERTAIN BENEFITS RELATING TO INJURIES TO THE BRAIN.**

(a) PERSONNEL OF CENTRAL INTELLIGENCE AGENCY.—Subsection (d) of section 19A of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b), as added by the HAVANA Act of 2021, is amended by adding at the end the following new paragraph:

"(5) NO EFFECT ON OTHER BENEFITS.—Payments made under paragraph (2) are supplemental to any other benefit furnished by the United States Government for which a covered dependent, covered employee, or covered individual is entitled, and the receipt of such payments may not affect the eligibility of such a person to any other benefit furnished by the United States Government.".

(b) PERSONNEL OF DEPARTMENT OF STATE.—Subsection (i) of section 901 of title IX of division J of the Further Consolidated Appropriations Act, 2020 (22 U.S.C. 2680b), as added by the HAVANA Act of 2021, is amended by adding at the end the following new paragraph:

"(5) NO EFFECT ON OTHER BENEFITS.—Payments made under paragraph (2) are supplemental to any other benefit furnished by the United States Government for which a covered dependent, dependent of a former employee, covered employee, former employee, or covered individual is entitled, and the receipt of such payments may not affect the eligibility of such a person to any other benefit furnished by the United States Government.".

# TITLE VI—MATTERS RELATING TO FOREIGN COUNTRIES

**SEC. 601. NATIONAL INTELLIGENCE ESTIMATE ON SECURITY SITUATION IN AFGHANISTAN AND RELATED REGION.**

(a) REQUIREMENT.—The Director of National Intelligence, acting through the National Intelligence Council, shall produce a National Intelligence Estimate on the situation in Afghanistan and the covered region.

(b) MATTERS.—The National Intelligence Estimate produced under subsection (a) shall include, with respect to the 2-year period beginning on the date on which the Estimate is produced, an assessment of the following:

(1) The presence in Afghanistan (including financial contributions to the Taliban, political relations with the Taliban, military presence in the covered region, economic presence in the covered region, and diplomatic presence in the covered region) of China, Iran, Pakistan, Russia, and any other foreign country determined relevant by the Director, respectively, and an assessment of the potential risks, or benefits, of any such presence, contributions, or relations.

(2) Any change in the threat to the United States homeland or United States entities abroad as a result of the withdrawal of the Armed Forces from Afghanistan on August 31, 2021, including an assessment of the risk of al-Qaeda or any affiliates thereof, the Islamic State of Iraq and ash Sham-Khorasan or any affiliates thereof, or any other similar international terrorist group, using Afghanistan as a safe haven for launching attacks on the United States and its interests abroad.

(3) The political composition and sustainability of the governing body of Afghanistan, including an assessment of the ability of the United States Government to influence the policies of such governing body on the following:

(A) Counterterrorism.

(B) Counternarcotics.

(C) Human rights (particularly regarding women and girls and traditionally targeted ethnic groups).

(D) The treatment and safe transit of Afghans holding special immigrant visa status under section 602 of the Afghan Allies Protection Act of 2009 (8 U.S.C. 1101 note) and other Afghans who, during the period beginning in 2001, assisted efforts of the United States in Afghanistan or the covered region.

(4) The effect on the covered region, and Europe, of refugees leaving Afghanistan.

(5) The commitments of the Taliban relating to counterterrorism, including an assessment of—

(A) whether such commitments required under the agreement entered into between the United States Government and the Taliban in February 2020, have been tested, or will be tested during the 2-year period covered by the Estimate, and what such commitments entail;

(B) whether any additional commitments relating to counterterrorism agreed to by the Taliban pursuant to subsequent negotiations with the United States Government following February 2020, have been tested, or will be tested during the 2-year period covered by the Estimate, and, if applicable, what such commitments entail;

(C) any benchmarks against which the Taliban are to be evaluated with respect to commitments relating to counterterrorism; and

(D) the intentions and capabilities of the Taliban with respect to counterterrorism (as such term is understood by the United States and by the Taliban, respectively), including the relations of the Taliban with al-Qaeda or any affiliates thereof, the Islamic State of Iraq and ash Sham-Khorasan or any affiliates thereof, or any other similar international terrorist group.

(c) SUBMISSION TO CONGRESS.—

(1) SUBMISSION.—Not later than one year after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees the National Intelligence Estimate produced under subsection (a), including all intelligence reporting underlying the Estimate.

(2) FORM.—The National Intelligence Estimate shall be submitted under paragraph (1) in classified form.

(d) PUBLIC VERSION.—Consistent with the protection of intelligence sources and methods, at the same time as the Director submits to the congressional intelligence committees the National Intelligence Estimate under subsection (c), the Director shall make publicly available on the internet website of the Director an unclassified version of the key findings of the National Intelligence Estimate.

(e) DEFINITIONS.—In this section:

(1) COVERED REGION.—The term "covered region" includes the following countries:

(A) China.

(B) The Gulf Cooperation Council countries, including Qatar, Saudi Arabia, the United Arab Emirates.

(C) India.

(D) Iran.

(E) Pakistan.

(F) Tajikistan.

(G) Turkey.

(H) Turkmenistan.

(I) Uzbekistan.

(2) UNITED STATES ENTITY.—The term "United States entity" means a citizen of the United States, an embassy or consulate of the United States, or an installation, facility, or personnel of the United States Government.

**SEC. 602. REPORT ON LIKELIHOOD OF MILITARY ACTION BY COUNTRIES OF THE SOUTH CAUCASUS.**

(a) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report assessing the likelihood of a South Caucasus country taking military action against another country (including in Nagorno-Karabakh or any other disputed territory). Such report shall include an indication of the strategic balance in the region, including with respect to the offensive military capabilities of each South Caucasus country.

(b) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(c) SOUTH CAUCASUS COUNTRY DEFINED.—In this section, the term "South Caucasus country" means any of the following:

(1) Armenia.

(2) Azerbaijan.

(3) Georgia.

**SEC. 603. REPORT ON INTELLIGENCE COLLECTION POSTURE AND OTHER MATTERS RELATING TO AFGHANISTAN AND RELATED REGION.**

(a) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of elements of the intelligence community determined relevant by the Director, shall submit to the congressional intelligence committees a report on the collection posture of the intelligence community and other matters relating to Afghanistan and the covered region.

(b) MATTERS.—The report under subsection (a) shall include the following:

(1) A detailed description of the collection posture of the intelligence community with respect to Afghanistan, including with respect to the following:

(A) The countering of terrorism threats that are directed at the United States homeland or United States entities abroad.

(B) The finances of the Taliban, including financial contributions to the Taliban from foreign countries (particularly from China, Iran, Russia, and any other foreign country in the Arab Gulf region (or elsewhere) determined relevant by the Director, respectively).

(C) The detection, and prevention of, any increased threat to the United States homeland or United States entities abroad as a result of the withdrawal of the United States Armed Forces from Afghanistan on August 31, 2021, including any such increased threat resulting from al-Qaeda or any affiliates thereof, the Islamic State of Iraq and ash Sham-Khorasan or any affiliates thereof, or any other similar international terrorist group, using Afghanistan as a safe harbor.

(2) A detailed description of any plans, strategies, or efforts to improve the collection posture described in paragraph (1)(A), including by filling any gaps identified pursuant to such paragraph.

(3) An assessment of the effect of publicly documenting abuses engaged in by the Taliban, and a description of the efforts of the intelligence community to support other departments and agencies in the Federal Government with respect to the collection and documentation of such abuses.

(4) An assessment of the relationship between the intelligence community and countries in the covered region, including an assessment of the following:

(A) Intelligence and information sharing with such countries.

(B) Any change in the collection posture of the intelligence community with respect to the nuclear activities of such countries as a result of the withdrawal of the United States Armed Forces from Afghanistan on August 31, 2021.

(C) The collection posture of the intelligence community with respect to the presence of such countries in Afghanistan (including financial contributions to the Taliban, political relations with the Taliban, military presence in Afghanistan, economic presence in Afghanistan, and diplomatic presence in Afghanistan) and the understanding of the intelligence community regarding the potential risks, or benefits, of any such presence, contributions, or relations.

(D) The ability of the intelligence community to use the airspace of any such countries.

(5) An assessment of any financial contributions to the Taliban from foreign countries (particularly from China, Iran, Russia, and any other foreign country in the Arab Gulf region (or elsewhere) determined relevant by the Director, respectively) made during the year preceding the withdrawal of the United States Armed Forces from Afghanistan on August 31, 2021.

(c) FORM.—The report under subsection (a) may be submitted in classified form, but shall include an unclassified summary.

(d) BIANNUAL UPDATES.—On a biannual basis during the 5-year period following the date of the submission of the report under subsection (a), the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community determined relevant by the Director, shall submit to the congressional intelligence committees an update to such report.

(e) DEFINITIONS.—In this section:

(1) COVERED REGION.—The term "covered region" includes the following countries:

(A) China.

(B) The Gulf Cooperation Council countries, including Qatar, Saudi Arabia, the United Arab Emirates.

(C) India.

(D) Iran.

(E) Pakistan.

(F) Tajikistan.

(G) Turkey.
(H) Turkmenistan.
(I) Uzbekistan.

(2) UNITED STATES ENTITY.—The term "United States entity" means a citizen of the United States, an embassy or consulate of the United States, or an installation, facility, or personnel of the United States Government.

**SEC. 604. REPORT ON THREAT POSED BY EMERGING CHINESE TECHNOLOGY COMPANIES.**

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Assistant Secretary of the Treasury for Intelligence and Analysis and the Director of the Federal Bureau of Investigation, shall submit to the congressional intelligence committees a report on the threat to the national security of the United States posed by emerging Chinese technology companies.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment of the threat to the national security of the United States posed by emerging Chinese technology companies, including with respect to—

(A) the practices of the companies and their relationships to the government of China;

(B) the security of the communications, data, and commercial interests of the United States; and

(C) the privacy interests of United States persons.

(2) An assessment of the ability of the United States to counter any such threat, including with respect to different tools that could counter such a threat.

(c) FORM.—The report under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

(d) EMERGING CHINESE TECHNOLOGY COMPANIES DEFINED.—In this section, the term "emerging Chinese technology companies" means a Chinese technology company, including a company listed on the Science and Technology Innovation Board of the Shanghai Stock Exchange, that the Assistant Secretary of the Treasury for Intelligence and Analysis determines poses a significant threat to the national security of the United States.

**SEC. 605. REPORT ON COOPERATION BETWEEN CHINA AND UNITED ARAB EMIRATES.**

(a) REQUIREMENT.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of elements of the intelligence community that the Director determines appropriate, shall submit to the congressional intelligence committees a report containing the following:

(1) Details on the cooperation between China and the United Arab Emirates regarding defense, security, technology, and other strategically sensitive matters that implicate the national security interests of the United States.

(2) The most recent, as of the date of the report, quarterly assessment by the intelligence community of measures that the United Arab Emirates has implemented to safeguard technology of the United States and the reliability of any assurances by the United Arab Emirates (with respect to both current assurances and assurances being considered as of the date of the report).

(3) A certification by the Director regarding whether such assurances described in paragraph (2) are viable and sufficient to protect technology of the United States from being transferred to China or other third parties.

(b) FORM.—The report under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

**SEC. 606. REPORT ON PROPAGATION OF EXTREMIST IDEOLOGIES FROM SAUDI ARABIA.**

(a) REPORT.—Not later than February 1, 2022, the Director of National Intelligence, in consultation with other relevant Federal departments and agencies, shall submit to the congressional intelligence committees a report on the threat of extremist ideologies propagated from Saudi Arabia and the failure of the Government of Saudi Arabia to prevent the propagation of such ideologies. Such report shall include a detailed description of—

(1) the role of governmental and nongovernmental entities and individuals of Saudi Arabia in promoting, funding, and exporting ideologies, including so-called "Wahhabist ideology", that inspire extremism or extremist groups in other countries; and

(2) the practical and strategic consequences for vital national security interests of the United States as a result of such promotion, funding, or export.

(b) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

**SEC. 607. REPORT ON EFFECTS OF SANCTIONS BY UNITED STATES.**

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Assistant Secretary of the Treasury for Intelligence and Analysis, shall submit to the congressional intelligence committees a report on how covered countries respond to sanctions imposed by the United States.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment of whether sanctions imposed by the United States on entities, individuals, or the governments of covered countries have caused those countries to alter their behavior.

(2) An assessment of the effectiveness of—

(A) continuing such sanctions; and

(B) imposing additional sanctions.

(c) FORM.—The report under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

(d) COVERED COUNTRY DEFINED.—In this section, the term "covered country" means—

(1) China;

(2) Iran;

(3) Russia; and

(4) any other foreign country the Assistant Secretary of the Treasury for Intelligence and Analysis determines appropriate.

# TITLE VII—REPORTS AND OTHER MATTERS

**SEC. 701. PILOT PROGRAM FOR SECURITY VETTING OF CERTAIN INDIVIDUALS.**

(a) ESTABLISHMENT.—The Under Secretary of Defense for Intelligence and Security may establish a pilot program to identify risks associated with individuals who are performing unclassified research funded by the Department of Defense who would not otherwise undergo Federal personnel vetting.

(b) ELEMENTS.—In carrying out the pilot program under this section, the Under Secretary of Defense for Intelligence and Security may—

(1) identify the size of the population to be vetted under the pilot program;

(2) establish a process to obtain information from individuals to be vetted under the pilot program;

(3) determine the criteria to evaluate national security risks to research funded by the Department of Defense from individuals who are participating in such research;

(4) establish a process to conduct vetting, including referrals to appropriate counterintelligence and law enforcement entities, for the population to be screened under the pilot program; and

(5) carry out the process described in paragraph (4) with respect to the population to be screened under the pilot program.

(c) REPORT.—Before commencing the pilot program under this section, the Under Secretary of Defense for Intelligence and Security shall submit to the appropriate congressional committees a report containing details of the planned elements of the pilot program under subsection (b).

(d) BRIEFINGS.—Not less frequently than annually during the 3-year period beginning on the date that is 1 year after the date of the enactment of this Act, the Under Secretary of Defense for Intelligence and Security shall provide to the appropriate congressional committees a briefing on the status of the pilot program under this section.

(e) TERMINATION.—The authority to conduct the pilot program under this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(f) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term "appropriate congressional committees" means—

(1) the congressional intelligence committees; and

(2) the congressional defense committees (as such term is defined in section 101(a) of title 10, United States Code).

**SEC. 702. INTELLIGENCE ASSESSMENT AND REPORTS ON FOREIGN RACIALLY MOTIVATED VIOLENT EXTREMISTS.**

(a) INTELLIGENCE ASSESSMENT.—

(1) REQUIREMENT.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence, acting through the Director of the National Counterterrorism Center, in coordination with the Director of the

Federal Bureau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis, and in consultation with other relevant Federal departments and agencies, shall submit to the appropriate congressional committees an intelligence assessment on significant threats to the United States associated with foreign racially motivated violent extremist organizations.

(2) ELEMENTS.—The assessment under paragraph (1) shall include the following:

(A) A list of foreign racially motivated violent extremist organizations that pose a significant threat to the national security of the United States.

(B) With respect to each such organization—

(i) an overview of the membership, ideology, and activities;

(ii) a description of any transnational links to the United States or United States persons;

(iii) a description of the leadership, plans, intentions, and capabilities;

(iv) whether (and if so, to what extent) foreign governments or their proxies provide any manner of support to such organizations, including a list of each such foreign government or proxy;

(v) a description of the composition and characteristics of the members and support networks, including whether (and if so, to what extent) the members are also a part of a military, security service, or police;

(vi) a description of financing and other forms of material support;

(vii) an assessment of trends and patterns relative to communications, travel, and training (including whether and to what extent the organization is engaged in or facilitating military or paramilitary training);

(viii) an assessment of the radicalization and recruitment, including an analysis of the extremist messaging motivating members and supporters; and

(ix) whether (and if so, to what extent) foreign governments have sufficient laws and policies to counter threats to the United States associated with the organization, including best practices and gaps.

(C) An assessment of the status and extent of information sharing, intelligence partnerships, foreign police cooperation, and mutual legal assistance between the United States and foreign governments relative to countering threats to the United States associated with foreign racially motivated violent extremist organizations.

(D) An assessment of intelligence gaps and recommendations on how to remedy such gaps.

(E) An opportunity analysis regarding countering such threats, including, at a minimum, with respect to mitigating and disrupting the transnational nexus.

(3) STANDARDS.—The intelligence assessment under paragraph (1) shall be conducted in a manner that meets the analytic integrity and tradecraft standards of the intelligence community.

(4) FORM.—The intelligence assessment under paragraph (1) shall be submitted in unclassified form, but may include a classified annex in electronic form that is fully indexed and searchable. In carrying out this paragraph, the officials specified in paragraph (1) shall—

(A) ensure that the assessment is unclassified to the extent possible; and

(B) ensure that the assessment is drafted in a way to maximize the ability to share the assessment, including the classified annex, with the entities under paragraph (5).

(5) SHARING.—Consistent with the protection of classified information, the Director of National Intelligence, acting through the Director of the National Counterterrorism Center, in coordination with the Director of the Federal Bureau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis, shall share the intelligence assessment under paragraph (1) with—

(A) appropriate Federal departments and agencies;

(B) Joint Terrorism Task Forces and the Domestic Terrorism-Hate Crimes Fusion Cell of the Federal Bureau of Investigation;

(C) State, local, and Tribal law enforcement officials, including officials who operate within State, local, and regional fusion centers through the Department of Homeland Security State, Local, and Regional Fusion Center Initiative established in accordance with section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h); and

(D) appropriate foreign governments, including foreign intelligence services and foreign police, and international institutions, that partner with the United States on countering significant threats associated with foreign racially motivated violent extremist organizations.

(b) REPORT.—

(1) REQUIREMENT.—Not later than 150 days after the date of the enactment of this Act, the Director of National Intelligence, acting through the Director of the National Counterterrorism Center, in coordination with the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Homeland Security, and in a manner consistent with the authorities and responsibilities of such Secretary or Director, shall submit to the appropriate congressional committees a report on the use of Federal laws, regulations, and policies by the Federal Government to counter significant threats to the United States and United States persons associated with foreign racially motivated violent extremist organizations.

(2) ELEMENTS.—The report under paragraph (1) shall include the following:

(A) An identification, description, and assessment of the use and efficacy of, Federal laws, regulations, and policies used by the Federal Government to address significant threats to the United States and United States persons associated with foreign racially motivated violent extremist organizations, including pursuant to—

(i) section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) and section 119 of the National Security Act of 1949 (50 U.S.C. 3056), particularly with respect to the coordination and integration of all instruments of national power;

(ii) Executive Order 12333 (50 U.S.C. 3001 note), as amended;

(iii) the designation of foreign terrorist organizations under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189);

(iv) the designation of specially designated terrorists, specially designated global terrorists, or specially designated nationals and blocked persons, pursuant to Executive Orders 13886, 13372, and 13224 and parts 594, 595, 596, and 597 of title 31, Code of Federal Regulations;

(v) National Security Presidential Memorandums 7 and 9, particularly with respect to the sharing of terrorism information and screening and vetting activities; and

(vi) any other applicable Federal laws, regulations, or policies.

(B) An assessment of whether (and if so, to what extent and why) such Federal laws, regulations, and policies are sufficient to counter such threats, including a description of any gaps and specific examples to illustrate such gaps.

(C) Recommendations regarding how to remedy the gaps under subparagraph (B).

(3) PRIVACY AND CIVIL LIBERTIES ASSESSMENT.—Not later than 180 days after the date of the enactment of this Act, the Privacy and Civil Liberties Oversight Board, in consultation with the civil liberties and privacy officers of the Federal departments and agencies the Board determines appropriate, shall submit to the appropriate congressional committees a report containing—

(A) an assessment of the impacts on the privacy and civil liberties of United States persons concerning the use or recommended use of any Federal laws, regulations, and policies specified in paragraph (2); and

(B) recommendations on options to develop protections to mitigate such impacts.

(4) FORM.—The reports under paragraphs (1) and (2) shall be submitted in unclassified form, but may include a classified annex in electronic form that is fully indexed and searchable. In carrying out this paragraph, the officials responsible for submitting such reports shall ensure that the reports are unclassified to the extent possible.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Permanent Select Committee on Intelligence, the Committee on Homeland Security, the Committee on Foreign Affairs, and the Committee on the Judiciary of the House of Representatives; and

(B) the Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, and the Committee on the Judiciary of the Senate.

(2) TERRORISM INFORMATION.—The term "terrorism information" has the meaning given that term in section 1016(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(a)).

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

**SEC. 703. PERIODIC REPORT ON POSITIONS IN 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 amended—

(1) by striking "this Act and not less frequently than once every 5 years thereafter," and inserting "this Act, and biennially thereafter,"; and

(2) by adding at the end the following new sentence: "Such report shall take into account the potential effect of maintaining continuity of operations during a covered national emergency (as defined by section 303 of the Intelligence Authorization Act for Fiscal Year 2021 (division W of Public Law 116–260)) and the assessed needs of the intelligence community to maintain such continuity of operations.".

**SEC. 704. BIENNIAL REPORTS ON FOREIGN BIOLOGICAL THREATS.**

(a) REQUIREMENT.—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 new section (and conforming the table of contents at the beginning of such Act accordingly):

**"SEC. 1111. BIENNIAL REPORTS ON FOREIGN BIOLOGICAL THREATS.**

"(a) REPORTS.—On a biennial basis until the date that is 10 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, the Director of National Intelligence shall submit to the congressional intelligence committees a comprehensive report on the activities, prioritization, and responsibilities of the intelligence community with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country.

"(b) MATTERS INCLUDED.—Each report under subsection (a) shall include, with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country, the following:

"(1) A detailed description of all activities relating to such threats undertaken by each element of the intelligence community, and an assessment of any gaps in such activities.

"(2) A detailed description of all duties and responsibilities relating to such threats explicitly authorized or otherwise assigned, exclusively or jointly, to each element of the intelligence community, and an assessment of any identified gaps in such duties or responsibilities.

"(3) A description of the coordination among the relevant elements of the intelligence community with respect to the activities specified in paragraph (1) and the duties and responsibilities specified in paragraph (2).

"(4) An inventory of the strategies, plans, policies, and interagency agreements of the intelligence community relating to the collection, monitoring, analysis, mitigation, and attribution of such threats, and an assessment of any identified gaps therein.

"(5) A description of the coordination and interactions among the relevant elements of the intelligence community and non-intelligence community partners.

"(6) An assessment of foreign malign influence efforts relating to such threats, and a description of how the intelligence community contributes to efforts by non-intelligence community partners to counter such foreign malign influence.

"(c) FORM.—Each report submitted under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

"(d) DEFINITIONS.—In this section:

"(1) COVERED COUNTRY.—The term 'covered country' means—

"(A) China;

"(B) Iran;

"(C) North Korea;

"(D) Russia; and

"(E) any other foreign country—

"(i) from which the Director of National Intelligence determines a biological threat emanates; or

"(ii) that the Director determines has a known history of, or has been assessed as having conditions present for, infectious disease outbreaks or epidemics.

"(2) FOREIGN BIOLOGICAL THREAT.—The term 'foreign biological threat' means biological warfare, bioterrorism, naturally occurring infectious diseases, or accidental exposures to biological materials, without regard to whether the threat

originates from a state actor, a non-state actor, natural conditions, or an undetermined source.

"(3) FOREIGN MALIGN INFLUENCE.—The term 'foreign malign influence' has the meaning given such term in section 119C(e).

"(4) NON-INTELLIGENCE COMMUNITY PARTNER.—The term 'non-intelligence community partner' means a Federal department or agency that is not an element of the intelligence community.".

(b) FIRST REPORT.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees the first report required under section 1111 of the National Security Act of 1947, as added by subsection (a).

**SEC. 705. ANNUAL REPORTS ON DOMESTIC ACTIVITIES OF INTELLIGENCE COMMUNITY.**

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

(1) the Federal Bureau of Investigation and the Department of Homeland Security conduct vital work in enforcing the rule of law and safeguarding the people of the United States from harm;

(2) the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3638) sought to facilitate greater information sharing between law enforcement and intelligence communities for the purpose of thwarting attacks on the homeland from international terrorist organizations;

(3) National Intelligence Program funds should be expended only in support of intelligence activities with a foreign nexus, consistent with the definition of "intelligence" provided by Congress in section 3 of the National Security Act of 1947 (50 U.S.C. 3003); and

(4) the intelligence community should not engage in the collection, assessment, or analysis of information that pertains exclusively to United States persons absent a foreign nexus.

(b) REQUIREMENT.—Title XI of the National Security Act of 1947 (50 U.S.C. 3231 et seq.), as amended by section 704, is further amended by adding at the end the following new section (and conforming the table of contents at the beginning of such Act accordingly):

**"SEC. 1112. ANNUAL REPORTS ON THE DOMESTIC ACTIVITIES OF THE INTELLIGENCE COMMUNITY.**

"(a) REPORTS.—Not later than January 31 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report—

"(1) identifying all domestic activities undertaken by each element of the intelligence community during the prior fiscal year; and

"(2) for each activity identified under paragraph (1), a statement of the legal authority authorizing such activity to be undertaken.

"(b) FORM.—Each report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.".

(c) FIRST REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees the first report required under section 1112 of the National Security Act of 1947, as added by subsection (a).

**SEC. 706. ANNUAL REPORTS ON CERTAIN CYBER VULNERABILITIES PROCURED BY INTELLIGENCE COMMUNITY AND FOREIGN COMMERCIAL PROVIDERS OF CYBER VULNERABILITIES.**

(a) REQUIREMENT.—Title XI of the National Security Act of 1947 (50 U.S.C. 3231 et seq.), as amended by section 705, is further amended by adding at the end the following new section (and conforming the table of contents at the beginning of such Act accordingly):

**"SEC. 1113. ANNUAL REPORTS ON CERTAIN CYBER VULNERABILITIES PROCURED BY INTELLIGENCE COMMUNITY AND FOREIGN COMMERCIAL PROVIDERS OF CYBER VULNERABILITIES.**

"(a) ANNUAL REPORTS.—On an annual basis through 2026, the Director of the Central Intelligence Agency and the Director of the National Security Agency, in coordination with the Director of National Intelligence, shall jointly submit to the congressional intelligence committees a report containing information on foreign commercial providers and the cyber vulnerabilities procured by the intelligence community through foreign commercial providers.

"(b) ELEMENTS.—Each report under subsection (a) shall include, with respect to the period covered by the report, the following:

"(1) A description of each cyber vulnerability procured through a foreign commercial provider, including—

"(A) a description of the vulnerability;

"(B) the date of the procurement;

"(C) whether the procurement consisted of only that vulnerability or included other vulnerabilities;

"(D) the cost of the procurement;

"(E) the identity of the commercial provider and, if the commercial provider was not the original supplier of the vulnerability, a description of the original supplier;

"(F) the country of origin of the vulnerability; and

"(G) an assessment of the ability of the intelligence community to use the vulnerability, including whether such use will be operational or for research and development, and the approximate timeline for such use.

"(2) An assessment of foreign commercial providers that—

"(A) pose a significant threat to the national security of the United States; or

"(B) have provided cyber vulnerabilities to any foreign government that—

"(i) has used the cyber vulnerabilities to target United States persons, the United States Government, journalists, or dissidents; or

"(ii) has an established pattern or practice of violating human rights or suppressing dissent.

"(3) An assessment of whether the intelligence community has conducted business with the foreign commercial providers identified under paragraph (2) during the 5-year period preceding the date of the report.

"(c) FORM.—Each report under subsection (a) may be submitted in classified form.

"(d) DEFINITIONS.—In this section:

"(1) COMMERCIAL PROVIDER.—The term 'commercial provider' means any person that sells, or acts as a broker, for a cyber vulnerability.

"(2) CYBER VULNERABILITY.—The term 'cyber vulnerability' means any tool, exploit, vulnerability, or code that is intended to compromise a device, network, or system, including such a tool, exploit, vulnerability, or code procured by the intelligence community for purposes of research and development.".

(b) FIRST REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency and the Director of the National Security Agency shall jointly submit to the appropriate congressional committees the first report required under section 1113 of the National Security Act of 1947, as added by subsection (a).

**SEC. 707. IMPROVEMENTS TO ANNUAL REPORT ON DEMOGRAPHIC DATA OF EMPLOYEES OF INTELLIGENCE COMMUNITY.**

Section 5704(c) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334b(c)) is amended—

(1) in the matter preceding paragraph (1), by striking "After making available a report under subsection (b), the Director of National Intelligence shall annually provide a report" and inserting "Not later than March 31 of each year, the Director of National Intelligence shall provide a report"; and

(2) by striking paragraph (1) and inserting the following new paragraph:

"(1) demographic data and information on the status of diversity and inclusion efforts of the intelligence community, including demographic data relating to—

"(A) the average years of service;

"(B) the average number of years of service for each level in the General Schedule, Senior Executive Service, Senior Intelligence Service, or equivalent; and

"(C) career categories;".

**SEC. 708. NATIONAL INTELLIGENCE ESTIMATE ON ESCALATION AND DE-ESCALATION OF GRAY ZONE ACTIVITIES IN GREAT POWER COMPETITION.**

(a) FINDINGS.—Congress finds the following:

(1) The conventional power of the United States has driven foreign adversaries to a level of competition that does not always depend on military confrontation with the United States.

(2) Rather than challenging the United States in a manner that could provoke a kinetic military response, foreign adversaries of the United States have turned to carrying out gray zone activities to advance the interests of such adversaries, weaken the power of the United States, and erode the norms that underpin the United States-led international order.

(3) Gray zone activity falls on a spectrum of attribution and deniability that ranges from covert adversary operations, to detectible covert adversary operations, to unattributable adversary operations, to deniable adversary operations, to open adversary operations.

(4) To adequately address such a shift to gray zone activity, the United States must understand what actions tend to either escalate or de-escalate such activity by our adversaries.

(5) The laws, principles, and values of the United States are strategic advantages in great power competition with authoritarian foreign adversaries that carry out gray zone activities, because such laws, principles, and values increase the appeal of the governance model of the United States, and the United States-led international order, to states and peoples around the world.

(6) The international security environment has demonstrated numerous examples of gray zone activities carried out by foreign adversaries, including the following activities of foreign adversaries:

(A) Information operations, such as efforts by Russia to influence the 2020 United States Federal elections (as described in the March 15, 2021, intelligence community assessment of the Office of the Director of National Intelligence made publicly available on March 15, 2021).

(B) Adversary political coercion operations, such as the wielding of energy by Russia, particularly in the context of Ukrainian gas pipelines, to coerce its neighbors into compliance with its policies.

(C) Cyber operations, such as the use by China of cyber tools to conduct industrial espionage.

(D) Provision of support to proxy forces, such as the support provided by Iran to Hezbollah and Shia militia groups.

(E) Provocation by armed forces controlled by the government of the foreign adversary through measures that do not rise to the level of an armed attack, such as the use of the China Coast Guard and maritime militia by China to harass the fishing vessels of other countries in the South China Sea.

(F) Alleged uses of lethal force on foreign soil, such as the 2018 poisoning of Sergei Skripal in London by Russia.

(G) The potential use by an adversary of technology that causes anomalous health incidents among United States Government personnel.

(b) NATIONAL INTELLIGENCE ESTIMATE.—

(1) REQUIREMENT.—The Director of National Intelligence, acting through the National Intelligence Council, shall produce a National Intelligence Estimate on how foreign adversaries use gray zone activities to advance interests, what responses by the United States (or the allies or partners of the United States) would tend to result in the escalation or de-escalation of such gray zone activities by foreign adversaries, and any opportunities for the United States to minimize the extent to which foreign adversaries use gray zone activities in furtherance of great power competition.

(2) MATTERS INCLUDED.—To the extent determined appropriate by the National Intelligence Council, the National Intelligence Estimate produced under paragraph (1) may include an assessment of the following topics:

(A) Any potential or actual lethal or harmful gray zone activities carried out against the United States by foreign adversaries, including against United States Government employees and United States persons, whether located within or outside of the United States.

(B) To the extent such activities have occurred, or are predicted to occur—

(i) opportunities to reduce or deter any such activities; and

(ii) any actions of the United States Government that would tend to result in the escalation or de-escalation of such activities.

(C) Any incidents in which foreign adversaries could have used, but ultimately did not use, gray zone activities to advance the interests of such adversaries, including an assessment as to why the foreign adversary ultimately did not use gray zone activities.

(D) The effect of lowering the United States Government threshold for the public attribution of detectible covert adversary operations, unattributable adversary operations, and deniable adversary operations.

(E) The effect of lowering the United States Government threshold for responding to detectible covert adversary operations, unattributable adversary operations, and deniable adversary operations.

(F) The extent to which the governments of foreign adversaries exercise control over any proxies or parastate actors used by such governments in carrying out gray zone activities.

(G) The extent to which gray zone activities carried out by foreign adversaries affect the private sector of the United States.

(H) The international norms that provide the greatest deterrence to gray zone activities carried out by foreign adversaries, and opportunities for strengthening those norms.

(I) The effect, if any, of the strengthening of democratic governance abroad on the resilience of United States allies and partners to gray zone activities.

(J) Opportunities to strengthen the resilience of United States allies and partners to gray zone activities, and associated tactics, carried out by foreign adversaries.

(K) Opportunities for the United States to improve the detection of, and early warning for, such activities and tactics.

(L) Opportunities for the United States to galvanize international support in responding to such activities and tactics.

(3) SUBMISSION TO CONGRESS.—

(A) SUBMISSION.—Not later than 1 year after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees the National Intelligence Estimate produced under paragraph (1), including all intelligence reporting underlying the Estimate.

(B) NOTICE REGARDING SUBMISSION.—If at any time before the deadline specified in subparagraph (A), the Director determines that the National Intelligence Estimate produced under paragraph (1) cannot be submitted by such deadline, the Director shall (before such deadline) submit to the congressional intelligence committees a report setting forth the reasons why the National Intelligence Estimate cannot be submitted by such deadline and an estimated date for the submission of the National Intelligence Estimate.

(C) FORM.—Any report under subparagraph (B) shall be submitted in unclassified form.

(4) PUBLIC VERSION.—Consistent with the protection of intelligence sources and methods, at the same time as the Director submits to the congressional intelligence committees the National Intelligence Estimate under paragraph (1), the Director shall make publicly available on the internet website of the Director an unclassified version of the key findings of the National Intelligence Estimate.

(5) DEFINITIONS.—In this subsection:

(A) GRAY ZONE ACTIVITY.—The term "gray zone activity" means an activity to advance the national interests of a State that—

(i) falls between ordinary statecraft and open warfare;

(ii) is carried out with an intent to maximize the advancement of interests of the state without provoking a kinetic military response by the United States; and

(iii) falls on a spectrum that ranges from covert adversary operations, to detectible covert adversary operations, to unattributable adversary operations, to deniable adversary operations, to open adversary operations.

(B) COVERT ADVERSARY OPERATION.—The term "covert adversary operation" means an operation by an adversary that—

(i) the adversary intends to remain below the threshold at which the United States detects the operation; and

(ii) does stay below such threshold.

(C) DETECTIBLE COVERT ADVERSARY OPERATION.—The term "detectible covert adversary operation" means an operation by an adversary that—

(i) the adversary intends to remain below the threshold at which the United States detects the operation; but

(ii) is ultimately detected by the United States at a level below the level at which the United States will publicly attribute the operation to the adversary.

(D) UNATTRIBUTABLE ADVERSARY OPERATION.—The term "unattributable adversary operation" means an operation by an adversary that the adversary intends to be detected by the United States, but remain below the threshold at which the United States will publicly attribute the operation to the adversary.

(E) DENIABLE ADVERSARY OPERATION.—The term "deniable adversary operation" means an operation by an adversary that—

(i) the adversary intends to be detected and publicly or privately attributed by the United States; and

(ii) the adversary intends to deny, to limit the response by the United States, and any allies of the United States.

(F) OPEN ADVERSARY OPERATION.—The term "open adversary operation" means an operation by an adversary that the adversary openly acknowledges as attributable to the adversary.

(c) REQUIREMENT TO DEVELOP LEXICON.—

(1) REQUIREMENT.—The Director of National Intelligence, acting through the National Intelligence Council, shall develop a lexicon of common terms (and corresponding definitions for such terms) for concepts associated with gray zone activities.

(2) CONSIDERATIONS.—In developing the lexicon under paragraph (1), the National Intelligence Council shall include in the lexicon each term (and the corresponding definition for each term) specified in subsection (b)(5), unless the National Intelligence Council determines that an alternative term (or alternative definition)—

(A) more accurately describes a concept associated with gray zone activities; or

(B) is preferable for any other reason.

(3) REPORT.—

(A) PUBLICATION.—The Director of National Intelligence shall publish a report containing the lexicon developed under paragraph (1).

(B) FORM.—The report under subparagraph (A) shall be published in unclassified form.

**SEC. 709. REPORT ON CERTAIN ACTIONS TAKEN BY INTELLIGENCE COMMUNITY WITH RESPECT TO HUMAN RIGHTS AND INTERNATIONAL HUMANITARIAN LAW.**

(a) REPORT.—Not later than 120 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, the Director of the National Security Agency, the Secretary of Defense, and the Director of the Defense Intelligence Agency, shall submit to the congressional intelligence committees a report on certain actions taken by the intelligence community with respect to human rights and international humanitarian law.

(b) ELEMENTS.—The report under subsection (a) shall include the following:

(1) A detailed explanation of whether, and to what extent, each element of the intelligence community has provided intelligence products relating to the efforts of the Secretary of State and the Secretary of Treasury regarding the categorization, determinations on eligibility for assistance and training, and general understanding, of covered entities that commit, engage, or are otherwise complicit in, violations of human rights or international humanitarian law.

(2) A detailed explanation of whether, and to what extent, each element of the intelligence community has provided intelligence products relating to any of the following:

(A) Section 7031(c) of the Department of State, Foreign Operations, and Related Programs Appropriations Act, 2020 (division G of Public Law 116–94; 8 U.S.C. 1182 note).

(B) The visa restriction policy of the Department of State announced on February 26, 2021, and commonly referred to as the "Khashoggi Ban".

(C) The annual report requirement of the Department of Defense under section 1057 of the National Defense Authorization Act for Fiscal Year 2018 (131 Stat. 1572).

(D) The Global Magnitsky Human Rights Accountability Act (subtitle F of title XII of Public Law 114–328; 22 U.S.C. 2656 note).

(3) A detailed explanation of the following processes:

(A) The process of each element of the intelligence community for monitoring covered entities for derogatory human rights or international humanitarian law information.

(B) The process of each element of the intelligence community for determining the credibility of derogatory human rights or international humanitarian law information.

(C) The process of each element of the intelligence community for determining what further action is appropriate if derogatory human rights or international humanitarian law information is determined to be credible.

(4) An unredacted copy of each policy or similar document that describes a process specified in paragraph (3).

(5) A detailed explanation of whether, with respect to each element of the intelligence community, the head of the element has changed or restricted any activities of the element in response to derogatory human rights or international humanitarian law information.

(6) Examples of any changes or restrictions specified in paragraph (5) taken by the head of the element of the intelligence community during the two years preceding the date of the submission of the report.

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

(d) DEFINITIONS.—In this section:

(1) COVERED ENTITY.—The term "covered entity"—

(A) means an individual, unit, or foreign government that—

(i) has a cooperative relationship with the United States Government; or

(ii) is the target of an intelligence collection activity carried out by the United States Government; but

(B) does not include an employee of the United States Government.

(2) DEROGATORY HUMAN RIGHTS OR INTERNATIONAL HUMANITARIAN LAW INFORMATION.—The term "derogatory human rights or international humanitarian law information" means information tending to suggest that a covered entity committed, participated, or was otherwise complicit in, a violation of human rights or international humanitarian law, regardless of the credibility of such information, the source of the information, or the level of classification of the information.

(3) VIOLATION OF HUMAN RIGHTS OR INTERNATIONAL HUMANITARIAN LAW.—The term "violation of human rights or international humanitarian law" includes a violation of any authority or obligation of the United States Government related to human rights or international humanitarian law, without regard to whether such authority or obligation is codified in a provision of law, regulation, or policy.

**SEC. 710. BRIEFING ON TRAININGS RELATING TO BLOCKCHAIN TECHNOLOGY.**

(a) BRIEFING.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall provide to the congressional intelligence committees a briefing on the feasibility and benefits of providing training described in subsection (b).

(b) TRAINING DESCRIBED.—Training described in this subsection is training that meets the following criteria:

(1) The training is on cryptocurrency, blockchain technology, or both subjects.

(2) The training may be provided through partnerships with universities or private sector entities.

**SEC. 711. REPORT ON PROSPECTIVE ABILITY TO ADMINISTER COVID–19 VACCINES AND OTHER MEDICAL INTERVENTIONS TO CERTAIN INTELLIGENCE COMMUNITY PERSONNEL.**

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence and the Under Secretary of Defense for Intelligence and Security, in consultation with the elements of the intelligence community and relevant public health agencies of the United States, shall jointly develop and submit to the congressional intelligence committees a report on the prospective ability of the intelligence community to administer COVID–19 vaccines, and such other medical interventions as may be relevant in the case of a future covered national emergency, to covered personnel (particularly with respect to essential covered personnel and covered personnel deployed outside of the United States).

(b) MATTERS INCLUDED.—The report under subsection (a) shall include an assessment of the following:

(1) The prospective ability of the elements of the intelligence community to administer COVID–19 vaccines (including subsequent booster shots for COVID–19), to covered personnel, and whether additional authorities or resources are necessary for, or may otherwise facilitate, such administration.

(2) The potential risks and benefits of granting the additional authorities or resources described in paragraph (1) to the Director, the Under Secretary, or both.

(3) With respect to potential future covered national emergencies, including future outbreaks of an infectious pandemic disease or similar public health emergencies, the following:

(A) The ability of the intelligence community to ensure the timely administration of medical interventions to covered personnel during the covered national emergency.

(B) Whether additional authorities or resources are necessary to ensure, or may otherwise facilitate, such timely administration, including with respect to the ability of the Director or Under Secretary to provide an alternative means of access to covered personnel with reduced access to the interventions provided by the respective element.

(C) The potential risks and benefits of granting the additional authorities or resources described in subparagraph (B) to the Director, the Under Secretary, or both.

(4) A summary of the findings of the survey under subsection (c).

(c) SURVEY.—Not later than 120 days after the date of the enactment of this Act, and prior to submitting the report under subsection (a), the Director and the Under Secretary shall jointly conduct a survey to determine the process by which each element of the intelligence community has administered COVID–19 vaccines to covered personnel, to inform continued medical care relating to COVID–19 and future responses to covered national emergencies. Such survey shall address, with respect to each element, the following:

(1) The timeline of the element with respect to the administration of COVID–19 vaccines prior to the date of the enactment of this Act.

(2) The process by which the element determined when covered personnel would become eligible to receive the COVID–19 vaccine (including if certain categories of such personnel became eligible before others).

(3) A general approximation of the percentage of covered personnel of the element that received the COVID–19 vaccine from the element versus through an alternative means (such as a private sector entity, foreign government, State, or local government), particularly with respect to covered personnel deployed outside of the United States.

(4) Any challenges encountered by the element with respect to the administration of COVID–19 vaccines prior to the date of the enactment of this Act.

(5) Any other feedback determined relevant for purposes of the survey.

(d) PRIVACY CONSIDERATIONS.—In carrying out the report and survey requirements under this section, the Director, the Under Secretary, and the heads of the elements of the intelligence community shall ensure, to the extent practicable, the preservation of medical privacy and the anonymity of data.

(e) DEFINITIONS.—In this section:

(1) COVERED NATIONAL EMERGENCY.—The term "covered national emergency" has the meaning given such term in section 303 of the Intelligence Authorization Act for Fiscal Year 2021 (50 U.S.C. 3316b).

(2) COVERED PERSONNEL.—The term "covered personnel" means personnel who are—

(A) employees of, or otherwise detailed or assigned to, an element of the intelligence community; or

(B) funded under the National Intelligence Program or the Military Intelligence Program.

(3) ESSENTIAL COVERED PERSONNEL.—The term "essential covered personnel" means covered personnel deemed essential to—

(A) continuity of operations of the intelligence community;

(B) continuity of operations of the United States Government; or

(C) other purposes related to the national security of the United States.

(4) NATIONAL INTELLIGENCE PROGRAM.—The term "National Intelligence Program" has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

**SEC. 712. REPORT ON POTENTIAL INCLUSION WITHIN INTELLIGENCE COMMUNITY OF THE OFFICE OF NATIONAL SECURITY OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES.**

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Secretary of Health and Human Services, shall submit to the appropriate congressional committees a report on the potential advantages and disadvantages of adding the Office of National Security of the Department of Health and Human Services as a new element of the intelligence community.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment of the following:

(A) The likelihood that the addition of the Office of National Security as a new element of the intelligence community would increase connectivity between other elements of the intelligence community working on health security topics and the Department of Health and Human Services.

(B) The likelihood that such addition would increase the flow of raw intelligence and finished intelligence products to officials of the Department of Health and Human Services.

(C) The likelihood that such addition would facilitate the flow of information relating to health security topics to intelligence analysts of various other elements of the intelligence community working on such topics.

(D) The extent to which such addition would clearly demonstrate to both the national security community and the public health community that health security is national security.

(E) Any anticipated impediments to such addition relating to additional budgetary oversight by the executive branch or Congress.

(F) Any other significant advantages or disadvantages of such addition, as identified by either the Director of National Intelligence or the Secretary of Health and Human Services.

(2) A joint recommendation by the Director of National Intelligence and the Secretary of Health and Human Services as to whether to add the Office of National Security as a new element of the intelligence community.

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

(d) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term "appropriate congressional committees" means—

(1) the congressional intelligence committees; and

(2) the Committee on Energy and Commerce of the House of Representatives and the Committee on Health, Education, Labor, and Pensions of the Senate.

**SEC. 713. REPORTS RELATING TO INSPECTOR GENERAL OF DEFENSE INTELLIGENCE AGENCY.**

(a) REPORT ON RESPONSES BY INSPECTOR GENERAL TO SUBSTANTIATED ALLEGATIONS.—

(1) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of the Defense Intelligence Agency shall submit to the congressional intelligence committees a report on allegations of reprisal or abuse of authority determined to be substantiated by the Inspector General of the Defense Intelligence Agency during the 5-year period preceding the date of the enactment of this Act.

(2) MATTERS INCLUDED.—The report under paragraph (1) shall include, with respect to each allegation determined to be substantiated during the 5-year period specified in such paragraph, a description of the following:

(A) Details of each substantiated allegation.

(B) The rank or grade of the individuals involved in the allegation.

(C) Any disciplinary action recommended by the Inspector General in response to the allegation, or, if the Inspector General recommended no disciplinary action be taken in response, any justification for such recommendation.

(D) Any disciplinary action taken by the relevant manager of the Defense Intelligence Agency in response to the allegation.

(E) Whether the relevant manager reduced, or declined to take, a disciplinary action recommended by the Inspector General in response to the allegation.

(F) Any justification from the relevant manager regarding the decision to take, reduce, or decline to take, a disciplinary action recommended by the Inspector General in response to the allegation.

(G) The process by which Defense Intelligence Agency management reviews and makes decisions regarding disciplinary actions in response to substantiated allegations, including—

(i) the criteria applied by management in making the decision to take, reduce, or decline to take, a disciplinary action;

(ii) a description of which managers have the authority to make such decisions, including the rank or grade of the managers; and

(iii) a description of any formal or informal appeals processes available with respect to such decisions.

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

(b) REPORT ON PROCESSES FOR ENSURING INDEPENDENCE OF INSPECTOR GENERAL.—

(1) REPORT.—Not later than 30 days after the date of the enactment of this Act, the Director of the Defense Intelligence Agency shall submit to the congressional intelligence committees and the Council of the Inspectors General on Integrity and Efficiency established under section 11 of the Inspector General Act of 1978 (5 U.S.C. App.) a report on the processes of the Defense Intelligence Agency for ensuring the independence of the position of the Inspector General of the Defense Intelligence Agency.

(2) MATTERS INCLUDED.—The report under paragraph (1) shall include a description of the following:

(A) The selection criteria used by the Director in the appointment of the Inspector General.

(B) The methods used by the Director to ensure the independence of the position of the Inspector General, including—

(i) the process for vetting candidates for such position for independence from leadership of the Defense Intelligence Agency and from officials occupying positions in the Defense Intelligence Senior Executive Service; and

(ii) the process for evaluating such candidates for conflicts of interest.

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

(c) ASSESSMENT BY COUNCIL OF INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY.—

(1) ASSESSMENT.—Not later than 120 days after the date of the enactment of this Act, the Council of the Inspectors General on Integrity and Efficiency shall—

(A) conduct an assessment of the effectiveness of the selection criteria and methods specified in subsection (b)(2) with respect to the position of the Inspector General of the Defense Intelligence Agency; and

(B) submit to the congressional intelligence committees a report containing the results of such assessment.

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

**SEC. 714. REPORT ON RARE EARTH ELEMENTS.**

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Director of the Defense Intelligence Agency, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, and any other head of an element of the intelligence community that the Director of National Intelligence determines relevant, shall submit to the congressional intelligence committees a report on rare earth elements.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment coordinated by the National Intelligence Council of—

(A) long-term trends in the global rare earth element industry;

(B) the national security, economic, and industrial risks to the United States, and to the partners and allies of the United States, with respect to relying on foreign countries for rare earth mining and the processing or production of rare earth elements;

(C) the intentions of foreign governments with respect to limiting, reducing, or ending access of the United States or the partners and allies of the United States to—

(i) rare earth elements; or

(ii) any aspect of the rare earth mining, processing, or production chain; and

(D) opportunities for the United States, and for the partners and allies of the United States, to assure continued access to—

(i) rare earth elements; and

(ii) the rare earth mining, processing, or production chain.

(2) A description of—

(A) any relevant procurement, use, and supply chain needs of the intelligence community with respect to rare earth elements;

(B) any relevant planning or efforts by the intelligence community to assure secured access to rare earth elements;

(C) any assessed vulnerabilities or risks to the intelligence community with respect to rare earth elements;

(D) any relevant planning or efforts by the intelligence community to coordinate with departments and agencies of the United States Government that are not elements of the intelligence community on securing the rare earth element supply chain; and

(E) any previous or anticipated efforts by the Supply Chain and Counterintelligence Risk Management Task Force established under 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) with respect to rare earth elements.

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

(d) RARE EARTH ELEMENTS DEFINED.—In this section, the term "rare earth elements" includes products that contain rare earth elements, including rare earth magnets.

**SEC. 715. REPORT ON PLAN TO FULLY FUND THE INFORMATION SYSTEMS SECURITY PROGRAM AND NEXT GENERATION ENCRYPTION.**

(a) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Defense shall submit to the appropriate congressional committees a report on the resources necessary to fully fund the Information Systems Security Program during the period covered by the most recent future-years defense program submitted under section 221 of title 10, United States Code—

(1) to address the cybersecurity requirements of the Department of Defense; and

(2) for the adoption of next generation encryption into existing and future systems.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment by the Chief Information Officer of the Department of Defense, in coordination with the chiefs of the Armed Forces and in consultation with the Director of the National Security Agency, of the additional resources required to fund the Information Systems Security Program at a level that satisfies current and anticipated cybersecurity requirements of the Department.

(2) An identification of any existing funding not currently aligned to the Program that is more appropriately funded through the Program.

(3) A strategic plan, developed in coordination with the chiefs of the Armed Forces and in consultation with the Director of the National Security Agency, that provides options, timelines, and required funding by the Armed Forces or a component of the Department, for the adoption of next generation encryption into existing and future systems.

(c) FORM.—The report under subsection (a) may be submitted in classified form.

(d) BRIEFING.—Not later than 30 days after the date on which the Secretary submits the report under subsection (a), the Chief Information Officer of the Department and the Director of the National Security Agency shall jointly provide to the appropriate congressional committees a briefing on the report.

(e) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term "appropriate congressional committees" means—

(1) the Committee on Armed Services, the Committee on Appropriations, and the Permanent Select Committee on Intelligence of the House of Representatives; and

(2) the Committee on Armed Services, the Committee on Appropriations, and the Select Committee on Intelligence of the Senate.

**SEC. 716. REVIEW OF NATIONAL SECURITY AGENCY AND UNITED STATES CYBER COMMAND.**

(a) REVIEW REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Inspectors General of the National Security Agency, Intelligence Community, and Department of Defense shall jointly complete a review of the National Security Agency and the United States Cyber Command.

(b) ELEMENTS.—The review required by subsection (a) shall include assessment of the following:

(1) Whether and what resources, authorities, activities, missions, facilities, and personnel are appropriately being delineated and used to conduct the intelligence and cybersecurity missions at the National Security Agency as well as the cyber offense and defense missions of the United States Cyber Command.

(2) The extent to which current resource-sharing arrangements between the National Security Agency and the United States Cyber Command lead to conflicts of interest in directing intelligence collection in support of United States Cyber Command missions rather than foreign intelligence collection.

(3) The intelligence analysis and production conducted by the United States Cyber Command using National Security Agency authorities, with a focus on analytic integrity and intelligence oversight to ensure proper analysis is informing mission operations.

(4) The number of personnel detailed from the National Security Agency to the United States Cyber Command, including from which offices such personnel have been detailed, and an assessment of the mission impact on the sponsoring office.

(c) REPORT AND BRIEF.—Not later than 180 days after the date of the enactment of this Act, the Inspectors General of the National Security Agency, Intelligence Community, and Department of Defense shall jointly submit to the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) a report and provide such committees a briefing on the findings of the inspectors general with respect to the review completed under subsection (a).

## PURPOSE

The purpose of H.R. 5412, the Intelligence Authorization Act for Fiscal Year 2022 (the Act), is to authorize the intelligence and intelligence-related activities of the United States Government for Fiscal Year (FY) 2022.

## CLASSIFIED ANNEX AND COMMITTEE INTENT

The classified annex to this report includes the classified schedule of authorizations and associated explanatory and directive language. The classified schedule of authorizations is incorporated directly into the legislation by Section 102 of the bill. Elements of the Intelligence Community shall strictly comply with all Committee direction and other guidance set forth in the classified annex.

The classified annex and classified schedule of authorizations have been made available for review by all Members of the House of Representatives, on conditions set by the Committee at the time of its consideration of H.R. 5412.

## SCOPE OF COMMITTEE REVIEW

The bill authorizes United States intelligence and intelligence-related activities within the jurisdiction of the Committee, including the National Intelligence Program (NIP) and the Military Intelligence Program (MIP), the Homeland Security Intelligence Program (HSIP), and the Information Systems Security Program (ISSP).

The NIP consists of all activities of the Office of the Director of National Intelligence (ODNI), as well as intelligence, intelligence-related, and counterintelligence activities conducted by: the Central Intelligence Agency; the Department of Defense, including the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and certain activities of the Departments of the Army, Navy, and Air Force; the Department of Energy; the Department of Justice, including the Federal Bureau of Investigation and the Drug Enforcement Administration; the Department of Homeland Security, including the U.S. Coast Guard and intelligence elements of DHS; the Department of State; and the Department of the Treasury.

The MIP consists of certain activities of the Undersecretary of Defense for Intelligence and Security, intelligence, intelligence-related, and counterintelligence activities of the Departments of the Army, Navy, and Air Force, the Marine Corps and Space Force, Special Operations Command, other elements of the Department of Defense and Combat Support Agencies, including the Defense Intelligence Agency, the National Security Agency, the National Geospatial Agency, and certain activities of the National Reconnaissance Office.

The Committee has exclusive or concurrent legislative, authorizing, and oversight jurisdiction of these activities—and exclusive jurisdiction to study the sources and methods of the Intelligence Community.

## COMMITTEE VIEWS

H.R. 5412, the Intelligence Authorization Act for FY 2022 (the Act) authorizes the activities of, and funding for, the 18 elements comprising the United States Intelligence Community. Because most of the intelligence budget involves classified programs, the bulk of the Committee's recommendations each year are found in the classified annex accompanying the bill.

## COMMITTEE STATEMENT REGARDING ANOMALOUS HEALTH INCIDENTS

The Intelligence Authorization Act for Fiscal Year 2022 advances the Committee's continuing, bipartisan efforts with respect to anomalous health incidents, or "AHIs"—which Intelligence Community (IC) and other United States personnel have suffered for years. From the earliest reports of "Havana Syndrome" onward, an utmost priority for the Committee has been to enable a vigorous and comprehensive response by the U.S. Government.

In exercise of its legislative and oversight jurisdiction, and during the 116th and 117th Congresses, the Committee has focused on ensuring that:

- Victims of AHIs are strongly encouraged—at all levels, including by senior and supervisory personnel—to come forward with their accounts immediately and to seek treatment, without fear of being disbelieved, or of other negative consequences;
- Throughout the Executive Branch, clear processes and procedures are established and implemented for reporting, analyzing, and disseminating information about AHIs;
- Victims and their families promptly receive medical care and support of the highest quality, and without encountering bureaucratic obstacles or delays, including in pursuit of specialized care for traumatic brain injuries and in planning for potential long-term physiological and psychological effects;
- Every effort is undertaken throughout the Executive Branch in order to determine the cause or causes of AHIs, and thereafter immediately to report any relevant information to Congress and the American people; and that
- Any actor responsible for these injuries is swiftly held to account.

During the 117th Congress, the Committee's Members and staff have been, and continue to be, regularly briefed on all facets of AHI matters, including the direct experiences of AHI victims and their families. These engagements indicated deficiencies, some of them quite serious, in how AHI issues were handled by the IC in the past—especially with respect to the provision and adequacy of medical care.

Informed by these oversight activities, the IAA takes remedial steps, among other things by:

- Incentivizing doctors in the CIA's Office of Medical Services (OMS) to maintain their medical accreditation, and requiring that such doctors be afforded time to maintain clinical practice;
- Creating an expert advisory board to assist with a top-to-bottom modernization of OMS;

- Mandating a comprehensive review by IC Inspectors General of OMS; and
- Requiring the President to develop uniform protocols for voluntary, pre-deployment testing—or "baselining"—of individuals, and comprehensive treatment and care of individuals (and their families) following an AHI. The IAA further requires creation of protocols that encourage the reporting of AHIs and for handling complaints or concerns regarding the government's treatment of employees who report an AHI.

***

The Committee welcomes the Administration's visible and serious efforts related to providing care to those harmed by AHIs, and to prioritizing investigation of AHI's cause or causes. The Committee notes in particular the significant advances within the IC during the past year, regarding the reporting of AHIs and the provision of medical treatment to affected personnel.

As important as these steps have been, a great deal remains to be done. The Committee remains concerned that, despite the Administration's initiatives, and repeated legislative interventions by Congress, the Executive Branch's AHI policies are not uniform across Departments and agencies. Some victims also continue to be frustrated in their attempts to report AHIs, and are afforded inconsistent or slow access to important treatment and benefits. Going forward, it will be imperative for the Executive Branch to make sure that, in every case, the highest possible quality care and support is provided, expeditiously, to AHI victims and their families. That is a central goal of the IAA's AHI-related provisions, and of the HAVANA Act and related measures championed by the Committee.

The Committee underscores, to the public and to all U.S. personnel and their families, its enduring commitment to providing all necessary resources and authorities—so as to guarantee that AHI victims and their families receive care and support; to quickly determine the origins of this most serious threat to U.S. national security; and to swiftly hold those responsible to account.

## COMMITTEE STATEMENT REGARDING DOMESTIC TERRORISM

During the previous administration, the Department of Homeland Security (DHS) assessed that "white supremacist extremists (WSEs)—will remain the most persistent and lethal threat in the Homeland." Acting Secretary Chad Wolf noted in his preface to DHS's Homeland Threat Assessment, issued in October 2020, that he was "particularly concerned about white supremacist violent extremists" who have become "exceptionally lethal" over the past few years.

The Committee shares this deep concern about the threat of WSEs. To better understand and focus on this threat, the Committee included in this Act Section 702, which aims to improve federal intelligence agencies' ability to prioritize the threat of Racially Motivated Violent Extremists (RMVEs), especially WSEs, which are the most concerning such group. In particular, Sec. 702 adopts H.R. 4038, an act authored by Subcommittee Chairman André Carson, "to direct the Director of National Intelligence to submit to

Congress an intelligence assessment on threats to the United States associated with foreign violent White supremacist extremist organizations." The provision also aims to address intelligence gaps about this threat, including regarding white supremacist extremists' objectives and operational structure.

While the Committee is deeply concerned about the domestic terrorist threat, the Committee is also mindful of the importance of protecting the civil rights and civil liberties of United States persons, and notes that the Intelligence Community plays a vital role in response to that threat.

## OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held multiple hearings, briefings, and other engagements on the classified budgetary issues raised by H.R. 5412. The bill, as reported by the Committee, reflects conclusions reached by the Committee in light of this oversight activity.

## GENERAL PERFORMANCE GOALS AND OBJECTIVES

Broadly stated, the goals and objectives of H.R. 5412 are to authorize the intelligence and intelligence-related activities of the United States Government for Fiscal Year 2022. The classified annex accompanying the legislation reflects in detail the Committee's specific performance goals and objectives with respect to classified programs.

## NON-DUPLICATION OF FEDERAL PROGRAMS

With respect to clause 3(c)(5) of rule XIII of the Rules of the House of Representatives, no provision of H.R. 5412 establishes or reauthorizes a program of the Federal Government that is known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

## COMMITTEE CONSIDERATION

The Committee marked up H.R. 5412 on September 30, 2021. Chairman Schiff offered an amendment in the nature of a substitute, which the Committee adopted by unanimous consent. No other amendments were offered, and the bill as amended was approved and ordered to be reported to the House by voice vote.

## UNCLASSIFIED COMMITTEE DIRECTION

### *Expediting Comprehensive Processing and Resettlement of Vulnerable Afghans*

A continuing Committee priority is the safe evacuation and resettlement of vulnerable foreign nationals fleeing Afghanistan—to include Afghan women and girls, and Afghans and others who assisted the United States or its mission before its departure from Afghanistan on August 30, 2021. In that regard, Section 309 of the Act authorizes non-reimbursable details by Intelligence Community

(IC) personnel to other Executive Branch agencies, for the purpose of assisting with the processing and resettlement of refugees, parolees, and other aliens at risk of being harmed by the Taliban.

The Committee urges Departments and agencies of the Executive Branch to make full and innovative use of this processing and resettlement authority, and of all other related authorities and capabilities, in order to ensure that such persons are evacuated and resettled safely. The Committee also instructs each relevant IC element to continue to provide regular, timely updates to the Committee regarding both processing and resettlement efforts, and any challenges or issues relating to those efforts.

*Intelligence Lessons Learned regarding Afghanistan*

The Committee directs the Director of National Intelligence, in consultation with key heads of elements of the Intelligence Community (IC) as determined appropriate, to create a task force to conduct a review of the intelligence analysis provided by IC elements beginning in September 2018, and up and until the United States withdrawal from Afghanistan on August 31, 2021, and to submit a corresponding report based on that review no later than June 30, 2022. The review, and corresponding report, shall include:

1. An objective overview of the intelligence analysis, products, briefings, and any other relevant information provided by key intelligence elements in connection with deliberations relating to Afghanistan policy during the relevant time period, including counterterrorism (CT), the future stability of the Afghanistan government under President Ghani, the ability of that government to withstand the United States' withdrawal, the threat of terrorist organizations, including Al Qaeda and ISIS–K as a result of potential U.S. withdrawal, and any other relevant issues the element reported on during that period;

2. An assessment of the accuracy of those intelligence materials, including taking into account the extent and quality of information that was available to analysts at the time the assessments were made;

3. An assessment as to whether the IC provided sufficient intelligence materials relating to, and had a sufficient understanding of, the evolving dynamics within Afghanistan, including the subsequent timing of the fall of the Afghanistan government to the Taliban;

4. An assessment of what factors, such as intelligence gaps, and/or limitations in analytic tradecraft, information sharing, and/or other issues, limited the accuracy or usability of the intelligence materials;

5. An assessment of ways to improve the assessment, collection, usability, and information sharing, both internally among the key intelligence elements and between the IC and the Executive Branch, of intelligence materials, based on the limitations identified in (4);

6. An assessment of how to apply the limitations and issues identified in the report to improve U.S. intelligence collection, monitoring, and deterrence in Afghanistan over the next two years, including in the areas of CT, and the U.S. interaction with the Taliban and/or any intelligence elements in Afghanistan; and

7. An overview of lessons learned as applied to future, comparable missions.

*Afghanistan's Tactical Intelligence Capture*

A significant amount of intelligence was collected by tactical military units over the past two decades of conflict in Afghanistan. The Committee acknowledges the challenge in capturing intelligence data from echelons, units, and groups, but believes this information should be appropriately retained for further use as necessary or appropriate. Further, this data should be standardized and formatted in order to effectively share operational intelligence and intelligence mission data across the joint force.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence and Security in coordination with the Defense Intelligence Agency to provide a briefing to the Committee by February 4, 2022, on how the Department will properly utilize, standardize, and format this data, as well as ensure long-term access to this information across relevant echelons, units, branches, and commands within the Department.

*DNI Reporting on Saudi Entities Linked to Murder of Jamal Khashoggi*

The Committee welcomes the Director of National Intelligence's (DNI) submission of the unclassified report required by the Intelligence Authorization Act for Fiscal Year 2021 (P.L. 116–260) confirming the culpability of Saudi government officials in the brutal murder of United States resident and journalist Jamal Khashoggi.

To further inform the Committee's and Congress' ongoing oversight regarding any possible role of Saudi government-affiliated entities and individuals in this heinous act, especially amid public reports implicating the Saudi Public Investment Fund, the Committee directs the DNI to produce an unclassified report, if needed with a classified annex, no later than March 1, 2022, that lists all of the Saudi entities, if any, that the Intelligence Community (IC) assesses as having been linked to the killing. The report shall detail the IC's confidence in that assessment, as well as a summary of all relevant information—unclassified and classified—that informed the IC's assessment. The DNI shall make this report available to the congressional intelligence committees, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate.

*Biodefense Steering Committee*

The Committee directs the Director of National Intelligence (DNI), in coordination with the heads of such other elements of the Intelligence Community (IC) as the DNI may determine relevant, to submit to the congressional intelligence committees by no later than June 30, 2022, a report on the efforts of the IC to support the Biodefense Steering Committee in the implementation of the National Biodefense Strategy. Such report shall at minimum include:

1. A description of previous, ongoing, and planned IC efforts or activities in support of the Committee's, or any successor's, implementation of the National Biodefense Strategy by the Biodefense Steering Committee;

2. An inventory and assessment of any existing IC strategy, plan, or policy of the IC, or interagency agreement entered into by the IC, that relates to the provision of support to the Biodefense Steering Committee, including for the implementation of the National Biodefense Strategy; and

3. A description of assessed opportunities for the IC to further enhance the capabilities and effectiveness of the Biodefense Steering Committee with respect to its implementation of the National Biodefense Strategy.

Such report may be submitted in classified form but should include an unclassified executive summary.

*Examining the Use of Other Transaction Authority*

The barrier to entry for commercial entities to work with the Intelligence Community (IC) is high. Federal contracting and acquisitions processes can be complex, and the IC in particular has strict security and background check requirements that can be difficult for companies, particularly those that are new and small, to meet. It is the belief of the Committee that the IC underutilizes versatile models of acquisition, like Other Transaction Authority (OTA), for work with these nontraditional partners.

Therefore, the Committee directs the Director of National Intelligence to submit to the congressional intelligence committees, by no later than May 31, 2022, a written report on the use of OTA procurement by IC elements for research and prototyping activities. The report shall examine and detail the current use of OTA and identify additional areas in which IC elements could leverage OTA for more efficient and innovative acquisition.

*Security and Resiliency of Intelligence Community*

The Committee is concerned that the Intelligence Community's (IC) cyber infrastructure and capabilities are at risk of supply chain vulnerabilities that could compromise key elements of our national security. Recent revelations confirm that near-peer competitors have heavily invested in the capability to penetrate the IC's communications infrastructure. Those reports present substantial questions about our supply chain vulnerabilities. To counter this challenge, the Committee directs the Director of National Intelligence to develop an acquisition strategy that ensures that critical communications technologies remain secure and resilient in the face of current and future cyber threats.

When developing a strategy for the construction of, or upgrades to, IC communications, the Committee directs IC procurement and acquisition officers to consider mission effectiveness and operational suitability prioritizing factors such as:

1. Components and devices that are engineered, sourced, and manufactured domestically;

2. The accessibility-risk of components and devices responsible for routing and disseminating information, and mitigation measures supported by deterministic systems authoritatively certified and deployed to isolate network communications;

3. The cost of reconfiguring systems in response to dynamic mission requirements and challenges;

4. Physical, logistical, or operational measures to mitigate insider threats; and

5. Consistent with the IC's desire to evaluate energy efficiencies and long-term costs, consideration shall also be given to whether the systems will support next generation technologies and readily incorporate upgrades, reduce the size of the data centers, moderate energy consumption, use clean energy alternatives, and decrease the area needed for rack space and other essential hardware.

*Intelligence Sharing Frameworks*

The Committee notes the importance of intelligence and resource sharing agreements as well as the need to further strengthen connections with alliance countries and others as a key component of fully implementing the National Intelligence and National Defense Strategies.

Therefore, the Committee directs the Director of National Intelligence, in coordination with the Secretary of Defense, and the Director of the Defense Intelligence Agency, to provide a report to the Committee by May 20, 2022, outlining the current intelligence and resource sharing agreements between the United States and Australia, Canada, New Zealand, and the United Kingdom (the Five Eyes); as well as the risks, benefits, and feasibility of expanding such intelligence and resource sharing agreements to South Korea, Japan, India, Germany, and France.

The report shall include a catalogue of the current agreements for Five Eyes intelligence and resource sharing agreements, including the date of any relevant or recent updates, and changes which may be made to increase efficiency and/or enhance security. It shall also include the current significant intelligence and resource sharing efforts among other partner countries, and the risk/gain factors which may be considered for any future intelligence or resource sharing opportunities with countries to include South Korea, Japan, India, Germany, France, and any other countries deemed appropriate.

*IC Support to DoD Emerging Technology Steering Committee*

The Committee continues to encourage the Intelligence Community (IC) to fully engage and coordinate with appropriate science and technology counterparts in the Federal Government to address national and military intelligence scientific and technological priorities. The Strategic Technologies and Advanced Research (STAR) Subcommittee report from 2020 highlighted the need for stronger leadership within the Office of the Director of National Intelligence to coordinate and integrate science and technology efforts across the defense and intelligence enterprise.

Therefore, the Committee directs the Director of National Intelligence to submit to the congressional intelligence committees by no later than April 29, 2022, a report about the IC's interactions with, or activities undertaken in explicit support of, the Department of Defense's steering committee on emerging technology and national security threats, as established by Section 236 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (P.L. 116–283).

*DNI Reporting on the United Arab Emirates*

The Committee is concerned with multiple, credible public reports that the Government of the United Arab Emirates (UAE) has engaged in troubling activities contrary to United States interests, including: security and defense cooperation with adversaries of the United States, most especially China; recruited former U.S. intelligence personnel to engage in surveillance and related activities that may have violated the privacy of American citizens; and prolonged the Saudi-led war in and contributed to a fragmentation of Yemen.

To further inform the Committee's ongoing oversight and in light of ongoing Emirati efforts focused on influencing Congress and the U.S. Government, including efforts to secure the most advanced U.S. weapons and technology, the Committee directs the Director of National Intelligence (DNI) to produce an unclassified report, if needed with a classified annex, no later than March 1, 2022, detailing the Intelligence Community's (IC) assessment as to whether the UAE's actions and interests are aligned with the United States, including but not limited to the following areas:

1. Stabilizing Libya and supporting the internationally-recognized government;
2. Ending the war in Yemen;
3. Reducing Arab-Israeli tensions and sustainably resolving the Israeli-Palestinian conflict;
4. Promoting and respecting human rights, including prohibitions under international law against torture and the repression of journalists;
5. Containing the spread of Chinese influence as well as the growth of Chinese technological capabilities, including through the theft or unapproved acquisition of U.S. technology;
6. Sustainably combatting international terrorists that pose a confirmed threat to the United States; and
7. Preventing the proliferation of unmanned and autonomous weapons systems.

The DNI shall submit this report to the congressional intelligence committees as well as the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate.

*DNI Reporting on the Declassification and Public Release of Documents Related to the September 11 Terrorist Attacks*

The Committee supports the President's decision to order a declassification review of documents related to the September 11 terrorist attacks, including previously classified documents related to Saudi Arabia's involvement. The Committee has long pressed, on a bipartisan basis, for the release of this information and the passage of time has mitigated concerns over sources and methods. As such, the Committee is strongly committed to closely overseeing the declassification process to ensure that all Intelligence Community elements adhere to the President's guidance to apply the maximum degree of transparency allowed by law when conducting the review and encourages the Director of National Intelligence (DNI) to expeditiously complete the classification process and public release of these documents.

To advance its ongoing oversight, the Committee directs the DNI to produce to the congressional intelligence committees, within 30 days of the enactment of this Act and no later than January 15, 2022, a report containing the following elements: (1) a schedule for expeditiously completing the declassification process and public release of these documents; and (2) a written explanation of the processes and procedures that will govern the review and declassification of documents, to include the processes that the DNI will utilize to arbitrate any disagreements between elements. In addition, if there is any instance in which documents cannot be declassified during this process, the Committee directs the DNI to provide a written justification to the congressional intelligence committees as to why it cannot declassify such documents.

*Cyber Notification Requirements*

The Intelligence Community (IC) is a high priority target for foreign cyber actors. The private companies who contract with the IC on technical, analytic, or other types of support are similarly at risk, but often lack requirements for notifying the U.S. Government, including Congress, of a breach. Identifying, assessing, and sharing information related to a cyber-attack is critical to stopping a more widespread attack and protecting U.S. national security.

Therefore, the Committee directs the Director of National Intelligence (DNI), in coordination with relevant elements as the DNI deems appropriate, to brief the congressional intelligence committees on the IC's process for identifying, assessing, and disseminating information related to a cyber-attack or intrusion affecting IC contract companies or their networks, including efforts by the relevant elements to share and receive information relating to such attacks with such companies. Further, the Committee directs the DNI to notify the congressional intelligence committees within 10 days of discovering a compromise to any IC contractor's unclassified or classified networks.

*Required Training for IC Personnel*

The Committee recognizes that the Federal Government's ability to maintain safe and respectful workplaces is essential to the recruitment and retention of personnel. Anti-harassment and anti-discrimination training that is clear and accessible can ensure that employees are aware of their rights and responsibilities, and can foster more inclusive workplaces.

Therefore, the Committee encourages elements of the Intelligence Community to implement mandatory anti-harassment and anti-discrimination training for supervisors and non-supervisors, as well as bystander intervention training and executive leadership training related to harassment, discrimination, and related retaliation. Such training should follow best practices in the field, as studied by the Equal Employment Opportunity Commission's Select Task Force on the Study of Harassment in the Workplace. The Committee further directs the Director of National Intelligence to provide a report to the congressional intelligence committees on these efforts by no later than June 30, 2022.

*Prevalence of Nondisclosure Clauses Related to Harassment, Discrimination and Related Retaliation*

The Committee recognizes that nondisclosure agreements related to experiences of workplace harassment, discrimination, and related retaliation may interfere with the Federal Government's ability to maintain safe and respectful workplaces and attract and retain personnel by deterring victims from coming forward to participate in future investigations, shielding perpetrators from reputational harm and accountability, and leaving victims confused about their legal rights and vulnerability to legal action. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (P.L. 116–283) recognized the potential negative impact of nondisclosure agreements by barring such agreements if they prohibit or restrict federal employees or applicants for employment from disclosing to Congress, the Special Counsel, the Inspector General of an agency, or any other agency component responsible for internal investigation or review, any information that relates to any violation of any law, rule, regulation, mismanagement, a gross waste of funds, an abuse of authority, a substantial and specific danger to public health or safety, or any other whistleblower protection.

Therefore, the Committee directs the Director of National Intelligence (DNI), in consultation with other heads of elements that the DNI deems appropriate, to submit to the congressional intelligence committees by no later than April 29, 2022, an unclassified report on the prevalence of nondisclosure clauses related to experiences of workplace harassment, discrimination, and related retaliation in the Intelligence Community. Such report shall include a comprehensive review of employment contracts, settlements, and other agreements. If such clauses are utilized, the report shall detail in what circumstances those clauses are utilized, the rationale for usage, and any efforts to move away from the use of nondisclosure clauses.

*Strategy for Integration of Gender-Based Issues in Intelligence*

The Women, Peace, and Security Act of 2017 (H.R. 2484 and S. 1141) became Public Law and demonstrates the sense of Congress that the United States must be a global leader in promoting women's participation in conflict prevention, management, and resolution, as well as post-conflict relief and recovery efforts. In addition, studies have found, based on empirical data, that the fate of a nation is inextricably tied to the status of the women within it and that the subordination of women fatally jeopardizes the security and stability of global democracies. Further, it is the sense of this Committee that women are uniquely posed to provide essential and distinct insight, information, and analysis in unstable or potentially violent contexts, and to detect early signs of radicalization and intervene before individuals begin to act with violence, including because women oftentimes are able to access populations and sites that men cannot for the purposes of gathering key intelligence regarding potential threats to stability and security. And, when women are involved in peace processes, resulting agreements are more sustainable, partially due to unique access to wider community groups and the necessity of women to rebuild society within nations. Women's participation can also foster stability, and pre-

vent factors that challenge the effectiveness and implementation of peace agreements, such as corruption.

Therefore, the Committee directs the Director of National Intelligence (DNI), in coordination with the heads of other elements of the Intelligence Community (IC) as the DNI deems appropriate, to submit to the congressional intelligence committee by no later than April 29, 2022, a strategy for integrating gender-based issues and perspectives into intelligence collection, analysis, and tradecraft. Such strategy shall at minimum address the benefits, drawbacks, and feasibility of:

1. Developing a training curriculum, to be made available across the IC, that addresses gender-related issues in intelligence collection, analysis, and tradecraft; and

2. Implementing a requirement that introductory analytic trainings offered by elements of the IC include a module addressing gender-related issues in intelligence collection, analysis, and tradecraft.

*Accessibility in the IC*

Building an inclusive workforce and ensuring that the Intelligence Community (IC) remains a desirable employer for individuals of all backgrounds is a national security imperative. The Committee strongly encourages nascent and ongoing efforts to improve accessibility for persons with disabilities who aspire to join or are currently part of the IC workforce.

Therefore, the Committee directs the Director of National Intelligence (DNI), in consultation with the heads of other elements that the DNI deems appropriate, to submit to the congressional intelligence committees, by no later than April 29, 2022, a report that at minimum:

1. Provides an update on the IC's status and implementation of relevant executive orders, guidelines, and laws, including Executive Order 14035 and ICPG 110.1 ("Employment of Individuals with Disabilities");

2. Documents the number of instances within the past 10 years that an IC element has invoked an exception to:

   a. Sec. 508 of the Rehabilitation Act of 1973, as amended;

   b. The Architectural Barriers Act of 1968; or

   c. Any other law or executive order pertaining to enhancing accessibility for persons with disabilities in the Federal Government;

3. Describes anticipated or current activities or policies of the IC to increase the availability of reasonable accommodations for information technology and accessible workplace facilities for persons with disabilities, including mechanisms for applicants to initiate and track accommodation requests, such as through formalized platforms; and

4. Describes anticipated or current opportunities for the IC to recruit and hire more persons with disabilities, including through the Department of Labor's Workforce Recruitment Program, or through other initiatives that address travel, accommodations, and security clearance concerns during the recruiting and onboarding process.

*DNI Reporting on the Intelligence Community's Compliance with the Freedom of Information Act*

The Committee applauds the Director of National Intelligence's (DNI) commitment to transparency, and believes that compliance with the Freedom of Information Act (FOIA) and the timely and appropriate processing of FOIA requests is a critical part of that commitment. Therefore, the Committee directs the DNI, in coordination with heads of elements of the Intelligence Community (IC) as the DNI deems appropriate, and by no later than June 1, 2022, to submit to the Committee a written report on compliance by IC elements with the FOIA. The report shall contain a detailed list, sorted by element, of:

1. The number of outstanding FOIA requests and how long ago they were filed;
2. The number of instances over the last five years in which the element provided a "Glomar Response" and asserted that it could "neither confirm nor deny" the existence of the records requested under the FOIA;
3. The number, for each of the following categories, of FOIA requests in which the requester initiated legal action in United States District Court in the last five years challenging the element's:
    a. Failure to respond in a timely fashion;
    b. Decision not to release records in whole or in part; and
    c. Adequacy of the search used to locate responsive records.

In addition, the report shall contain specific recommendations for how to enhance the FOIA process and ensure timely responses by IC entities, including the need for additional resources or any other reforms to ensure rigorous and appropriate responses to FOIA requests.

*Metrics for Modern Best Practices in Software Development*

Modern best practices for software development frequently rely on a set of standardized processes known as development, security, and operations (DevSecOps). DevSecOps combine software development and operations, with security integrated throughout every phase of the development lifecycle.

Standardized DevSecOps metrics such as availability, change lead time, and time to Authorization to Operate (ATO), among others, are vitally useful in assessing and understanding software development programs' adherence or deviation from modern best practices. Furthermore, many of these metrics can be collected in an automated fashion, allowing for rapid and frequent scoring of programs that can help predict future success or failure. It is clear to the Committee that different Intelligence Community (IC) elements are evolving to a DevSecOps approach at different rates.

Therefore, the Committee directs the Intelligence Community Chief Information Officer to submit to the congressional intelligence committees, by no later than May 31, 2022, a written report exploring adherence to modern best practices of software development programs throughout the IC. The report shall include, at a minimum:

1. Identification of the relevant metrics for programs' adherence to modern DevSecOps practices;
2. Identifications of programs and elements that struggle with best practices, and recommendations to migrate them towards best practices;
3. A plan to standardize automation of metrics across the IC; and
4. A discussion of any barriers preventing the adoption of DevSecOps practices throughout the IC.

*Intelligence Collection Prioritization on Advanced Technologies of Adversaries*

The Committee recognizes that strategic competitors and adversaries of the United States are innovating rapidly to develop and exploit technology-enabled tools that may harm the United States and allies of the United States. The Committee is concerned that the Defense Intelligence Enterprise (DIE) has not adequately prioritized collection of these emerging scientific and technical developments. The Committee believes the DIE must prioritize collection of emerging technologies of strategic competitors and adversaries of the United States to better understand those capabilities and intentions.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence and Security to provide a briefing to the congressional intelligence committees no later than March 15, 2022, on steps taken within the DIE to prioritize collection of emerging technologies being pursued by strategic competitors and adversaries of the United States, including developments in biotechnology, artificial intelligence and machine learning, lethal autonomous weapons, hypersonic weapons, and directed energy weapons.

*Department of Defense transformation through Project GAMECHANGER*

The Committee awaits complete implementation of the congressional intelligence and defense committees' direction contained in Section 1626 of the National Defense Authorization Act for Fiscal Year 2018 (P.L. 115–91). Core to the congressional intent for Section 1626 was first, the creation of a framework to more effectively manage elements of the Intelligence Community (IC), which are also Combat Support Agencies, and second, the reconciliation of variances in the definitions used by the Department and/or IC and clear codification of those terms.

The Committee supported the Department's creation of project GAMECHANGER as one of the ways to effectively answer Section 1626's direction. Further, the Committee supports the Department's continued maturation of the GAMECHANGER technology. This unique defense innovation effort will transform the way the Department sets policy, updates doctrine, and manages critical guidance documents. It is imperative that the GAMECHANGER technology be managed properly, effectively scaled, and transitioned to programs of record.

Therefore, the Committee directs the Undersecretary of Defense for Intelligence and Security and the Director of the Joint Artificial Intelligence Center, in consultation with the Chief Data Officer and Comptroller, to provide a briefing to the Committee no later than

February 4, 2022, on the current usage inside the Department of GAMECHANGER, as well as an approved plan of action and milestones to transition GAMECHANGER to a program of record by the Fiscal Year 2024 budget request.

*Office of the Undersecretary for Defense Intelligence and Security Oversight and Structure*

The Government Accountability Office (GAO) report entitled, "Defense Intelligence and Security: DoD Needs to Establish Oversight Expectations and to Develop Tools that Enhance Accountability" (GAO–21–295), raised certain issues about the ways the Office of the Under Secretary of Defense for Intelligence & Security (OUSD(I&S)) provides oversight and ensures accountability of the Defense Intelligence Enterprise (DIE) and the Defense Security Enterprise (DSE).

The report contained two recommendations. First, that the Secretary of Defense should ensure that the USD(I&S) establishes clear expectations for oversight, including refining business rules for governance bodies and clarifying key oversight terms. Second, that the Secretary of Defense should ensure that the USD(I&S) develops tools to enhance accountability—such as through strategies or other mechanisms with identified goals, desired outcomes, and performance metrics—for specific intelligence and security mission areas and use these tools to conduct oversight. The Department concurred with both recommendations.

The Committee appreciates USD(I&S)' acknowledgment of and work to address these recommendations, including an independent review of authorities and responsibilities assigned by statute and policy recommendations for organization staffing, optimum assignments of existing staffing, and other alignment of Roles and Missions—a longstanding interest item for the Committee. However, the Committee is concerned that, like certain recommendations from the 2018 USDI Roles and Missions study, certain actions will stall and fail to be fully implemented.

Therefore, the Committee directs the USD(I&S) to provide updates to the implementation of the GAO recommendations to the Committee on a quarterly basis. Further, the Committee understands that the review conducted by the Institute for Defense Analyses (IDA) is due no later than September 1, 2022. The Committee directs that USD(I&S) present a plan of action and milestones for implementation of accepted recommendations, to include those resulting from the IDA analysis, no later than December 1, 2022, and that the accepted recommendations be fully implemented no later than October 1, 2023.

*Hypersonic Aircraft*

The Committee is encouraged by recent efforts to mature the technologies necessary to develop high Mach and hypersonic aircraft. The Committee is also aware of ongoing investments by the Department of Defense (DoD) and private industry to develop high Mach flight for both defense and commercial applications. The Committee believes the Intelligence Community (IC) must ensure it is postured to leverage the development of hypersonic flight systems for intelligence related mission requirements.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence and Security, the Under Secretary of Defense for Research and Engineering, and the Director of National Intelligence (DNI) to jointly brief the congressional intelligence committees on their efforts to incorporate hypersonic flight research and development into the Fiscal Year 2023 budget request no later than March 31, 2022.

The Committee further directs the Under Secretary of Defense for Research and Engineering and the DNI, in coordination with the Under Secretary of Defense for Intelligence and Security, to provide the congressional intelligence committees a report no later than June 1, 2022, on the utility of establishing a joint DoD–IC program office to coordinate activities related to high Mach and hypersonic aircraft development programs. This report will include at a minimum:

1. A recommended timeline for establishing a joint program office;
2. An overview of how a program office will develop program requirements in consultation with the user community;
3. An overview of the remaining engineering challenges associated with producing high Mach and hypersonic aircraft; and
4. An assessment of the personnel, training, and logistical support requirements high Mach and hypersonic aircraft will generate.

*DIA Workforce Issues*

The Committee is concerned about the inherent isolation required of intelligence professionals and the lack of external resources or support due to the sensitive nature of their work. An additional challenge is the effects of COVID–19 on the workforce, including the added stress of crisis operations and shiftwork, which may exacerbate any underlying negative or challenging management culture or working environments.

The Committee applauds the Defense Intelligence Agency (DIA) for creating the Office of the Surgeon General and for internally realigning personnel, programs, and funding to consolidate existing medical, behavioral health, and wellness professionals under a single organization. The Committee strongly supports efforts to streamline workforce support mechanisms across DIA's therapeutic and medical services, particularly the renewed focus on mental health. However, continuing to collect, monitor, and respond to regular data and feedback will be critical to ensuring the health of current personnel and the creation or sustainment of programs to retain a talented, diverse workforce.

Therefore, the Committee directs DIA to notify the Committee within 10 days of the launch of any agency, Directorate, or Career Field annual or ad hoc workforce engagement or climate surveys, including the topic, rationale, accessibility, lead subject office or work unit, and timeframe. The Committee also directs the DIA, within 30 days of completion of such survey, to provide an initial summary of the results of such surveys, for example, participation rates and demographics, with full results made available to the Committee within 90 days of completion of the survey. Further, the Committee directs DIA to provide a briefing, by March 1, 2022, on

plans to ensure such surveys are available on both classified and unclassified systems and that exit surveys or exit interviews with the Office of the Ombuds are mandatory for all departing or permanently separating employees.

Additionally, the Committee directs DIA to provide a report, by September 30, 2022, on the data from the Office of the Ombuds, Equal Employment Opportunity Office (EEO), Employee Management Relations, and any other employee resource for seeking help with a perceived hostile work environment, reprisal, harassment, or abuse of authority. This report should include the total number of consultations related to a supervisor, chain of command, or management culture, the nature of the complaint, whether or not the complaint resulted in a formal EEO or Inspector General review or report, the consulting office's recommendations to the supervisory chain or the office in question, and the management actions taken in response. DIA should provide a briefing on the initial results of this study and any challenges in implementation by March 30, 2022.

Finally, the Committee directs DIA to provide a briefing, by February 14, 2022, on the mechanism by which supervisors receive feedback, including from peers and subordinates, on their ability to create and maintain a healthy and supportive workplace environment either as part of annual performance reviews or through regular training, development, or coaching, and the feasibility of conducting 360-degree performance reviews.

*Congressional Applicant Referrals for the Defense Intelligence Agency*

Members of Congress receive hundreds of applications for United States Military Academies every year. However, with only two slots allowed per Member, a significant number of highly qualified, motivated young Americans must look elsewhere for their education, and for the opportunity to serve their country. Many of these talented students go on to join the military through other avenues, but a large number would be ideally suited to careers as civilian intelligence officers and may be unaware of the opportunities that exist. Further, the geographic diversity represented by these candidates could add critical insight into the Defense Intelligence Agency (DIA) officer corps and further strengthen DIA's representation of American communities.

DIA provides internship and scholarship opportunities for undergraduate and graduate students to gain valuable national security work experience and an opportunity to serve their country. For many, this experience leads to a full-time career with DIA or an Intelligence Community partner after graduation.

Therefore, the Committee directs DIA to provide, by January 31, 2022, information about DIA student and internship programs so that those candidates not selected for a Military Academy appointment may receive details about available DIA programs, application requirements, and application deadlines. This information shall be provided to Members' personal offices to be made available to prospective student applicants.

*NSA's Cyber Collaboration Center and Cyber Deterrence*

The Committee supports the National Security Agency's (NSA) establishment of the Cyber Collaboration Center to provide greater information sharing between government and private industry. The Committee recognizes that cybersecurity is a national problem that benefits uniquely from private sector insights.

Therefore, the Committee directs the Director of NSA, by no later than May 2, 2022, to submit to the Committee a written description of how the Cyber Collaboration Center works with the Cybersecurity and Infrastructure Security Agency (CISA) to disseminate cyber threat information and what, if any, overlap exists between NSA and CISA with regard to collaboration with private industry.

## CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

# NATIONAL SECURITY ACT OF 1947

### SHORT TITLE

That this Act may be cited as the "National Security Act of 1947".

### TABLE OF CONTENTS

* * * * * * *

TITLE I—COORDINATION FOR NATIONAL SECURITY

* * * * * * *

*Sec. 116A. Authority for transportation of certain canines associated with force protection duties of intelligence community.*

* * * * * * *

Sec. 119A. National [Counter Proliferation] *Counterproliferation and Biosecurity* Center.

* * * * * * *

TITLE III—MISCELLANEOUS

* * * * * * *

[Sec. 304. Reporting of certain employment activities by former intelligence officers and employees.]

*Sec. 304. Requirements for certain employment activities by former intelligence officers and employees.*

*Sec. 305. Temporary authority for paid leave for a serious health condition.*

* * * * * * *

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

* * * * * * *

*Sec. 501A. Congressional oversight of certain special access programs.*

* * * * * * *

TITLE X—EDUCATION IN SUPPORT OF NATIONAL INTELLIGENCE

* * * * * * *

## TITLE I—COORDINATION FOR NATIONAL SECURITY

* * * * * * *

### RESPONSIBILITIES AND AUTHORITIES OF THE DIRECTOR OF NATIONAL INTELLIGENCE

SEC. 102A. (a) PROVISION OF INTELLIGENCE.—(1) The Director of National Intelligence shall be responsible for ensuring that national intelligence is provided—

(A) to the President;

(B) to the heads of departments and agencies of the executive branch;

(C) to the Chairman of the Joint Chiefs of Staff and senior military commanders;

(D) to the Senate and House of Representatives and the committees thereof; and

(E) to such other persons as the Director of National Intelligence determines to be appropriate.

(2) Such national intelligence should be timely, objective, independent of political considerations, and based upon all sources available to the intelligence community and other appropriate entities.

(b) ACCESS TO INTELLIGENCE.—Unless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any Federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence.

(c) BUDGET AUTHORITIES.—(1) With respect to budget requests and appropriations for the National Intelligence Program, the Director of National Intelligence shall—

(A) based on intelligence priorities set by the President, provide to the heads of departments containing agencies or organizations within the intelligence community, and to the heads of such agencies and organizations, guidance for developing the National Intelligence Program budget pertaining to such agencies and organizations;

(B) based on budget proposals provided to the Director of National Intelligence by the heads of agencies and organizations within the intelligence community and the heads of their respective departments and, as appropriate, after obtaining the

advice of the Joint Intelligence Community Council, develop and determine an annual consolidated National Intelligence Program budget; and

(C) present such consolidated National Intelligence Program budget, together with any comments from the heads of departments containing agencies or organizations within the intelligence community, to the President for approval.

(2) In addition to the information provided under paragraph (1)(B), the heads of agencies and organizations within the intelligence community shall provide the Director of National Intelligence such other information as the Director shall request for the purpose of determining the annual consolidated National Intelligence Program budget under that paragraph.

(3)(A) The Director of National Intelligence shall participate in the development by the Secretary of Defense of the annual budget for the Military Intelligence Program or any successor program or programs.

(B) The Director of National Intelligence shall provide guidance for the development of the annual budget for each element of the intelligence community that is not within the National Intelligence Program.

(4) The Director of National Intelligence shall ensure the effective execution of the annual budget for intelligence and intelligence-related activities.

(5)(A) The Director of National Intelligence shall be responsible for managing appropriations for the National Intelligence Program by directing the allotment or allocation of such appropriations through the heads of the departments containing agencies or organizations within the intelligence community and the Director of the Central Intelligence Agency, with prior notice (including the provision of appropriate supporting information) to the head of the department containing an agency or organization receiving any such allocation or allotment or the Director of the Central Intelligence Agency.

(B) Notwithstanding any other provision of law, pursuant to relevant appropriations Acts for the National Intelligence Program, the Director of the Office of Management and Budget shall exercise the authority of the Director of the Office of Management and Budget to apportion funds, at the exclusive direction of the Director of National Intelligence, for allocation to the elements of the intelligence community through the relevant host executive departments and the Central Intelligence Agency. Department comptrollers or appropriate budget execution officers shall allot, allocate, reprogram, or transfer funds appropriated for the National Intelligence Program in an expeditious manner.

(C) The Director of National Intelligence shall monitor the implementation and execution of the National Intelligence Program by the heads of the elements of the intelligence community that manage programs and activities that are part of the National Intelligence Program, which may include audits and evaluations.

(6) Apportionment and allotment of funds under this subsection shall be subject to chapter 13 and section 1517 of title 31, United States Code, and the Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. 621 et seq.).

(7)(A) The Director of National Intelligence shall provide a semiannual report, beginning April 1, 2005, and ending April 1, 2007, to the President and the Congress regarding implementation of this section.

(B) The Director of National Intelligence shall report to the President and the Congress not later than 15 days after learning of any instance in which a departmental comptroller acts in a manner inconsistent with the law (including permanent statutes, authorization Acts, and appropriations Acts), or the direction of the Director of National Intelligence, in carrying out the National Intelligence Program.

(d) ROLE OF DIRECTOR OF NATIONAL INTELLIGENCE IN TRANSFER AND REPROGRAMMING OF FUNDS.—(1)(A) No funds made available under the National Intelligence Program may be transferred or reprogrammed without the prior approval of the Director of National Intelligence, except in accordance with procedures prescribed by the Director of National Intelligence.

(B) The Secretary of Defense shall consult with the Director of National Intelligence before transferring or reprogramming funds made available under the Military Intelligence Program or any successor program or programs.

(2) Subject to the succeeding provisions of this subsection, the Director of National Intelligence may transfer or reprogram funds appropriated for a program within the National Intelligence Program—

(A) to another such program;

(B) to other departments or agencies of the United States Government for the development and fielding of systems of common concern related to the collection, processing, analysis, exploitation, and dissemination of intelligence information; or

(C) to a program funded by appropriations not within the National Intelligence Program to address critical gaps in intelligence information sharing or access capabilities.

(3) The Director of National Intelligence may only transfer or reprogram funds referred to in paragraph (1)(A)—

(A) with the approval of the Director of the Office of Management and Budget; and

(B) after consultation with the heads of departments containing agencies or organizations within the intelligence community to the extent such agencies or organizations are affected, and, in the case of the Central Intelligence Agency, after consultation with the Director of the Central Intelligence Agency.

(4) The amounts available for transfer or reprogramming in the National Intelligence Program in any given fiscal year, and the terms and conditions governing such transfers and reprogrammings, are subject to the provisions of annual appropriations Acts and this subsection.

(5)(A) A transfer or reprogramming of funds may be made under this subsection only if—

(i) the funds are being transferred to an activity that is a higher priority intelligence activity;

(ii) the transfer or reprogramming supports an emergent need, improves program effectiveness, or increases efficiency;

(iii) the transfer or reprogramming does not involve a transfer or reprogramming of funds to a Reserve for Contingencies of the Director of National Intelligence or the Reserve for Contingencies of the Central Intelligence Agency;

(iv) the transfer or reprogramming results in a cumulative transfer or reprogramming of funds out of any department or agency, as appropriate, funded in the National Intelligence Program in a single fiscal year—

(I) that is less than $150,000,000, and

(II) that is less than 5 percent of amounts available to a department or agency under the National Intelligence Program; and

(v) the transfer or reprogramming does not terminate an acquisition program.

(B) A transfer or reprogramming may be made without regard to a limitation set forth in clause (iv) or (v) of subparagraph (A) if the transfer has the concurrence of the head of the department involved or the Director of the Central Intelligence Agency (in the case of the Central Intelligence Agency). The authority to provide such concurrence may only be delegated by the head of the department involved or the Director of the Central Intelligence Agency (in the case of the Central Intelligence Agency) to the deputy of such officer.

(6) Funds transferred or reprogrammed under this subsection shall remain available for the same period as the appropriations account to which transferred or reprogrammed.

(7) Any transfer or reprogramming of funds under this subsection shall be carried out in accordance with existing procedures applicable to reprogramming notifications for the appropriate congressional committees. Any proposed transfer or reprogramming for which notice is given to the appropriate congressional committees shall be accompanied by a report explaining the nature of the proposed transfer or reprogramming and how it satisfies the requirements of this subsection. In addition, the congressional intelligence committees shall be promptly notified of any transfer or reprogramming of funds made pursuant to this subsection in any case in which the transfer or reprogramming would not have otherwise required reprogramming notification under procedures in effect as of the date of the enactment of this subsection.

(e) TRANSFER OF PERSONNEL.—(1)(A) In addition to any other authorities available under law for such purposes, in the first twelve months after establishment of a new national intelligence center, the Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in consultation with the congressional committees of jurisdiction referred to in subparagraph (B), may transfer not more than 100 personnel authorized for elements of the intelligence community to such center.

(B) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

(i) the congressional intelligence committees;

(ii) the Committees on Appropriations of the Senate and the House of Representatives;

(iii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and

(iv) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

(C) The Director shall include in any notice under subparagraph (B) an explanation of the nature of the transfer and how it satisfies the requirements of this subsection.

(2)(A) The Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in accordance with procedures to be developed by the Director of National Intelligence and the heads of the departments and agencies concerned, may transfer personnel authorized for an element of the intelligence community to another such element for a period of not more than 2 years.

(B) A transfer of personnel may be made under this paragraph only if—

(i) the personnel are being transferred to an activity that is a higher priority intelligence activity; and

(ii) the transfer supports an emergent need, improves program effectiveness, or increases efficiency.

(C) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

(i) the congressional intelligence committees;

(ii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and

(iii) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

(D) The Director shall include in any notice under subparagraph (C) an explanation of the nature of the transfer and how it satisfies the requirements of this paragraph.

(3)(A) In addition to the number of full-time equivalent positions authorized for the Office of the Director of National Intelligence for a fiscal year, there is authorized for such Office for each fiscal year an additional 100 full-time equivalent positions that may be used only for the purposes described in subparagraph (B).

(B) Except as provided in subparagraph (C), the Director of National Intelligence may use a full-time equivalent position authorized under subparagraph (A) only for the purpose of providing a temporary transfer of personnel made in accordance with paragraph (2) to an element of the intelligence community to enable such element to increase the total number of personnel authorized for such element, on a temporary basis—

(i) during a period in which a permanent employee of such element is absent to participate in critical language training; or

(ii) to accept a permanent employee of another element of the intelligence community to provide language-capable services.

(C) Paragraph (2)(B) shall not apply with respect to a transfer of personnel made under subparagraph (B).

(D) For each of the fiscal years 2010, 2011, and 2012, the Director of National Intelligence shall submit to the congressional intelligence committees an annual report on the use of authorities under this paragraph. Each such report shall include a description of—

(i) the number of transfers of personnel made by the Director pursuant to subparagraph (B), disaggregated by each element of the intelligence community;

(ii) the critical language needs that were fulfilled or partially fulfilled through the use of such transfers; and

(iii) the cost to carry out subparagraph (B).

(4) It is the sense of Congress that—

(A) the nature of the national security threats facing the United States will continue to challenge the intelligence community to respond rapidly and flexibly to bring analytic resources to bear against emerging and unforeseen requirements;

(B) both the Office of the Director of National Intelligence and any analytic centers determined to be necessary should be fully and properly supported with appropriate levels of personnel resources and that the President's yearly budget requests adequately support those needs; and

(C) the President should utilize all legal and administrative discretion to ensure that the Director of National Intelligence and all other elements of the intelligence community have the necessary resources and procedures to respond promptly and effectively to emerging and unforeseen national security challenges.

(f) TASKING AND OTHER AUTHORITIES.—(1)(A) The Director of National Intelligence shall—

(i) establish objectives, priorities, and guidance for the intelligence community to ensure timely and effective collection, processing, analysis, and dissemination (including access by users to collected data consistent with applicable law and, as appropriate, the guidelines referred to in subsection (b) and analytic products generated by or within the intelligence community) of national intelligence;

(ii) determine requirements and priorities for, and manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community, including—

(I) approving requirements (including those requirements responding to needs provided by consumers) for collection and analysis; and

(II) resolving conflicts in collection requirements and in the tasking of national collection assets of the elements of the intelligence community; and

(iii) provide advisory tasking to intelligence elements of those agencies and departments not within the National Intelligence Program.

(B) The authority of the Director of National Intelligence under subparagraph (A) shall not apply—

(i) insofar as the President so directs;

(ii) with respect to clause (ii) of subparagraph (A), insofar as the Secretary of Defense exercises tasking authority under

plans or arrangements agreed upon by the Secretary of Defense and the Director of National Intelligence; or

(iii) to the direct dissemination of information to State government and local government officials and private sector entities pursuant to sections 201 and 892 of the Homeland Security Act of 2002 (6 U.S.C. 121, 482).

(2) The Director of National Intelligence shall oversee the National Counterterrorism Center, the National Counterproliferation Center, and the National Counterintelligence and Security Center and may establish such other national intelligence centers as the Director determines necessary.

(3)(A) The Director of National Intelligence shall prescribe, in consultation with the heads of other agencies or elements of the intelligence community, and the heads of their respective departments, personnel policies and programs applicable to the intelligence community that—

(i) encourage and facilitate assignments and details of personnel to national intelligence centers, and between elements of the intelligence community;

(ii) set standards for education, training, and career development of personnel of the intelligence community;

(iii) encourage and facilitate the recruitment and retention by the intelligence community of highly qualified individuals for the effective conduct of intelligence activities;

(iv) ensure that the personnel of the intelligence community are sufficiently diverse for purposes of the collection and analysis of intelligence through the recruitment and training of women, minorities, and individuals with diverse ethnic, cultural, and linguistic backgrounds;

(v) make service in more than one element of the intelligence community a condition of promotion to such positions within the intelligence community as the Director shall specify; and

(vi) ensure the effective management of intelligence community personnel who are responsible for intelligence community-wide matters.

(B) Policies prescribed under subparagraph (A) shall not be inconsistent with the personnel policies otherwise applicable to members of the uniformed services.

(4) The Director of National Intelligence shall ensure compliance with the Constitution and laws of the United States by the Central Intelligence Agency and shall ensure such compliance by other elements of the intelligence community through the host executive departments that manage the programs and activities that are part of the National Intelligence Program.

(5) The Director of National Intelligence shall ensure the elimination of waste and unnecessary duplication within the intelligence community.

(6) The Director of National Intelligence shall establish requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for national intelligence purposes, except that the Director shall have no authority to direct or under-

take electronic surveillance or physical search operations pursuant to that Act unless authorized by statute or Executive order.

(7)(A) The Director of National Intelligence shall, if the Director determines it is necessary, or may, if requested by a congressional intelligence committee, conduct an accountability review of an element of the intelligence community or the personnel of such element in relation to a failure or deficiency within the intelligence community.

(B) The Director of National Intelligence, in consultation with the Attorney General, shall establish guidelines and procedures for conducting an accountability review under subparagraph (A).

(C)(i) The Director of National Intelligence shall provide the findings of an accountability review conducted under subparagraph (A) and the Director's recommendations for corrective or punitive action, if any, to the head of the applicable element of the intelligence community. Such recommendations may include a recommendation for dismissal of personnel.

(ii) If the head of such element does not implement a recommendation made by the Director under clause (i), the head of such element shall submit to the congressional intelligence committees a notice of the determination not to implement the recommendation, including the reasons for the determination.

(D) The requirements of this paragraph shall not be construed to limit any authority of the Director of National Intelligence under subsection (m) or with respect to supervision of the Central Intelligence Agency.

(8) The Director of National Intelligence shall perform [such other functions] *such other intelligence-related functions* as the President may direct.

(9) Nothing in this title shall be construed as affecting the role of the Department of Justice or the Attorney General under the Foreign Intelligence Surveillance Act of 1978.

(g) INTELLIGENCE INFORMATION SHARING.—(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

(A) establish uniform security standards and procedures;

(B) establish common information technology standards, protocols, and interfaces;

(C) ensure development of information technology systems that include multi-level security and intelligence integration capabilities;

(D) establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;

(E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture;

(F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program; and

(G) in accordance with Executive Order No. 13526 (75 Fed. Reg. 707; relating to classified national security information) (or any subsequent corresponding executive order), and part

2001 of title 32, Code of Federal Regulations (or any subsequent corresponding regulation), establish—

(i) guidance to standardize, in appropriate cases, the formats for classified and unclassified intelligence products created by elements of the intelligence community for purposes of promoting the sharing of intelligence products; and

(ii) policies and procedures requiring the increased use, in appropriate cases, and including portion markings, of the classification of portions of information within one intelligence product.

(2) The President shall ensure that the Director of National Intelligence has all necessary support and authorities to fully and effectively implement paragraph (1).

(3) Except as otherwise directed by the President or with the specific written agreement of the head of the department or agency in question, a Federal agency or official shall not be considered to have met any obligation to provide any information, report, assessment, or other material (including unevaluated intelligence information) to that department or agency solely by virtue of having provided that information, report, assessment, or other material to the Director of National Intelligence or the National Counterterrorism Center.

(4) The Director of National Intelligence shall, in a timely manner, report to Congress any statute, regulation, policy, or practice that the Director believes impedes the ability of the Director to fully and effectively ensure maximum availability of access to intelligence information within the intelligence community consistent with the protection of the national security of the United States.

(h) ANALYSIS.—To ensure the most accurate analysis of intelligence is derived from all sources to support national security needs, the Director of National Intelligence shall—

(1) implement policies and procedures—

(A) to encourage sound analytic methods and tradecraft throughout the elements of the intelligence community;

(B) to ensure that analysis is based upon all sources available; and

(C) to ensure that the elements of the intelligence community regularly conduct competitive analysis of analytic products, whether such products are produced by or disseminated to such elements;

(2) ensure that resource allocation for intelligence analysis is appropriately proportional to resource allocation for intelligence collection systems and operations in order to maximize analysis of all collected data;

(3) ensure that differences in analytic judgment are fully considered and brought to the attention of policymakers; and

(4) ensure that sufficient relationships are established between intelligence collectors and analysts to facilitate greater understanding of the needs of analysts.

(i) PROTECTION OF INTELLIGENCE SOURCES AND METHODS.—(1) The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.

(2) Consistent with paragraph (1), in order to maximize the dissemination of intelligence, the Director of National Intelligence

shall establish and implement guidelines for the intelligence community for the following purposes:

(A) Classification of information under applicable law, Executive orders, or other Presidential directives.

(B) Access to and dissemination of intelligence, both in final form and in the form when initially gathered.

(C) Preparation of intelligence products in such a way that source information is removed to allow for dissemination at the lowest level of classification possible or in unclassified form to the extent practicable.

(3) The Director may only delegate a duty or authority given the Director under this subsection to the Principal Deputy Director of National Intelligence.

(j) UNIFORM PROCEDURES FOR CLASSIFIED INFORMATION.—The Director of National Intelligence, subject to the direction of the President, shall—

(1) establish uniform standards and procedures for the grant of access to sensitive compartmented information to any officer or employee of any agency or department of the United States and to employees of contractors of those agencies or departments;

(2) ensure the consistent implementation of those standards and procedures throughout such agencies and departments;

(3) ensure that security clearances granted by individual elements of the intelligence community are recognized by all elements of the intelligence community, and under contracts entered into by those agencies;

(4) ensure that the process for investigation and adjudication of an application for access to sensitive compartmented information is performed in the most expeditious manner possible consistent with applicable standards for national security;

(5) ensure that the background of each employee or officer of an element of the intelligence community, each contractor to an element of the intelligence community, and each individual employee of such a contractor who has been determined to be eligible for access to classified information is monitored on a continual basis under standards developed by the Director, including with respect to the frequency of evaluation, during the period of eligibility of such employee or officer of an element of the intelligence community, such contractor, or such individual employee to such a contractor to determine whether such employee or officer of an element of the intelligence community, such contractor, and such individual employee of such a contractor continues to meet the requirements for eligibility for access to classified information; and

(6) develop procedures to require information sharing between elements of the intelligence community concerning potentially derogatory security information regarding an employee or officer of an element of the intelligence community, a contractor to an element of the intelligence community, or an individual employee of such a contractor that may impact the eligibility of such employee or officer of an element of the intelligence community, such contractor, or such individual employee of such a contractor for a security clearance.

(k) COORDINATION WITH FOREIGN GOVERNMENTS.—Under the direction of the President and in a manner consistent with section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), the Director of National Intelligence shall oversee the coordination of the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

(l) ENHANCED PERSONNEL MANAGEMENT.—(1)(A) The Director of National Intelligence shall, under regulations prescribed by the Director, provide incentives for personnel of elements of the intelligence community to serve—

(i) on the staff of the Director of National Intelligence;

(ii) on the staff of the national intelligence centers;

(iii) on the staff of the National Counterterrorism Center; and

(iv) in other positions in support of the intelligence community management functions of the Director.

(B) Incentives under subparagraph (A) may include financial incentives, bonuses, and such other awards and incentives as the Director considers appropriate.

(2)(A) Notwithstanding any other provision of law, the personnel of an element of the intelligence community who are assigned or detailed under paragraph (1)(A) to service under the Director of National Intelligence shall be promoted at rates equivalent to or better than personnel of such element who are not so assigned or detailed.

(B) The Director may prescribe regulations to carry out this paragraph.

(3)(A) The Director of National Intelligence shall prescribe mechanisms to facilitate the rotation of personnel of the intelligence community through various elements of the intelligence community in the course of their careers in order to facilitate the widest possible understanding by such personnel of the variety of intelligence requirements, methods, users, and capabilities.

(B) The mechanisms prescribed under subparagraph (A) may include the following:

(i) The establishment of special occupational categories involving service, over the course of a career, in more than one element of the intelligence community.

(ii) The provision of rewards for service in positions undertaking analysis and planning of operations involving two or more elements of the intelligence community.

(iii) The establishment of requirements for education, training, service, and evaluation for service involving more than one element of the intelligence community.

(C) It is the sense of Congress that the mechanisms prescribed under this subsection should, to the extent practical, seek to duplicate for civilian personnel within the intelligence community the joint officer management policies established by chapter 38 of title 10, United States Code, and the other amendments made by title IV of the Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99–433).

(D) The mechanisms prescribed under subparagraph (A) and any other policies of the Director—

(i) may not require an employee of an office of inspector general for an element of the intelligence community, including the Office of the Inspector General of the Intelligence Community, to rotate to a position in an office or organization of such an element over which such office of inspector general exercises jurisdiction; and

(ii) shall be implemented in a manner that exempts employees of an office of inspector general from a rotation that may impact the independence of such office.

(4)(A) Except as provided in subparagraph (B) and subparagraph (D), this subsection shall not apply with respect to personnel of the elements of the intelligence community who are members of the uniformed services.

(B) Mechanisms that establish requirements for education and training pursuant to paragraph (3)(B)(iii) may apply with respect to members of the uniformed services who are assigned to an element of the intelligence community funded through the National Intelligence Program, but such mechanisms shall not be inconsistent with personnel policies and education and training requirements otherwise applicable to members of the uniformed services.

(C) The personnel policies and programs developed and implemented under this subsection with respect to law enforcement officers (as that term is defined in section 5541(3) of title 5, United States Code) shall not affect the ability of law enforcement entities to conduct operations or, through the applicable chain of command, to control the activities of such law enforcement officers.

(D) Assignment to the Office of the Director of National Intelligence of commissioned officers of the Armed Forces shall be considered a joint-duty assignment for purposes of the joint officer management policies prescribed by chapter 38 of title 10, United States Code, and other provisions of that title.

(m) ADDITIONAL AUTHORITY WITH RESPECT TO PERSONNEL.—(1) In addition to the authorities under subsection (f)(3), the Director of National Intelligence may exercise with respect to the personnel of the Office of the Director of National Intelligence any authority of the Director of the Central Intelligence Agency with respect to the personnel of the Central Intelligence Agency under the Central Intelligence Agency Act of 1949 (50 U.S.C. 403a et seq.), and other applicable provisions of law, as of the date of the enactment of this subsection to the same extent, and subject to the same conditions and limitations, that the Director of the Central Intelligence Agency may exercise such authority with respect to personnel of the Central Intelligence Agency.

(2) Employees and applicants for employment of the Office of the Director of National Intelligence shall have the same rights and protections under the Office of the Director of National Intelligence as employees of the Central Intelligence Agency have under the Central Intelligence Agency Act of 1949, and other applicable provisions of law, as of the date of the enactment of this subsection.

(n) ACQUISITION AND OTHER AUTHORITIES.—(1) In carrying out the responsibilities and authorities under this section, the Director of National Intelligence may exercise the acquisition and appropriations authorities referred to in the Central Intelligence Agency

Act of 1949 (50 U.S.C. 403a et seq.) other than the authorities referred to in section 8(b) of that Act (50 U.S.C. 403j(b)).

(2) For the purpose of the exercise of any authority referred to in paragraph (1), a reference to the head of an agency shall be deemed to be a reference to the Director of National Intelligence or the Principal Deputy Director of National Intelligence.

(3)(A) Any determination or decision to be made under an authority referred to in paragraph (1) by the head of an agency may be made with respect to individual purchases and contracts or with respect to classes of purchases or contracts, and shall be final.

(B) Except as provided in subparagraph (C), the Director of National Intelligence or the Principal Deputy Director of National Intelligence may, in such official's discretion, delegate to any officer or other official of the Office of the Director of National Intelligence any authority to make a determination or decision as the head of the agency under an authority referred to in paragraph (1).

(C) The limitations and conditions set forth in section 3(d) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403c(d)) shall apply to the exercise by the Director of National Intelligence of an authority referred to in paragraph (1).

(D) Each determination or decision required by an authority referred to in the second sentence of section 3(d) of the Central Intelligence Agency Act of 1949 shall be based upon written findings made by the official making such determination or decision, which findings shall be final and shall be available within the Office of the Director of National Intelligence for a period of at least six years following the date of such determination or decision.

(4)(A) In addition to the authority referred to in paragraph (1), the Director of National Intelligence may authorize the head of an element of the intelligence community to exercise an acquisition authority referred to in section 3 or 8(a) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403c and 403j(a)) for an acquisition by such element that is more than 50 percent funded under the National Intelligence Program.

(B) The head of an element of the intelligence community may not exercise an authority referred to in subparagraph (A) until—

(i) the head of such element (without delegation) submits to the Director of National Intelligence a written request that includes—

(I) a description of such authority requested to be exercised;

(II) an explanation of the need for such authority, including an explanation of the reasons that other authorities are insufficient; and

(III) a certification that the mission of such element would be—

(aa) impaired if such authority is not exercised; or

(bb) significantly and measurably enhanced if such authority is exercised; and

(ii) the Director of National Intelligence issues a written authorization that includes—

(I) a description of the authority referred to in subparagraph (A) that is authorized to be exercised; and

(II) a justification to support the exercise of such authority.

(C) A request and authorization to exercise an authority referred to in subparagraph (A) may be made with respect to an individual acquisition or with respect to a specific class of acquisitions described in the request and authorization referred to in subparagraph (B).

(D)(i) A request from a head of an element of the intelligence community located within one of the departments described in clause (ii) to exercise an authority referred to in subparagraph (A) shall be submitted to the Director of National Intelligence in accordance with any procedures established by the head of such department.

(ii) The departments described in this clause are the Department of Defense, the Department of Energy, the Department of Homeland Security, the Department of Justice, the Department of State, and the Department of the Treasury.

(E)(i) The head of an element of the intelligence community may not be authorized to utilize an authority referred to in subparagraph (A) for a class of acquisitions for a period of more than 3 years, except that the Director of National Intelligence (without delegation) may authorize the use of such an authority for not more than 6 years.

(ii) Each authorization to utilize an authority referred to in subparagraph (A) may be extended in accordance with the requirements of subparagraph (B) for successive periods of not more than 3 years, except that the Director of National Intelligence (without delegation) may authorize an extension period of not more than 6 years.

(F) Subject to clauses (i) and (ii) of subparagraph (E), the Director of National Intelligence may only delegate the authority of the Director under subparagraphs (A) through (E) to the Principal Deputy Director of National Intelligence or a Deputy Director of National Intelligence.

(G) The Director of National Intelligence shall submit—

(i) to the congressional intelligence committees a notification of an authorization to exercise an authority referred to in subparagraph (A) or an extension of such authorization that includes the written authorization referred to in subparagraph (B)(ii); and

(ii) to the Director of the Office of Management and Budget a notification of an authorization to exercise an authority referred to in subparagraph (A) for an acquisition or class of acquisitions that will exceed $50,000,000 annually.

(H) Requests and authorizations to exercise an authority referred to in subparagraph (A) shall remain available within the Office of the Director of National Intelligence for a period of at least 6 years following the date of such request or authorization.

(I) Nothing in this paragraph may be construed to alter or otherwise limit the authority of the Central Intelligence Agency to independently exercise an authority under section 3 or 8(a) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403c and 403j(a)).

(o) CONSIDERATION OF VIEWS OF ELEMENTS OF INTELLIGENCE COMMUNITY.—In carrying out the duties and responsibilities under this section, the Director of National Intelligence shall take into account the views of a head of a department containing an element

of the intelligence community and of the Director of the Central Intelligence Agency.

(p) RESPONSIBILITY OF DIRECTOR OF NATIONAL INTELLIGENCE REGARDING NATIONAL INTELLIGENCE PROGRAM BUDGET CONCERNING THE DEPARTMENT OF DEFENSE.—Subject to the direction of the President, the Director of National Intelligence shall, after consultation with the Secretary of Defense, ensure that the National Intelligence Program budgets for the elements of the intelligence community that are within the Department of Defense are adequate to satisfy the national intelligence needs of the Department of Defense, including the needs of the Chairman of the Joint Chiefs of Staff and the commanders of the unified and specified commands, and wherever such elements are performing Government-wide functions, the needs of other Federal departments and agencies.

(q) ACQUISITIONS OF MAJOR SYSTEMS.—(1) For each intelligence program within the National Intelligence Program for the acquisition of a major system, the Director of National Intelligence shall—

(A) require the development and implementation of a program management plan that includes cost, schedule, security risks, and performance goals and program milestone criteria, except that with respect to Department of Defense programs the Director shall consult with the Secretary of Defense;

(B) serve as exclusive milestone decision authority, except that with respect to Department of Defense programs the Director shall serve as milestone decision authority jointly with the Secretary of Defense or the designee of the Secretary; and

(C) periodically—

(i) review and assess the progress made toward the achievement of the goals and milestones established in such plan; and

(ii) submit to Congress a report on the results of such review and assessment.

(2) If the Director of National Intelligence and the Secretary of Defense are unable to reach an agreement on a milestone decision under paragraph (1)(B), the President shall resolve the conflict.

(3) Nothing in this subsection may be construed to limit the authority of the Director of National Intelligence to delegate to any other official any authority to perform the responsibilities of the Director under this subsection.

(4) In this subsection:

(A) The term "intelligence program", with respect to the acquisition of a major system, means a program that—

(i) is carried out to acquire such major system for an element of the intelligence community; and

(ii) is funded in whole out of amounts available for the National Intelligence Program.

(B) The term "major system" has the meaning given such term in section 4(9) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 403(9)).

(r) PERFORMANCE OF COMMON SERVICES.—The Director of National Intelligence shall, in consultation with the heads of departments and agencies of the United States Government containing elements within the intelligence community and with the Director of the Central Intelligence Agency, coordinate the performance by

the elements of the intelligence community within the National Intelligence Program of such services as are of common concern to the intelligence community, which services the Director of National Intelligence determines can be more efficiently accomplished in a consolidated manner.

(s) PAY AUTHORITY FOR CRITICAL POSITIONS.—(1) Notwithstanding any pay limitation established under any other provision of law applicable to employees in elements of the intelligence community, the Director of National Intelligence may, in coordination with the Director of the Office of Personnel Management and the Director of the Office of Management and Budget, grant authority to the head of a department or agency to fix the rate of basic pay for one or more positions within the intelligence community at a rate in excess of any applicable limitation, subject to the provisions of this subsection. The exercise of authority so granted is at the discretion of the head of the department or agency employing the individual in a position covered by such authority, subject to the provisions of this subsection and any conditions established by the Director of National Intelligence when granting such authority.

(2) Authority under this subsection may be granted or exercised only—

(A) with respect to a position that requires an extremely high level of expertise and is critical to successful accomplishment of an important mission; and

(B) to the extent necessary to recruit or retain an individual exceptionally well qualified for the position.

(3) The head of a department or agency may not fix a rate of basic pay under this subsection at a rate greater than the rate payable for level II of the Executive Schedule under section 5313 of title 5, United States Code, except upon written approval of the Director of National Intelligence or as otherwise authorized by law.

(4) The head of a department or agency may not fix a rate of basic pay under this subsection at a rate greater than the rate payable for level I of the Executive Schedule under section 5312 of title 5, United States Code, except upon written approval of the President in response to a request by the Director of National Intelligence or as otherwise authorized by law.

(5) Any grant of authority under this subsection for a position shall terminate at the discretion of the Director of National Intelligence.

(6)(A) The Director of National Intelligence shall notify the congressional intelligence committees not later than 30 days after the date on which the Director grants authority to the head of a department or agency under this subsection.

(B) The head of a department or agency to which the Director of National Intelligence grants authority under this subsection shall notify the congressional intelligence committees and the Director of the exercise of such authority not later than 30 days after the date on which such head exercises such authority.

(t) AWARD OF RANK TO MEMBERS OF THE SENIOR NATIONAL INTELLIGENCE SERVICE.—(1) The President, based on the recommendation of the Director of National Intelligence, may award a rank to a member of the Senior National Intelligence Service or other intelligence community senior civilian officer not already covered by such a rank award program in the same manner in which

a career appointee of an agency may be awarded a rank under section 4507 of title 5, United States Code.

(2) The President may establish procedures to award a rank under paragraph (1) to a member of the Senior National Intelligence Service or a senior civilian officer of the intelligence community whose identity as such a member or officer is classified information (as defined in section 606(1)).

(u) CONFLICT OF INTEREST REGULATIONS.—The Director of National Intelligence, in consultation with the Director of the Office of Government Ethics, shall issue regulations prohibiting an officer or employee of an element of the intelligence community from engaging in outside employment if such employment creates a conflict of interest or appearance thereof.

(v) AUTHORITY TO ESTABLISH POSITIONS IN EXCEPTED SERVICE.—(1) The Director of National Intelligence, with the concurrence of the head of the covered department concerned and in consultation with the Director of the Office of Personnel Management, may—

(A) convert competitive service positions, and the incumbents of such positions, within an element of the intelligence community in such department, to excepted service positions as the Director of National Intelligence determines necessary to carry out the intelligence functions of such element; and

(B) establish new positions in the excepted service within an element of the intelligence community in such department, if the Director of National Intelligence determines such positions are necessary to carry out the intelligence functions of such element.

(2) An incumbent occupying a position on the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2012 selected to be converted to the excepted service under this section shall have the right to refuse such conversion. Once such individual no longer occupies the position, the position may be converted to the excepted service.

(3) A covered department may appoint an individual to a position converted or established pursuant to this subsection without regard to the civil-service laws, including parts II and III of title 5, United States Code.

(4) In this subsection, the term "covered department" means the Department of Energy, the Department of Homeland Security, the Department of State, or the Department of the Treasury.

(w) NUCLEAR PROLIFERATION ASSESSMENT STATEMENTS INTELLIGENCE COMMUNITY ADDENDUM.—The Director of National Intelligence, in consultation with the heads of the appropriate elements of the intelligence community and the Secretary of State, shall provide to the President, the congressional intelligence committees, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate an addendum to each Nuclear Proliferation Assessment Statement accompanying a civilian nuclear cooperation agreement, containing a comprehensive analysis of the country's export control system with respect to nuclear-related matters, including interactions with other countries of proliferation concern and the actual or suspected nuclear, dual-use, or missile-related transfers to such countries.

(x) REQUIREMENTS FOR INTELLIGENCE COMMUNITY CONTRACTORS.—The Director of National Intelligence, in consultation with

the head of each department of the Federal Government that contains an element of the intelligence community and the Director of the Central Intelligence Agency, shall—

(1) ensure that—

(A) any contractor to an element of the intelligence community with access to a classified network or classified information develops and operates a security plan that is consistent with standards established by the Director of National Intelligence for intelligence community networks; and

(B) each contract awarded by an element of the intelligence community includes provisions requiring the contractor comply with such plan and such standards;

(2) conduct periodic assessments of each security plan required under paragraph (1)(A) to ensure such security plan complies with the requirements of such paragraph; and

(3) ensure that the insider threat detection capabilities and insider threat policies of the intelligence community apply to facilities of contractors with access to a classified network.

(y) FUNDRAISING.—(1) The Director of National Intelligence may engage in fundraising in an official capacity for the benefit of nonprofit organizations that—

(A) provide support to surviving family members of a deceased employee of an element of the intelligence community; or

(B) otherwise provide support for the welfare, education, or recreation of employees of an element of the intelligence community, former employees of an element of the intelligence community, or family members of such employees.

(2) In this subsection, the term "fundraising" means the raising of funds through the active participation in the promotion, production, or presentation of an event designed to raise funds and does not include the direct solicitation of money by any other means.

(3) Not later than 7 days after the date the Director engages in fundraising authorized by this subsection or at the time the decision is made to participate in such fundraising, the Director shall notify the congressional intelligence committees of such fundraising.

(4) The Director, in consultation with the Director of the Office of Government Ethics, shall issue regulations to carry out the authority provided in this subsection. Such regulations shall ensure that such authority is exercised in a manner that is consistent with all relevant ethical constraints and principles, including the avoidance of any prohibited conflict of interest or appearance of impropriety.

(z) ANALYSES AND IMPACT STATEMENTS REGARDING PROPOSED INVESTMENT INTO THE UNITED STATES.—(1) Not later than 20 days after the completion of a review or an investigation of any proposed investment into the United States for which the Director has prepared analytic materials, the Director shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representative copies of such analytic materials, including any supplements or amendments to such analysis made by the Director.

(2) Not later than 60 days after the completion of consideration by the United States Government of any investment described in paragraph (1), the Director shall determine whether such investment will have an operational impact on the intelligence community, and, if so, shall submit a report on such impact to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives. Each such report shall—

(A) describe the operational impact of the investment on the intelligence community; and

(B) describe any actions that have been or will be taken to mitigate such impact.

*(aa) RESPONSIBILITY OF DIRECTOR OF NATIONAL INTELLIGENCE REGARDING NATIONAL INTELLIGENCE PROGRAM BUDGET CONCERNING FEDERAL BUREAU OF INVESTIGATION.—(1) Consistent with subsection (c)(5)(C), the Director of National Intelligence shall, after consultation with the Director of the Federal Bureau of Investigation, ensure that the programs and activities of the Federal Bureau of Investigation that are part of the National Intelligence Program are executed in a manner that conforms with the requirements of the national intelligence strategy under section 108A and the National Intelligence Priorities Framework of the Office of the Director of National Intelligence (or any successor mechanism established for the prioritization of such programs and activities).*

*(2) Consistent with subsection (c)(5)(C), the Director of National Intelligence shall ensure that the programs and activities that are part of the National Intelligence Program, including those of the Federal Bureau of Investigation, are structured and executed in a manner than enables budget traceability.*

* * * * * * *

NON-REIMBURSABLE DETAIL OF OTHER PERSONNEL

SEC. 113A. ⟦An officer⟧ *(a) IN GENERAL.—An officer* or employee of the United States or member of the Armed Forces may be detailed to the staff of an element of the intelligence community funded through the National Intelligence Program from another element of the intelligence community or from another element of the United States Government on a non-reimbursable basis, as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed three years. This ⟦section⟧ *subsection* does not limit any other source of authority for reimbursable or non-reimbursable details. A non-reimbursable detail made under this ⟦section⟧ *subsection* shall not be considered an augmentation of the appropriations of the receiving element of the intelligence community.

*(b) PROCESSING AND RESETTLEMENT OF REFUGEES, PAROLEES, AND OTHER ALIENS FROM AFGHANISTAN.—An officer or employee of an element of the intelligence community may be detailed to another element of the United States Government on a non-reimbursable basis for the purpose of providing assistance with the processing and resettlement of refugees, parolees, and other aliens, from Afghanistan, as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed 1 year. This subsection does not limit any other source of authority for reimbursable or non-*

*reimbursable details. A non-reimbursable detail made under this subsection shall not be considered an augmentation of the appropriations of the receiving element of the United States Government.*

* * * * * * *

***SEC. 116A. AUTHORITY FOR TRANSPORTATION OF CERTAIN CANINES ASSOCIATED WITH FORCE PROTECTION DUTIES OF INTELLIGENCE COMMUNITY.***

*(a) TRANSPORTATION.—For purposes of section 1344 of title 31, United States Code, the transportation of federally owned canines associated with force protection duties of an element of the intelligence community between the residence of an officer or employee of the element and various locations that is essential for the performance of the force protection duty shall be deemed essential for the safe and efficient performance of intelligence duties.*

*(b) OFFICERS AND EMPLOYEES COVERED.—In the administration of section 1344 of title 31, United States Code, an officer or employee of an element of the intelligence community shall be treated as being listed in subsection (b).*

* * * * * * *

NATIONAL [COUNTER PROLIFERATION] *COUNTERPROLIFERATION AND BIOSECURITY* CENTER

SEC. 119A. (a) ESTABLISHMENT.—(1) The President shall establish a [National Counter Proliferation Center] *National Counterproliferation and Biosecurity Center*, taking into account all appropriate [government tools to prevent] *government tools to—*

*(A) prevent* and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies[.]*; and*

*(B) lead integration and mission management of all intelligence activities pertaining to biosecurity and foreign biological threats.*

(2) The head of the [National Counter Proliferation Center] *National Counterproliferation and Biosecurity Center* shall be the Director of the [National Counter Proliferation Center] *National Counterproliferation and Biosecurity Center*, who shall be appointed by the Director of National Intelligence.

(3) The [National Counter Proliferation Center] *National Counterproliferation and Biosecurity Center* shall be located within the Office of the Director of National Intelligence.

*(4) The Director of the National Counterproliferation and Biosecurity Center shall serve as the principal coordinator for the intelligence community, and as the principal advisor to the Director of National Intelligence, with respect to biosecurity and foreign biological threats.*

(b) MISSIONS AND OBJECTIVES.—[In establishing]

*(1) COUNTERPROLIFERATION.—In establishing* the [National Counter Proliferation Center] *National Counterproliferation and Biosecurity Center*, the President shall address the following missions and objectives to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies:

[(1)] *(A)* Establishing a primary organization within the United States Government for analyzing and integrating

all intelligence possessed or acquired by the United States pertaining to proliferation.

[(2)] *(B)* Ensuring that appropriate agencies have full access to and receive all-source intelligence support needed to execute their [counter proliferation] *counterproliferation* plans or activities, and perform independent, alternative analyses.

[(3)] *(C)* Establishing a central repository on known and suspected proliferation activities, including the goals, strategies, capabilities, networks, and any individuals, groups, or entities engaged in proliferation.

[(4)] *(D)* Disseminating proliferation information, including proliferation threats and analyses, to the President, to the appropriate departments and agencies, and to the appropriate committees of Congress.

[(5)] *(E)* Conducting net assessments and warnings about the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.

[(6)] *(F)* Coordinating [counter proliferation] *counterproliferation* plans and activities of the various departments and agencies of the United States Government to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.

[(7)] *(G)* Conducting strategic operational [counter proliferation] *counterproliferation* planning for the United States Government to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.

*(2) BIOSECURITY.—In establishing the National Counterproliferation and Biosecurity Center, the President shall address the following missions and objectives to ensure that the Center serves as the lead for the intelligence community for the integration, mission management, and coordination of intelligence activities pertaining to biosecurity and foreign biological threats, regardless of origin:*

*(A) Ensuring that the elements of the intelligence community provide timely and effective warnings to the President and the Director of National Intelligence regarding emerging foreign biological threats, including diseases with pandemic potential.*

*(B) Overseeing and coordinating the collection and analysis of intelligence on biosecurity and foreign biological threats in support of the intelligence needs of the Federal departments and agencies responsible for public health, including by conveying collection priorities to elements of the intelligence community.*

*(C) Coordinating intelligence support to the Federal departments and agencies responsible for public health, including by ensuring that intelligence pertaining to biosecurity and foreign biological threats is disseminated among appropriately cleared personnel of such departments and agencies.*

*(D) Coordinating with the Federal departments and agencies responsible for public health to encourage information sharing with the intelligence community.*

*(E) Identifying gaps in the capabilities of the intelligence community regarding biosecurity and countering foreign biological threats and providing to the Director of National Intelligence recommended solutions for such gaps, including by encouraging research and development of new capabilities to counter foreign biological threats.*

(c) NATIONAL SECURITY WAIVER.—The President may waive the requirements of this section, and any parts thereof, if the President determines that such requirements do not materially improve the ability of the United States Government to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies. Such waiver shall be made in writing to Congress and shall include a description of how the missions and objectives in subsection (b) are being met.

(d) REPORT TO CONGRESS.—(1) Not later than nine months after the implementation of this Act, the President shall submit to Congress, in classified form if necessary, the findings and recommendations of the President's Commission on Weapons of Mass Destruction established by Executive Order in February 2004, together with the views of the President regarding the establishment of a ⟦National Counter Proliferation Center⟧ *National Counterproliferation and Biosecurity Center*.

(2) If the President decides not to exercise the waiver authority granted by subsection (c), the President shall submit to Congress from time to time updates and plans regarding the establishment of a ⟦National Counter Proliferation Center⟧ *National Counterproliferation and Biosecurity Center*.

(e) SENSE OF CONGRESS.—It is the sense of Congress that a central feature of ⟦counter proliferation⟧ *counterproliferation* activities, consistent with the President's Proliferation Security Initiative, should include the physical interdiction, by air, sea, or land, of weapons of mass destruction, their delivery systems, and related materials and technologies, and enhanced law enforcement activities to identify and disrupt proliferation networks, activities, organizations, and persons.

* * * * * * *

**SEC. 120. CLIMATE SECURITY ADVISORY COUNCIL.**

(a) ESTABLISHMENT.—The Director of National Intelligence shall establish a Climate Security Advisory Council for the purpose of—

(1) assisting intelligence analysts of various elements of the intelligence community with respect to analysis of climate security and its impact on the areas of focus of such analysts;

(2) facilitating coordination between the elements of the intelligence community and elements of the Federal Government that are not elements of the intelligence community in collecting data on, and conducting analysis of, climate change and climate security; and

(3) ensuring that the intelligence community is adequately prioritizing climate change in carrying out its activities.

(b) COMPOSITION OF COUNCIL.—

(1) MEMBERS.—The Council shall be composed of the following individuals appointed by the Director of National Intelligence:

(A) An appropriate official from the National Intelligence Council, who shall chair the Council.

(B) The lead official with respect to climate and environmental security analysis from—

(i) the Central Intelligence Agency;

(ii) the Bureau of Intelligence and Research of the Department of State;

(iii) the National Geospatial-Intelligence Agency;

(iv) the Office of Intelligence and Counterintelligence of the Department of Energy;

(v) the Office of the Under Secretary of Defense for Intelligence *and Security*; and

(vi) the Defense Intelligence Agency.

(C) Three appropriate officials from elements of the Federal Government that are not elements of the intelligence community that are responsible for—

(i) providing decision makers with a predictive understanding of the climate;

(ii) making observations of our Earth system that can be used by the public, policymakers, and to support strategic decisions; or

(iii) coordinating Federal research and investments in understanding the forces shaping the global environment, both human and natural, and their impacts on society.

(D) Any other officials as the Director of National Intelligence or the chair of the Council may determine appropriate.

(2) RESPONSIBILITIES OF CHAIR.—The chair of the Council shall have responsibility for—

(A) identifying agencies to supply individuals from elements of the Federal Government that are not elements of the intelligence community;

(B) securing the permission of the relevant agency heads for the participation of such individuals on the Council; and

(C) any other duties that the Director of National Intelligence may direct.

(c) DUTIES AND RESPONSIBILITIES OF COUNCIL.—The Council shall carry out the following duties and responsibilities:

(1) To meet at least quarterly to—

(A) exchange appropriate data between elements of the intelligence community and elements of the Federal Government that are not elements of the intelligence community;

(B) discuss processes for the routine exchange of such data and implementation of such processes; and

(C) prepare summaries of the business conducted at each meeting.

(2) To assess and determine best practices with respect to the analysis of climate security, including identifying publicly

available information and intelligence acquired through clandestine means that enables such analysis.

(3) To assess and identify best practices with respect to prior efforts of the intelligence community to analyze climate security.

(4) To assess and describe best practices for identifying and disseminating climate intelligence indications and warnings.

(5) To recommend methods of incorporating analysis of climate security and the best practices identified under paragraphs (2) through (4) into existing analytic training programs.

(6) To consult, as appropriate, with other elements of the intelligence community that conduct analysis of climate change or climate security and elements of the Federal Government that are not elements of the intelligence community that conduct analysis of climate change or climate security, for the purpose of sharing information about ongoing efforts and avoiding duplication of existing efforts.

(7) To work with elements of the intelligence community that conduct analysis of climate change or climate security and elements of the Federal Government that are not elements of the intelligence community that conduct analysis of climate change or climate security—

(A) to exchange appropriate data between such elements, establish processes, procedures and practices for the routine exchange of such data, discuss the implementation of such processes; and

(B) to enable and facilitate the sharing of findings and analysis between such elements.

(8) To assess whether the elements of the intelligence community that conduct analysis of climate change or climate security may inform the research direction of academic work and the sponsored work of the United States Government.

(9) At the discretion of the chair of the Council, to convene conferences of analysts and nonintelligence community personnel working on climate change or climate security on subjects that the chair shall direct.

(d) ANNUAL REPORT.—**[**Not later**]**

*(1) REQUIREMENT.—Not later* than January 31, 2021, and not less frequently than annually thereafter, the chair of the Council shall submit, on behalf of the Council, to the congressional intelligence committees a report describing the activities of the Council as described in subsection (c) during the year preceding the year during which the report is submitted.

*(2) MATTERS INCLUDED.—Each report under paragraph (1) shall include a description of any obstacles or gaps relating to—*

*(A) the Council fulfilling its duties and responsibilities under subsection (c); or*

*(B) the responsiveness of the intelligence community to the climate security needs and priorities of the policymaking elements of the Federal Government.*

(e) SUNSET.—The Council shall terminate on **[**the date that is 4 years after the date of the enactment of this section**]** *December 31, 2025*.

**[**(e)**]** *(f)* DEFINITIONS.—In this section:

(1) CLIMATE SECURITY.—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.

(2) CLIMATE INTELLIGENCE INDICATIONS AND WARNINGS.—The term "climate intelligence indications and warnings" means developments relating to climate security with the potential to—

(A) imminently and substantially alter the political stability or degree of human security in a country or region; or

(B) imminently and substantially threaten—

(i) the national security of the United States;

(ii) the military, political, or economic interests of allies and partners of the United States; or

(iii) citizens of the United States abroad.

* * * * * * *

## TITLE III—MISCELLANEOUS

* * * * * * *

**[SEC. 304. REPORTING OF CERTAIN EMPLOYMENT ACTIVITIES BY FORMER INTELLIGENCE OFFICERS AND EMPLOYEES.**

[(a) IN GENERAL.—The head of each element of the intelligence community shall issue regulations requiring each employee of such element occupying a covered position to sign a written agreement requiring the regular reporting of covered employment to the head of such element.

[(b) AGREEMENT ELEMENTS.—The regulations required under subsection (a) shall provide that an agreement contain provisions requiring each employee occupying a covered position to, during the two-year period beginning on the date on which such employee ceases to occupy such covered position—

[(1) report covered employment to the head of the element of the intelligence community that employed such employee in such covered position upon accepting such covered employment; and

[(2) annually (or more frequently if the head of such element considers it appropriate) report covered employment to the head of such element.

[(c) DEFINITIONS.—In this section:

[(1) COVERED EMPLOYMENT.—The term "covered employment" means direct employment by, representation of, or the provision of advice relating to national security to the government of a foreign country or any person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized, in whole or in major part, by any government of a foreign country.

[(2) COVERED POSITION.—The term "covered position" means a position within an element of the intelligence community

that, based on the level of access of a person occupying such position to information regarding sensitive intelligence sources or methods or other exceptionally sensitive matters, the head of such element determines should be subject to the requirements of this section.

[(3) GOVERNMENT OF A FOREIGN COUNTRY.—The term "government of a foreign country" has the meaning given the term in section 1(e) of the Foreign Agents Registration Act of 1938 (22 U.S.C. 611(e)).]

***SEC. 304. REQUIREMENTS FOR CERTAIN EMPLOYMENT ACTIVITIES BY FORMER INTELLIGENCE OFFICERS AND EMPLOYEES.***

*(a) TEMPORARY RESTRICTION.—An employee of an element of the intelligence community who occupies a covered intelligence position may not occupy a covered post-service position during the 30-month period following the date on which the employee ceases to occupy a covered intelligence position.*

*(b) COVERED POST-SERVICE EMPLOYMENT REPORTING.—*

*(1) REQUIREMENT.—During the 5-year period beginning on the date on which an employee ceases to occupy a covered intelligence position, the employee shall—*

*(A) report covered post-service employment to the head of the element of the intelligence community that employed such employee in such covered intelligence position upon accepting such covered post-service employment; and*

*(B) annually (or more frequently if the head of such element considers it appropriate) report covered post-service employment to the head of such element.*

*(2) REGULATIONS.—The head of each element of the intelligence community shall issue regulations requiring, as a condition of employment, each employee of such element occupying a covered intelligence position to sign a written agreement requiring the regular reporting of covered post-service employment to the head of such element pursuant to paragraph (1).*

*(c) PENALTIES.—*

*(1) CRIMINAL PENALTIES.—A former employee who knowingly and willfully violates subsection (a) or who knowingly and willfully fails to make a required report under subsection (b) shall be fined under title 18, United States Code, or imprisoned for not more than 5 years, or both. Each report under subsection (b) shall be subject to section 1001 of title 18, United States Code.*

*(2) SECURITY CLEARANCES.—The head of an element of the intelligence community shall revoke the security clearance of a former employee if the former employee knowingly and willfully fails to make a required report under subsection (b) or knowingly and willfully makes a false report under such subsection.*

*(d) PROVISION OF INFORMATION.—*

*(1) TRAINING.—The head of each element of the intelligence community shall regularly provide training on the reporting requirements under subsection (b) to employees of that element who occupy a covered intelligence position.*

*(2) WRITTEN NOTICE.—The head of each element of the intelligence community shall provide written notice of the reporting requirements under subsection (b) to an employee when the employee ceases to occupy a covered intelligence position.*

*(e) ANNUAL REPORTS.—*

*(1) REQUIREMENT.—Not later than March 31 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report on covered post-service employment occurring during the year covered by the report.*

*(2) ELEMENTS.—Each report under paragraph (1) shall include the following:*

*(A) The number of former employees who occupy a covered post-service position, broken down by—*

*(i) the name of the employer;*

*(ii) the foreign government, including by the specific foreign individual, agency, or entity, for whom the covered post-service employment is being performed; and*

*(iii) the nature of the services provided as part of the covered post-service employment.*

*(B) A certification by the Director that—*

*(i) each element of the intelligence community maintains adequate systems and processes for ensuring that former employees are submitting reports required under subsection (b);*

*(ii) to the knowledge of the heads of the elements of the intelligence community, all former employees who occupy a covered post-service position are in compliance with this section;*

*(iii) the services provided by former employees who occupy a covered post-service position do not—*

*(I) pose a current or future threat to the national security of the United States; or*

*(II) pose a counterintelligence risk; and*

*(iv) the Director and the heads of such elements are not aware of any credible information or reporting that any former employee who occupies a covered post-service position has engaged in activities that violate Federal law, infringe upon the privacy rights of United States persons, or constitute abuses of human rights.*

*(3) FORM.—Each report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.*

*(f) NOTIFICATION.—In addition to the annual reports under subsection (e), if a head of an element of the intelligence community determines that the services provided by a former employee who occupies a covered post-service position pose a threat or risk described in clause (iii) of paragraph (2)(B) of such subsection, or include activities described in clause (iv) of such paragraph, the head shall notify the congressional intelligence committees of such determination by not later than 7 days after making such determination. The notification shall include the following:*

*(1) The name of the former employee.*

*(2) The name of the employer.*

*(3) The foreign government, including the specific foreign individual, agency, or entity, for whom the covered post-service employment is being performed.*

*(4) As applicable, a description of—*

*(A) the risk to national security, the counterintelligence risk, or both; and*

*(B) the activities that may violate Federal law, infringe upon the privacy rights of United States persons, or constitute abuses of human rights.*

*(g) DEFINITIONS.—In this section:*

*(1) COVERED INTELLIGENCE POSITION.—The term "covered intelligence position" means a position within an element of the intelligence community that, based on the level of access of a person occupying such position to information regarding sensitive intelligence sources or methods or other exceptionally sensitive matters, the head of such element determines should be subject to the requirements of this section.*

*(2) COVERED POST-SERVICE EMPLOYMENT.—The term "covered post-service employment" means direct or indirect employment by, representation of, or any provision of advice or services relating to national security, intelligence, the military, or internal security to, the government of a foreign country or any company, entity, or other person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized, in whole or in major part, by any government of a foreign country.*

*(3) COVERED POST-SERVICE POSITION.—The term "covered post-service position" means a position of employment described in paragraph (2).*

*(4) EMPLOYEE.—The term "employee", with respect to an employee occupying a covered intelligence position, includes an officer or official of an element of the intelligence community, a contractor of such an element, a detailee to such an element, or a member of the Armed Forces assigned to such an element.*

*(5) FORMER EMPLOYEE.—The term "former employee" means an individual—*

*(A) who was an employee occupying a covered intelligence position; and*

*(B) who is subject to the requirements under subsection (a) or (b).*

*(6) GOVERNMENT OF A FOREIGN COUNTRY.—The term "government of a foreign country" has the meaning given the term in section 1(e) of the Foreign Agents Registration Act of 1938 (22 U.S.C. 611(e)).*

***SEC. 305. TEMPORARY AUTHORITY FOR PAID LEAVE FOR A SERIOUS HEALTH CONDITION.***

*(a) DEFINITIONS.—In this section:*

*(1) PAID SERIOUS HEALTH CONDITION LEAVE.—The term "paid serious health condition leave" means paid leave taken under subsection (b).*

*(2) SERIOUS HEALTH CONDITION.—The term "serious health condition" has the meaning given the term in section 6381 of title 5, United States Code.*

*(3) SON OR DAUGHTER.—The term "son or daughter" has the meaning given the term in section 6381 of title 5, United States Code.*

*(b) PAID SERIOUS HEALTH CONDITION LEAVE.—During the period specified in subsection (f), and notwithstanding any other provision of law, a civilian employee of an element of the intelligence community shall have available a total of 12 administrative workweeks of*

*paid leave during any 12-month period for one or more of the following:*

*(1) In order to care for the spouse, or a son, daughter, or parent, of the employee, if such spouse, son, daughter, or parent has a serious health condition.*

*(2) Because of a serious health condition that makes the employee unable to perform the functions of the employee's position.*

*(c) TREATMENT OF SERIOUS HEALTH CONDITION LEAVE REQUEST.—Notwithstanding any other provision of law, an element of the intelligence community shall accommodate an employee's leave schedule request under subsection (b), including a request to use such leave intermittently or on a reduced leave schedule, to the extent that the requested leave schedule does not unduly disrupt agency operations.*

*(d) RULES RELATING TO PAID LEAVE.—During the period specified in subsection (f), and notwithstanding any other provision of law—*

*(1) an employee of an element of the intelligence community—*

*(A) shall be required to first use all accrued or accumulated paid sick leave before being allowed to use paid serious health condition leave; and*

*(B) may not be required to first use all or any portion of any unpaid leave available to the employee before being allowed to use paid serious health condition leave; and*

*(2) paid serious health condition leave—*

*(A) shall be payable from any appropriation or fund available for salaries or expenses for positions within the employing element;*

*(B) may not be considered to be annual or vacation leave for purposes of section 5551 or 5552 of title 5, United States Code, or for any other purpose;*

*(C) if not used by the employee before the end of the 12-month period described in subsection (b) to which the leave relates, may not be available for any subsequent use and may not be converted into a cash payment;*

*(D) may be granted only to the extent that the employee does not receive a total of more than 12 weeks of paid serious health condition leave in any 12-month period;*

*(E) shall be used in increments of hours (or fractions thereof), with 12 administrative workweeks equal to 480 hours for employees of elements of the intelligence community with a regular full-time work schedule and converted to a proportional number of hours for employees of such elements with part-time, seasonal, or uncommon tours of duty; and*

*(F) may not be used during off-season (nonpay status) periods for employees of such elements with seasonal work schedules.*

*(e) IMPLEMENTATION.—*

*(1) CONSISTENCY WITH SERIOUS HEALTH CONDITION LEAVE UNDER TITLE 5.—The Director of National Intelligence shall carry out this section in a manner consistent, to the extent appropriate, with the administration of leave taken under section 6382 of title 5, United States Code, for a reason described in subparagraph (C) or (D) of subsection (a)(1) of that section, in-*

*cluding with respect to the authority to require a certification described in section 6383 of such title.*

*(2) IMPLEMENTATION PLAN.—Not later than 1 year after the date of enactment of this section, the Director of National Intelligence shall submit to the congressional intelligence committees an implementation plan that includes—*

*(A) processes and procedures for implementing the paid serious health condition leave policies under subsections (b) through (d) during the period specified in subsection (f);*

*(B) an explanation of how such implementation will be reconciled with policies of other elements of the Federal Government, including the impact on elements funded by the National Intelligence Program that are housed within agencies outside the intelligence community;*

*(C) the projected impact of such implementation on the workforce of the intelligence community, including take rates, retention, recruiting, and morale, broken down by each element of the intelligence community; and*

*(D) all costs or operational expenses associated with such implementation.*

*(3) DIRECTIVE.—Not later than 90 days after the Director of National Intelligence submits the implementation plan under paragraph (2), the Director of National Intelligence shall issue a written directive to implement this section, which directive shall take effect on the date of issuance.*

*(f) DURATION OF AUTHORITY.—The authority and requirements under subsections (b) through (d) shall only apply during the 3-year period beginning on the date on which the Director of National Intelligence issues the written directive under subsection (e)(3).*

*(g) ANNUAL REPORT.—During the period specified in subsection (f), the Director of National Intelligence shall submit to the congressional intelligence committees an annual report that—*

*(1) details the number of employees of each element of the intelligence community who applied for and took paid serious health condition leave during the year covered by the report;*

*(2) includes updates on major implementation challenges or costs associated with paid serious health condition leave; and*

*(3) includes a recommendation of the Director with respect to whether to extend the period specified in subsection (f).*

* * * * * * *

## TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

* * * * * * *

***SEC. 501A. CONGRESSIONAL OVERSIGHT OF CERTAIN SPECIAL ACCESS PROGRAMS.***

*(a) REPORTS AND NOTIFICATIONS.—At the same time that the Secretary of Defense submits any report or notification under section 119 of title 10, United States Code, that relates to a covered special access program or a new covered special access program, the Secretary shall also submit such report or notification to the congressional intelligence committees.*

*(b) BRIEFINGS.—On a periodic basis, but not less frequently than semiannually, the Secretary of Defense shall provide to the chair-*

*men and ranking minority members of the congressional intelligence committees, and to any staff of such a committee designated by either the chair or ranking member for purposes of this subsection, a briefing on covered special access programs. Each such briefing shall include, at a minimum—*

*(1) a description of the activity of the program during the period covered by the briefing; and*

*(2) documentation with respect to how the program has achieved outcomes consistent with requirements documented by the Director of National Intelligence and the Secretary of Defense.*

*(c) NOTIFICATIONS ON COMPARTMENTS AND SUBCOMPARTMENTS.—*

*(1) REQUIREMENT.—Except as provided by paragraph (2), a head of an element of the intelligence community may not establish a compartment or a subcompartment under a covered special access program until the head notifies the congressional intelligence committees of such compartment or subcompartment, as the case may be.*

*(2) WAIVER.—*

*(A) DETERMINATION.—On a case-by-case basis, the Director of National Intelligence may waive the requirement under paragraph (1). Not later than two days after making such a waiver, the Director shall notify the congressional intelligence committees of the waiver, including a justification for the waiver.*

*(B) SUBMISSION.—Not later than 30 days after the date on which the Director makes a waiver under subparagraph (A), the head of the element of the intelligence community for whom the waiver was made shall submit to the congressional intelligence committees the notification required under paragraph (1) relating to such waiver.*

*(d) ANNUAL REPORTS.—*

*(1) REQUIREMENT.—On an annual basis, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report on covered special access programs administered by the head.*

*(2) MATTERS INCLUDED.—Each report shall include, with respect to the period covered by the report, the following:*

*(A) A list of all compartments and subcompartments of covered special access programs active as of the date of the report.*

*(B) A list of all compartments and subcompartments of covered special access programs terminated during the period covered by the report.*

*(C) With respect to the report submitted by the Director of National Intelligence, in addition to the matters specified in subparagraphs (A) and (B)—*

*(i) a certification regarding whether the creation, validation, or substantial modification, including termination, for all existing and proposed covered special access programs, and the compartments and subcompartments within each, are substantiated and justified based on the information required by clause (ii); and*

*(ii) for each certification—*

*(I) the rationale for the revalidation, validation, or substantial modification, including termination, of each covered special access program, compartment, and subcompartment;*

*(II) the identification of a control officer for each covered special access program; and*

*(III) a statement of protection requirements for each covered special access program.*

*(e) COVERED SPECIAL ACCESS PROGRAM DEFINED.—In this section, the term "covered special access program" means a special access program that receives funding under the National Intelligence Program or the Military Intelligence Program, relates to an intelligence or intelligence-related activity, or both.*

* * * * * * *

FUNDING OF INTELLIGENCE ACTIVITIES

SEC. 504. (a) Appropriated funds available to an intelligence agency may be obligated or expended for an intelligence or intelligence-related activity only if—

[(1) those funds were specifically authorized by the Congress for use for such activities; or]

*(1) those funds were specifically authorized by Congress for use for such intelligence or intelligence-related activities; or*

(2) in the case of funds from the Reserve for Contingencies of the Central Intelligence Agency and consistent with the provisions of section 503 of this Act concerning any significant anticipated intelligence activity, the Director of the Central Intelligence Agency has notified the appropriate congressional committees of the intent to make such funds available for such activity; or

(3) in the case of funds specifically authorized by the Congress for a different activity—

(A) the activity to be funded is a higher priority intelligence or intelligence-related activity;

(B) the use of such funds for such activity supports an emergent need, improves program effectiveness, or increases efficiency; and

(C) the Director of National Intelligence, the Secretary of Defense, or the Attorney General, as appropriate, has notified the appropriate congressional committees of the intent to make such funds available for such activity;

(4) nothing in this subsection prohibits obligation or expenditure of funds available to an intelligence agency in accordance with sections 1535 and 1536 of title 31, United States Code.

(b) Funds available to an intelligence agency may not be made available for any intelligence or intelligence-related activity for which funds were denied by the Congress.

(c) No funds appropriated for, or otherwise available to, any department, agency, or entity of the United States Government may be expended, or may be directed to be expended, for any covert action, as defined in section 503(e), unless and until a Presidential finding required by subsection (a) of section 503 has been signed or otherwise issued in accordance with that subsection.

(d)(1) Except as otherwise specifically provided by law, funds available to an intelligence agency that are not appropriated funds may be obligated or expended for an intelligence or intelligence-related activity only if those funds are used for activities reported to the appropriate congressional committees pursuant to procedures which identify—

(A) the types of activities for which nonappropriated funds may be expended; and

(B) the circumstances under which an activity must be reported as a significant anticipated intelligence activity before such funds can be expended.

(2) Procedures for purposes of paragraph (1) shall be jointly agreed upon by the congressional intelligence committees and, as appropriate, the Director of National Intelligence or the Secretary of Defense.

(e) As used in this section—

(1) the term "intelligence agency" means any department, agency, or other entity of the United States involved in intelligence or intelligence-related activities;

(2) the term "appropriate congressional committees" means the Permanent Select Committee on Intelligence and the Committee on Appropriations of the House of Representatives and the Select Committee on Intelligence and the Committee on Appropriations of the Senate; and

(3) the term "specifically authorized by the Congress" means that—

(A) the activity and the amount of funds proposed to be used for that activity were identified in a formal budget request to the Congress, but funds shall be deemed to be specifically authorized for that activity only to the extent that the Congress both authorized the funds to be appropriated for that activity and appropriated the funds for that activity; or

(B) although the funds were not formally requested, the Congress both specifically authorized the appropriation of the funds for the activity and appropriated the funds for the activity.

* * * * * * *

## TITLE X—EDUCATION IN SUPPORT OF NATIONAL INTELLIGENCE

* * * * * * *

### SUBTITLE C—ADDITIONAL EDUCATION PROVISIONS

* * * * * * *

***SEC. 1025. AUTHORIZATION OF SUPPORT BY DIRECTOR OF NATIONAL INTELLIGENCE FOR CERTAIN WORKFORCE ACTIVITIES.***

*(a) AUTHORIZATION.—The Director may, with or without reimbursement, obligate or expend amounts authorized to be appropriated or otherwise made available for the Office of the Director of National Intelligence for covered workforce activities for the purpose of supporting a covered workforce activity of an element of the intelligence community.*

*(b) COVERED WORKFORCE ACTIVITY DEFINED.—In this section, the term "covered workforce activity" means an activity relating to—*

*(1) recruitment or retention of the intelligence community workforce; or*

*(2) diversity, equality, inclusion, or accessibility, with respect to such workforce.*

* * * * * * *

## TITLE XI—ADDITIONAL MISCELLANEOUS PROVISIONS

* * * * * * *

**SEC. 1104. PROHIBITED PERSONNEL PRACTICES IN THE INTELLIGENCE COMMUNITY.**

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term "agency" means an executive department or independent establishment, as defined under sections 101 and 104 of title 5, United States Code, that contains an intelligence community element, except the Federal Bureau of Investigation.

(2) COVERED INTELLIGENCE COMMUNITY ELEMENT.—The term "covered intelligence community element"—

(A) means—

(i) the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office; and

(ii) any executive agency or unit thereof determined by the President under section 2302(a)(2)(C)(ii) of title 5, United States Code, to have as its principal function the conduct of foreign intelligence or counterintelligence activities; and

(B) does not include the Federal Bureau of Investigation.

(3) PERSONNEL ACTION.—The term "personnel action" means, with respect to an employee in a position in a covered intelligence community element (other than a position excepted from the competitive service due to its confidential, policy-determining, policymaking, or policy-advocating character) or a contractor employee—

(A) an appointment;

(B) a promotion;

(C) a disciplinary or corrective action;

(D) a detail, transfer, or reassignment;

(E) a demotion, suspension, or termination;

(F) a reinstatement or restoration;

(G) a performance evaluation;

(H) a decision concerning pay, benefits, or awards;

(I) a decision concerning education or training if such education or training may reasonably be expected to lead to an appointment, promotion, or performance evaluation; or

(J) any other significant change in duties, responsibilities, or working conditions.

(4) CONTRACTOR EMPLOYEE.—The term "contractor employee" means an employee of a contractor, subcontractor, grantee,

subgrantee, or personal services contractor, of a covered intelligence community element.

(b) AGENCY EMPLOYEES.—[Any employee of an agency] *Any employee of a covered intelligence community element or an agency* who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take*, or threaten to take or fail to take,* a personnel action with respect to any employee of a covered intelligence community element as a reprisal [for a lawful disclosure] *for*—

*(1) any lawful disclosure* of information by the employee to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose), the Inspector General of the Intelligence Community, *a supervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including* the head of the employing agency (or an employee designated by the head of that agency for such purpose), the appropriate inspector general of the employing agency, a congressional intelligence committee, or a member of a congressional intelligence committee, which the employee reasonably believes evidences—

[(1)] *(A)* a violation of any Federal law, rule, or regulation; or

[(2)] *(B)* mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

*(2) any lawful disclosure that complies with—*

*(A) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);*

*(B) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or*

*(C) subparagraphs (A), (D), and (I) of section 103H(k)(5); or*

*(3) if the actions do not result in the employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—*

*(A) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;*

*(B) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in subparagraph (A); or*

*(C) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.*

(c) CONTRACTOR EMPLOYEES.—(1) Any employee *of an agency or* of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a covered intelligence community element who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take*, or threaten to take or fail to take,* a per-

sonnel action with respect to any contractor employee as a reprisal [for a lawful disclosure] *for—*

*(A) any lawful disclosure* of information by the contractor employee to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose), the Inspector General of the Intelligence Community, *a supervisor in the contractor employee's direct chain of command, or a supervisor of the contracting agency with responsibility for the subject matter of the disclosure, up to and including* the head of the contracting agency (or an employee designated by the head of that agency for such purpose), the appropriate inspector general of the contracting agency, a congressional intelligence committee, or a member of a congressional intelligence committee, which the contractor employee reasonably believes evidences—

[(A)] *(i)* a violation of any Federal law, rule, or regulation (including with respect to evidence of another employee or contractor employee accessing or sharing classified information without authorization); or

[(B) gross mismanagement] *(ii) mismanagement*, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

*(B) any lawful disclosure that complies with—*

*(i) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);*

*(ii) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or*

*(iii) subparagraphs (A), (D), and (I) of section 103H(k)(5); or*

*(C) if the actions do not result in the contractor employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—*

*(i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;*

*(ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or*

*(iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.*

(2) A personnel action under paragraph (1) is prohibited even if the action is undertaken at the request of an agency official, unless the request takes the form of a nondiscretionary directive and is within the authority of the agency official making the request.

*(d) RULE OF CONSTRUCTION.—Consistent with the protection of sources and methods, nothing in subsection (b) or (c) shall be construed to authorize—*

*(1) the withholding of information from Congress; or*

*(2) the taking of any personnel action against an employee who lawfully discloses information to Congress.*

*(e) DISCLOSURES.—A disclosure shall not be excluded from this section because—*

*(1) the disclosure was made to an individual, including a supervisor, who participated in an activity that the employee reasonably believed to be covered under subsection (b)(1)(B) or the contractor employee reasonably believed to be covered under subsection (c)(1)(A)(ii);*

*(2) the disclosure revealed information that had been previously disclosed;*

*(3) the disclosure was not made in writing;*

*(4) the disclosure was made while the employee was off duty;*

*(5) of the amount of time which has passed since the occurrence of the events described in the disclosure; or*

*(6) the disclosure was made during the normal course of duties of an employee or contractor employee.*

**[**(d) ENFORCEMENT.—The President shall provide for the enforcement of this section.**]**

*(f) ENFORCEMENT.—The President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.*

**[**(e)**]** *(g)* EXISTING RIGHTS PRESERVED.—Nothing in this section shall be construed to—

(1) preempt or preclude any employee, contractor employee, or applicant for employment, at the Federal Bureau of Investigation from exercising rights provided under any other law, rule, or regulation, including section 2303 of title 5, United States Code; or

(2) repeal section 2303 of title 5, United States Code.

* * * * * * *

***SEC. 1111. BIENNIAL REPORTS ON FOREIGN BIOLOGICAL THREATS.***

*(a) REPORTS.—On a biennial basis until the date that is 10 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, the Director of National Intelligence shall submit to the congressional intelligence committees a comprehensive report on the activities, prioritization, and responsibilities of the intelligence community with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country.*

*(b) MATTERS INCLUDED.—Each report under subsection (a) shall include, with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country, the following:*

*(1) A detailed description of all activities relating to such threats undertaken by each element of the intelligence community, and an assessment of any gaps in such activities.*

*(2) A detailed description of all duties and responsibilities relating to such threats explicitly authorized or otherwise assigned, exclusively or jointly, to each element of the intelligence community, and an assessment of any identified gaps in such duties or responsibilities.*

*(3) A description of the coordination among the relevant elements of the intelligence community with respect to the activities specified in paragraph (1) and the duties and responsibilities specified in paragraph (2).*

*(4) An inventory of the strategies, plans, policies, and interagency agreements of the intelligence community relating to the collection, monitoring, analysis, mitigation, and attribution of such threats, and an assessment of any identified gaps therein.*

*(5) A description of the coordination and interactions among the relevant elements of the intelligence community and non-intelligence community partners.*

*(6) An assessment of foreign malign influence efforts relating to such threats, and a description of how the intelligence community contributes to efforts by non-intelligence community partners to counter such foreign malign influence.*

*(c) FORM.—Each report submitted under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.*

*(d) DEFINITIONS.—In this section:*

*(1) COVERED COUNTRY.—The term "covered country" means—*

*(A) China;*

*(B) Iran;*

*(C) North Korea;*

*(D) Russia; and*

*(E) any other foreign country—*

*(i) from which the Director of National Intelligence determines a biological threat emanates; or*

*(ii) that the Director determines has a known history of, or has been assessed as having conditions present for, infectious disease outbreaks or epidemics.*

*(2) FOREIGN BIOLOGICAL THREAT.—The term "foreign biological threat" means biological warfare, bioterrorism, naturally occurring infectious diseases, or accidental exposures to biological materials, without regard to whether the threat originates from a state actor, a non-state actor, natural conditions, or an undetermined source.*

*(3) FOREIGN MALIGN INFLUENCE.—The term "foreign malign influence" has the meaning given such term in section 119C(e).*

*(4) NON-INTELLIGENCE COMMUNITY PARTNER.—The term "non-intelligence community partner" means a Federal department or agency that is not an element of the intelligence community.*

***SEC. 1112. ANNUAL REPORTS ON THE DOMESTIC ACTIVITIES OF THE INTELLIGENCE COMMUNITY.***

*(a) REPORTS.—Not later than January 31 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report—*

*(1) identifying all domestic activities undertaken by each element of the intelligence community during the prior fiscal year; and*

*(2) for each activity identified under paragraph (1), a statement of the legal authority authorizing such activity to be undertaken.*

*(b) FORM.—Each report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.*

***SEC. 1113. ANNUAL REPORTS ON CERTAIN CYBER VULNERABILITIES PROCURED BY INTELLIGENCE COMMUNITY AND FOREIGN COMMERCIAL PROVIDERS OF CYBER VULNERABILITIES.***

*(a) ANNUAL REPORTS.—On an annual basis through 2026, the Director of the Central Intelligence Agency and the Director of the National Security Agency, in coordination with the Director of National Intelligence, shall jointly submit to the congressional intelligence committees a report containing information on foreign commercial providers and the cyber vulnerabilities procured by the intelligence community through foreign commercial providers.*

*(b) ELEMENTS.—Each report under subsection (a) shall include, with respect to the period covered by the report, the following:*

*(1) A description of each cyber vulnerability procured through a foreign commercial provider, including—*

*(A) a description of the vulnerability;*

*(B) the date of the procurement;*

*(C) whether the procurement consisted of only that vulnerability or included other vulnerabilities;*

*(D) the cost of the procurement;*

*(E) the identity of the commercial provider and, if the commercial provider was not the original supplier of the vulnerability, a description of the original supplier;*

*(F) the country of origin of the vulnerability; and*

*(G) an assessment of the ability of the intelligence community to use the vulnerability, including whether such use will be operational or for research and development, and the approximate timeline for such use.*

*(2) An assessment of foreign commercial providers that—*

*(A) pose a significant threat to the national security of the United States; or*

*(B) have provided cyber vulnerabilities to any foreign government that—*

*(i) has used the cyber vulnerabilities to target United States persons, the United States Government, journalists, or dissidents; or*

*(ii) has an established pattern or practice of violating human rights or suppressing dissent.*

*(3) An assessment of whether the intelligence community has conducted business with the foreign commercial providers identified under paragraph (2) during the 5-year period preceding the date of the report.*

*(c) FORM.—Each report under subsection (a) may be submitted in classified form.*

*(d) DEFINITIONS.—In this section:*

*(1) COMMERCIAL PROVIDER.—The term "commercial provider" means any person that sells, or acts as a broker, for a cyber vulnerability.*

*(2) CYBER VULNERABILITY.—The term "cyber vulnerability" means any tool, exploit, vulnerability, or code that is intended to compromise a device, network, or system, including such a tool, exploit, vulnerability, or code procured by the intelligence community for purposes of research and development.*

* * * * * * *

**INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004**

* * * * * * *

# TITLE III—SECURITY CLEARANCES

**SEC. 3001. SECURITY CLEARANCES.**

(a) DEFINITIONS.—In this section:

(1) The term "agency" means—

(A) an executive agency (as that term is defined in section 105 of title 5, United States Code);

(B) a military department (as that term is defined in section 102 of title 5, United States Code); [and] *or*

(C) an element of the intelligence community.

(2) The term "authorized investigative agency" means an agency designated by the head of the agency selected pursuant to subsection (b) to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(3) The term "authorized adjudicative agency" means an agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.

(4) The term "highly sensitive program" means—

(A) a government program designated as a Special Access Program (as that term is defined in section 4.1(h) of Executive Order 12958 or any successor Executive order); or

(B) a government program that applies restrictions required for—

(i) restricted data (as that term is defined in section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)); or

(ii) other information commonly referred to as "sensitive compartmented information".

(5) The term "current investigation file" means, with respect to a security clearance, a file on an investigation or adjudication that has been conducted during—

(A) the 5-year period beginning on the date the security clearance was granted, in the case of a Top Secret Clearance, or the date access was granted to a highly sensitive program;

(B) the 10-year period beginning on the date the security clearance was granted in the case of a Secret Clearance; and

(C) the 15-year period beginning on the date the security clearance was granted in the case of a Confidential Clearance.

(6) The term "personnel security investigation" means any investigation required for the purpose of determining the eligi-

bility of any military, civilian, or government contractor personnel to access classified information.

(7) The term "periodic reinvestigations" means investigations conducted for the purpose of updating a previously completed background investigation—

(A) every 5 years in the case of a top secret clearance or access to a highly sensitive program;

(B) every 10 years in the case of a secret clearance; or

(C) every 15 years in the case of a Confidential Clearance.

(8) The term "appropriate committees of Congress" means—

(A) the Permanent Select Committee on Intelligence and the Committees on Armed Services, Homeland Security, Government Reform, and the Judiciary of the House of Representatives; and

(B) the Select Committee on Intelligence and the Committees on Armed Services, Homeland Security and Governmental Affairs, and the Judiciary of the Senate.

(9) ACCESS DETERMINATION.—The term "access determination" means the determination regarding whether an employee—

(A) is eligible for access to classified information in accordance with Executive Order 12968 (60 Fed. Reg. 40245; relating to access to classified information), or any successor thereto, and Executive Order 10865 (25 Fed. Reg. 1583; relating to safeguarding classified information with industry), or any successor thereto; and

(B) possesses a need to know under such an Order.

(b) SELECTION OF ENTITY.—Except as otherwise provided, not later than 90 days after the date of the enactment of this Act, the President shall select a single department, agency, or element of the executive branch to be responsible for—

(1) directing day-to-day oversight of investigations and adjudications for personnel security clearances, including for highly sensitive programs, throughout the United States Government;

(2) developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations for access to highly sensitive programs, including the standardization of security questionnaires, financial disclosure requirements for security clearance applicants, and polygraph policies and procedures;

(3) serving as the final authority to designate an authorized investigative agency or authorized adjudicative agency;

(4) ensuring reciprocal recognition of access to classified information among the agencies of the United States Government, including acting as the final authority to arbitrate and resolve disputes involving the reciprocity of security clearances and access to highly sensitive programs pursuant to subsection (d);

(5) ensuring, to the maximum extent practicable, that sufficient resources are available in each agency to achieve clearance and investigative program goals;

(6) reviewing and coordinating the development of tools and techniques for enhancing the conduct of investigations and granting of clearances; and

(7) not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2014, and consistent with subsection (j)—

(A) developing policies and procedures that permit, to the extent practicable, individuals alleging reprisal for having made a protected disclosure (provided the individual does not disclose classified information or other information contrary to law) to appeal any action affecting an employee's access to classified information and to retain their government employment status while such challenge is pending; and

(B) developing and implementing uniform and consistent policies and procedures to ensure proper protections during the process for denying, suspending, or revoking a security clearance or access to classified information following a protected disclosure, including the ability to appeal such a denial, suspension, or revocation, except that there shall be no appeal of an agency's suspension of a security clearance or access determination for purposes of conducting an investigation, if that suspension lasts no longer than 1 year or the head of the agency or a designee of the head of the agency certifies that a longer suspension is needed before a final decision on denial or revocation to prevent imminent harm to the national security.

(c) PERFORMANCE OF SECURITY CLEARANCE INVESTIGATIONS.—(1) Notwithstanding any other provision of law, not later than 180 days after the date of the enactment of this Act, the President shall, in consultation with the head of the entity selected pursuant to subsection (b), select a single agency of the executive branch to conduct, to the maximum extent practicable, security clearance investigations of employees and contractor personnel of the United States Government who require access to classified information and to provide and maintain all security clearances of such employees and contractor personnel. The head of the entity selected pursuant to subsection (b) may designate other agencies to conduct such investigations if the head of the entity selected pursuant to subsection (b) considers it appropriate for national security and efficiency purposes.

(2) The agency selected under paragraph (1) shall—

(A) take all necessary actions to carry out the requirements of this section, including entering into a memorandum of understanding with any agency carrying out responsibilities relating to security clearances or security clearance investigations before the date of the enactment of this Act;

(B) as soon as practicable, integrate reporting of security clearance applications, security clearance investigations, and determinations of eligibility for security clearances, with the database required by subsection (e); and

(C) ensure that security clearance investigations are conducted in accordance with uniform standards and requirements established under subsection (b), including uniform security questionnaires and financial disclosure requirements.

(d) RECIPROCITY OF SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—(1) All security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be accepted by all agencies.

(2) All security clearance background investigations initiated by an authorized investigative agency shall be transferable to any other authorized investigative agency.

(3)(A) An authorized investigative agency or authorized adjudicative agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination) that exceed requirements specified in Executive Orders establishing security requirements for access to classified information without the approval of the head of the entity selected pursuant to subsection (b).

(B) Notwithstanding subparagraph (A), the head of the entity selected pursuant to subsection (b) may establish such additional requirements as the head of such entity considers necessary for national security purposes.

(4) An authorized investigative agency or authorized adjudicative agency may not conduct an investigation for purposes of determining whether to grant a security clearance to an individual where a current investigation or clearance of equal level already exists or has been granted by another authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may disallow the reciprocal recognition of an individual security clearance by an agency under this section on a case-by-case basis if the head of the entity selected pursuant to subsection (b) determines that such action is necessary for national security purposes.

(6) The head of the entity selected pursuant to subsection (b) shall establish a review procedure by which agencies can seek review of actions required under this section.

(e) DATABASE ON SECURITY CLEARANCES.—(1) Not later than 12 months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall, in cooperation with the heads of the entities selected pursuant to subsections (b) and (c), establish and commence operating and maintaining an integrated, secure, database into which appropriate data relevant to the granting, denial, or revocation of a security clearance or access pertaining to military, civilian, or government contractor personnel shall be entered from all authorized investigative and adjudicative agencies.

(2) The database under this subsection shall function to integrate information from existing Federal clearance tracking systems from other authorized investigative and adjudicative agencies into a single consolidated database.

(3) Each authorized investigative or adjudicative agency shall check the database under this subsection to determine whether an individual the agency has identified as requiring a security clearance has already been granted or denied a security clearance, or has had a security clearance revoked, by any other authorized investigative or adjudicative agency.

(4) The head of the entity selected pursuant to subsection (b) shall evaluate the extent to which an agency is submitting informa-

tion to, and requesting information from, the database under this subsection as part of a determination of whether to certify the agency as an authorized investigative agency or authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may authorize an agency to withhold information about certain individuals from the database under this subsection if the head of the entity considers it necessary for national security purposes.

(f) EVALUATION OF USE OF AVAILABLE TECHNOLOGY IN CLEARANCE INVESTIGATIONS AND ADJUDICATIONS.—(1) The head of the entity selected pursuant to subsection (b) shall evaluate the use of available information technology and databases to expedite investigative and adjudicative processes for all and to verify standard information submitted as part of an application for a security clearance.

(2) The evaluation shall assess the application of the technologies described in paragraph (1) for—

(A) granting interim clearances to applicants at the secret, top secret, and special access program levels before the completion of the appropriate full investigation;

(B) expediting investigations and adjudications of security clearances, including verification of information submitted by the applicant;

(C) ongoing verification of suitability of personnel with security clearances in effect for continued access to classified information;

(D) use of such technologies to augment periodic reinvestigations;

(E) assessing the impact of the use of such technologies on the rights of applicants to verify, correct, or challenge information obtained through such technologies; and

(F) such other purposes as the head of the entity selected pursuant to subsection (b) considers appropriate.

(3) An individual subject to verification utilizing the technology described in paragraph (1) shall be notified of such verification, shall provide consent to such use, and shall have access to data being verified in order to correct errors or challenge information the individual believes is incorrect.

(4) Not later than one year after the date of the enactment of this Act, the head of the entity selected pursuant to subsection (b) shall submit to the President and the appropriate committees of Congress a report on the results of the evaluation, including recommendations on the use of technologies described in paragraph (1).

(g) REDUCTION IN LENGTH OF PERSONNEL SECURITY CLEARANCE PROCESS.—(1) The head of the entity selected pursuant to subsection (b) shall, within 90 days of selection under that subsection, develop, in consultation with the appropriate committees of Congress and each authorized adjudicative agency, a plan to reduce the length of the personnel security clearance process.

(2)(A) To the extent practical the plan under paragraph (1) shall require that each authorized adjudicative agency make a determination on at least 90 percent of all applications for a personnel security clearance within an average of 60 days after the date of receipt of the completed application for a security clearance by an

authorized investigative agency. Such 60-day average period shall include—

(i) a period of not longer than 40 days to complete the investigative phase of the clearance review; and

(ii) a period of not longer than 20 days to complete the adjudicative phase of the clearance review.

(B) Determinations on clearances not made within 60 days shall be made without delay.

(3)(A) The plan under paragraph (1) shall take effect 5 years after the date of the enactment of this Act.

(B) During the period beginning on a date not later than 2 years after the date after the enactment of this Act and ending on the date on which the plan under paragraph (1) takes effect, each authorized adjudicative agency shall make a determination on at least 80 percent of all applications for a personnel security clearance pursuant to this section within an average of 120 days after the date of receipt of the application for a security clearance by an authorized investigative agency. Such 120-day average period shall include—

(i) a period of not longer than 90 days to complete the investigative phase of the clearance review; and

(ii) a period of not longer than 30 days to complete the adjudicative phase of the clearance review.

(h) REPORTS.—(1) Not later than February 15, 2006, and annually thereafter through 2011, the head of the entity selected pursuant to subsection (b) shall submit to the appropriate committees of Congress a report on the progress made during the preceding year toward meeting the requirements of this section.

(2) Each report shall include, for the period covered by such report—

(A) the periods of time required by the authorized investigative agencies and authorized adjudicative agencies for conducting investigations, adjudicating cases, and granting clearances, from date of submission to ultimate disposition and notification to the subject and the subject's employer;

(B) a discussion of any impediments to the smooth and timely functioning of the requirements of this section; and

(C) such other information or recommendations as the head of the entity selected pursuant to subsection (b) considers appropriate.

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such sums as may be necessary for fiscal year 2005 and each fiscal year thereafter for the implementation, maintenance, and operation of the database required by subsection (e).

(j) RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.—

(1) IN GENERAL.—Agency personnel with authority [over] *to take, direct others to take, recommend, or approve* personnel security clearance or access determinations shall not take or fail to take, or threaten to take or fail to take, any action with respect to any employee's security clearance or access determination in retaliation for—

(A) any lawful disclosure of information to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose) or *a su-*

*pervisor in the employee's direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including* the head of the employing agency (or employee designated by the head of that agency for such purpose) by an employee that the employee reasonably believes evidences—

(i) a violation of any Federal law, rule, or regulation; or

(ii) [gross mismanagement] *mismanagement*, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(B) any lawful disclosure to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee reasonably believes evidences—

(i) a violation of any Federal law, rule, or regulation; or

(ii) [gross mismanagement] *mismanagement*, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(C) any lawful disclosure that complies with—

(i) subsections (a)(1), (d), and [(h)] *(g)* of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

(ii) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or

(iii) subparagraphs (A), (D), and (I) of section 103H(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)); and

(D) if the actions do not result in the employee or applicant unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

(i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

(ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or

(iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.

(2) RULE OF CONSTRUCTION.—Consistent with the protection of sources and methods, nothing in paragraph (1) shall be construed to authorize the withholding of information from Congress or the taking of any personnel action *or clearance action* against an employee who lawfully discloses information to Congress.

(3) [DISCLOSURES.—

[(A) IN GENERAL.—] *DISCLOSURES.—A disclosure shall not be excluded from paragraph (1) because—* [A disclosure shall not be excluded from paragraph (1) because—]

[(i)] *(A)* the disclosure was made to a person, including a supervisor, who participated in an activity that the employee reasonably believed to be covered by paragraph (1)(A)(ii);

[(ii)] *(B)* the disclosure revealed information that had been previously disclosed;

[(iii)] *(C)* the disclosure was not made in writing;

[(iv)] *(D)* the disclosure was made while the employee was off duty; [or]

[(v)] *(E)* of the amount of time which has passed since the occurrence of the events described in the disclosure[.]*; or*

[(B) REPRISALS.—If a disclosure is made during the normal course of duties of an employee, the disclosure shall not be excluded from paragraph (1) if any employee who has authority to take, direct others to take, recommend, or approve any personnel action with respect to the employee making the disclosure, took, failed to take, or threatened to take or fail to take a personnel action with respect to that employee in reprisal for the disclosure.]

*(F) the disclosure was made during the normal course of duties of an employee.*

(4) AGENCY ADJUDICATION.—

(A) REMEDIAL PROCEDURE.—An employee or former employee who believes that he or she has been subjected to a reprisal prohibited by paragraph (1) may, within 90 days *(except as provided by subparagraph (D))* after the issuance of notice of such decision, appeal that decision within the agency of that employee or former employee through proceedings authorized by subsection (b)(7), except that there shall be no appeal of an agency's suspension of a security clearance or access determination for purposes of conducting an investigation, if that suspension lasts not longer than 1 year (or a longer period in accordance with a certification made under subsection (b)(7)).

(B) CORRECTIVE ACTION.—If, in the course of proceedings authorized under subparagraph (A), it is determined that the adverse security clearance or access determination violated paragraph (1), the agency shall take specific corrective action to return the employee or former employee, as nearly as practicable and reasonable, to the position such employee or former employee would have held had the violation not occurred. Such corrective action may include back pay and related benefits, travel expenses, and compensatory damages not to exceed $300,000.

(C) CONTRIBUTING FACTOR.—In determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual, unless the agency demonstrates by a preponderance of the evidence that it would have taken the same action in the absence of such disclosure, giving the utmost deference to the agency's assessment of the particular threat to the na-

tional security interests of the United States in the instant matter.

*(D) TOLLING.—The time requirement established by subparagraph (A) for an employee or former employee to appeal the decision of an agency may be tolled if the employee or former employee presents substantial credible evidence showing why the employee or former employee did not timely initiate the appeal and why the enforcement of the time requirement would be unfair, such as evidence showing that the employee or former employee—*

*(i) did not receive notice of the decision; or*

*(ii) could not timely initiate the appeal because of factors beyond the control of the employee or former employee.*

(5) APPELLATE REVIEW OF SECURITY CLEARANCE ACCESS DETERMINATIONS BY DIRECTOR OF NATIONAL INTELLIGENCE.—

(A) APPEAL.—Within 60 days after receiving notice of an adverse final agency determination under a proceeding under paragraph (4), an employee or former employee may appeal that determination in accordance with the procedures established under subparagraph (B).

(B) POLICIES AND PROCEDURES.—The Director of National Intelligence, in consultation with the Attorney General and the Secretary of Defense, shall develop and implement policies and procedures for adjudicating the appeals authorized by subparagraph (A).

(C) CONGRESSIONAL NOTIFICATION.—Consistent with the protection of sources and methods, at the time the Director of National Intelligence issues an order regarding an appeal pursuant to the policies and procedures established by this paragraph, the Director of National Intelligence shall notify the congressional intelligence committees.

(6) JUDICIAL REVIEW.—Nothing in this section shall be construed to permit or require judicial review of any—

(A) agency action under this section; or

(B) action of the appellate review procedures established under paragraph (5).

(7) PRIVATE CAUSE OF ACTION.—Nothing in this section shall be construed to permit, authorize, or require a private cause of action to challenge the merits of a security clearance determination.

*(8) ENFORCEMENT.—Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.*

**[**(8)**]** *(9)* INCLUSION OF CONTRACTOR EMPLOYEES.—In this subsection, the term "employee" includes an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of an agency. With respect to such employees, the term "employing agency" shall be deemed to be the contracting agency.

* * * * * * *

**INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2017**

* * * * * * *

# DIVISION N—INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2017

* * * * * * *

# TITLE VI—REPORTS AND OTHER MATTERS

* * * * * * *

**SEC. 608. IMPROVEMENT IN GOVERNMENT CLASSIFICATION AND DECLASSIFICATION.**

(a) REVIEW OF GOVERNMENT CLASSIFICATION AND DECLASSIFICATION.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall—

(1) review the system by which the Government classifies and declassifies information;

(2) develop recommendations—

(A) to make such system a more effective tool for the protection of information relating to national security;

(B) to improve the sharing of information with partners and allies of the Government; and

(C) to support the appropriate declassification of information; and

(3) submit to the congressional intelligence committees a report with—

(A) the findings of the Director with respect to the review conducted under paragraph (1); and

(B) the recommendations developed under paragraph (2).

[(b) ANNUAL CERTIFICATION OF CONTROLLED ACCESS PROGRAMS.—

[(1) IN GENERAL.—Not less frequently than once each year, the Director of National Intelligence shall certify in writing to the congressional intelligence committees whether the creation, validation, or substantial modification, including termination, for all existing and proposed controlled access programs, and the compartments and subcompartments within each, are substantiated and justified based on the information required by paragraph (2).

[(2) INFORMATION REQUIRED.—Each certification pursuant to paragraph (1) shall include—

[(A) the rationale for the revalidation, validation, or substantial modification, including termination, of each controlled access program, compartment and subcompartment;

[(B) the identification of a control officer for each controlled access program; and

[(C) a statement of protection requirements for each controlled access program.]

* * * * * * *

---

## CENTRAL INTELLIGENCE AGENCY ACT OF 1949

* * * * * * *

***SEC. 15A. PROTECTION OF CERTAIN FACILITIES AND ASSETS OF CENTRAL INTELLIGENCE AGENCY FROM UNMANNED AIRCRAFT.***

*(a) AUTHORITY.—In accordance with subsection (b), the Director shall have the same authority for the Agency as is available to the Secretary of Homeland Security for the Department of Homeland Security and the Attorney General for the Department of Justice under section 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n), and shall be subject to the same limitations and requirements under such section.*

*(b) ADMINISTRATION.—For purposes of subsection (a)—*

*(1) the reference in subsection (i) of section 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n) to "the date that is 4 years after the date of enactment of this section" shall be deemed to be a reference to "October 5, 2026";*

*(2) the term "appropriate congressional committees" as defined in paragraph (1) of subsection (k) of such section shall be deemed to mean the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate; and*

*(3) the term "covered facility or asset" as defined in paragraph (3) of such subsection (k) shall be deemed to mean installations, property, and persons—*

*(A) that are located in the United States;*

*(B) for which the Director may provide protection pursuant to section 5(a)(4) or 15(a)(1) of this Act; and*

*(C) that the Director identifies as high-risk and a potential target for unlawful unmanned aircraft activity.*

* * * * * * *

**SEC. 19A. SPECIAL RULES FOR CERTAIN INDIVIDUALS INJURED BY REASON OF WAR, INSURGENCY, HOSTILE ACT, TERRORIST ACTIVITIES, OR INCIDENTS DESIGNATED BY THE DIRECTOR.**

(a) DEFINITIONS.—In this section:

(1) COVERED DEPENDENT.—The term "covered dependent" means a family member (as defined by the Director) of a covered employee who, on or after September 11, 2001—

(A) accompanies the covered employee to an assigned duty station in a foreign country; and

(B) becomes injured by reason of a qualifying injury.

(2) COVERED EMPLOYEE.—The term "covered employee" means an officer or employee of the Central Intelligence Agency who, on or after September 11, 2001, becomes injured by reason of a qualifying injury.

(3) COVERED INDIVIDUAL.—The term "covered individual" means an individual who—

(A)(i) is detailed to the Central Intelligence Agency from other agencies of the United States Government or from the Armed Forces; or

(ii) is affiliated with the Central Intelligence Agency, as determined by the Director; and

(B) who, on or after September 11, 2001, becomes injured by reason of a qualifying injury.

(4) QUALIFYING INJURY.—The term "qualifying injury" means the following:

(A) With respect to a covered dependent, an injury incurred—

(i) during a period in which the covered dependent is accompanying the covered employee to an assigned duty station in a foreign country;

(ii) in connection with war, insurgency, hostile act, terrorist activity, or an incident designated for purposes of this section by the Director; and

(iii) that was not the result of the willful misconduct of the covered dependent.

(B) With respect to a covered employee or a covered individual—

(i) an injury incurred—

(I) during a period of assignment to a duty station in a foreign country;

(II) in connection with war, insurgency, hostile act, or terrorist activity; and

(III) that was not the result of the willful misconduct of the covered employee or the covered individual; or

(ii) an injury incurred—

(I) in connection with an incident designated for purposes of this section by the Director; and

(II) that was not the result of the willful misconduct of the covered employee or the covered individual.

(b) ADJUSTMENT OF COMPENSATION FOR TOTAL DISABILITY RESULTING FROM CERTAIN INJURIES.—

(1) INCREASE.—The Director may increase the amount of monthly compensation paid to a covered employee under section 8105 of title 5, United States Code. Subject to paragraph (2), the Director may determine the amount of each such increase by taking into account—

(A) the severity of the qualifying injury;

(B) the circumstances by which the covered employee became injured; and

(C) the seniority of the covered employee.

(2) MAXIMUM.—Notwithstanding chapter 81 of title 5, United States Code, the total amount of monthly compensation increased under paragraph (1) may not exceed the monthly pay of the maximum rate of basic pay for GS–15 of the General Schedule under section 5332 of such title.

(c) COSTS FOR TREATING QUALIFYING INJURIES.—The Director may pay the costs of treating a qualifying injury of a covered employee, a covered individual, or a covered dependent, or may reimburse a covered employee, a covered individual, or a covered de-

pendent for such costs, that are not otherwise covered by chapter 81 of title 5, United States Code, or other provision of Federal law.

(d) AUTHORITY TO MAKE PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN.—

(1) DEFINITIONS.—In this subsection:

(A) COVERED DEPENDENT.—The term "covered dependent" has the meaning given such term in subsection (a), except that the assigned duty station need not be in a foreign country.

(B) QUALIFYING INJURY.—The term "qualifying injury" has the meaning given such term in subsection (a), except that the assigned duty station need not be in a foreign country.

(2) AUTHORITY.—Notwithstanding any other provision of law but subject to paragraph (3), the Director may provide payment to a covered dependent, a covered employee, and a covered individual for a qualifying injury to the brain.

(3) LIMITATIONS.—

(A) APPROPRIATIONS REQUIRED.—Payment under paragraph (2) in a fiscal year may only be made using amounts appropriated in advance specifically for payments under such paragraph in such fiscal year.

(B) MATTER OF PAYMENTS.—Payments under paragraph (2) using amounts appropriated for such purpose shall be made on a first come, first serve, or pro rata basis.

(C) AMOUNTS OF PAYMENTS.—The total amount of funding obligated for payments under paragraph (2) may not exceed the amount specifically appropriated for providing payments under such paragraph during its period of availability.

(4) REGULATIONS.—

(A) IN GENERAL.—The Director shall prescribe regulations to carry out this subsection.

(B) ELEMENTS.—The regulations prescribed under subparagraph (A) shall include regulations detailing fair and equitable criteria for payment under paragraph (2).

*(5) NO EFFECT ON OTHER BENEFITS.—Payments made under paragraph (2) are supplemental to any other benefit furnished by the United States Government for which a covered dependent, covered employee, or covered individual is entitled, and the receipt of such payments may not affect the eligibility of such a person to any other benefit furnished by the United States Government.*

* * * * * * *

***SEC. 26. COMPENSATION AND PROFESSIONAL STANDARDS FOR CERTAIN MEDICAL OFFICERS.***

*(a) OFFICE OF MEDICAL SERVICES.—There is in the Agency an Office of Medical Services.*

*(b) COMPENSATION.—Beginning not later than 1 year after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, each medical officer of the Office of Medical Services who meets the qualifications under subsection (c) shall be compensated during a pay period pursuant to a pay range that is equal to the pay range published in the Federal Register pursuant to sec-*

*tion 7431(e)(1)(C) of title 38, United States Code (for the corresponding pay period), for a physician in the Veterans Health Administration in the District of Columbia region with a medical subspecialty that is the equivalent of the medical subspecialty of the officer.*

*(c) CLINICAL PRACTICE QUALIFICATIONS.—A medical officer meets the qualifications under this subsection if the officer provides direct care services to patients in connection with the official duties of the officer and—*

*(1) maintains current, active, full, and unrestricted licensure or registration as a physician from a State, the District of Columbia, or a commonwealth or territory of the United States;*

*(2) holds active board certification and maintains accreditation in an American Board of Medical Specialties direct care clinical specialty; and*

*(3) except as provided in subsection (d), maintains a minimum of 160 hours per year of clinical practice in an accredited clinic or hospital facility that is not affiliated with the Central Intelligence Agency.*

*(d) EXCEPTION FOR OVERSEAS SERVICE.—If a medical officer is a medical officer located in a duty station outside of the United States pursuant to a permanent change of station and greater than 50 percent of the official duties of the officer in such duty station involve direct patient care, the officer, in lieu of performing the minimum hours under subsection (c)(3) on an annual basis, may perform up to 480 hours of clinical practice as specified in such subsection prior to such change of station, to fulfil in advance the requirement under such subsection for up to 3 years.*

*(e) CLINICAL PRACTICE HOURS.—The head of the Office of Medical Services shall make available to medical officers excused absence time to allow for the maintenance of clinical practice hours in accordance with subsection (c)(3).*

***SEC. 27. MEDICAL ADVISORY BOARD.***

*(a) ESTABLISHMENT.—The Director shall establish within the Agency a medical advisory board (in this section referred to as the "Board").*

*(b) DUTIES.—The Board shall—*

*(1) conduct a study on the Office of Medical Services of the Agency, and submit reports regarding such study, in accordance with subsection (c); and*

*(2) upon request, provide advice and guidance in connection with any independent review of the Office conducted by an inspector general.*

*(c) STUDY.—*

*(1) OBJECTIVES.—In conducting the study under subsection (b)(1), the Board shall seek to—*

*(A) contribute to the modernization and reform of the Office of Medical Services;*

*(B) ensure that the activities of the Office are of the highest professional quality; and*

*(C) ensure that all medical care provided by the Office is provided in accordance with the highest professional medical standards.*

*(2) REPORTS.—The Board shall submit to the congressional intelligence committees, in writing—*

*(A) interim reports on the study; and*

*(B) a final report on the study, which shall—*

*(i) set forth in detail the findings of the study and the recommendations of the Board, based on such findings and taking into consideration the objectives under paragraph (1), regarding any changes to the activities of the Office of Medical Services; and*

*(ii) include, as applicable, any additional or dissenting views submitted by a member of the Board.*

*(d) MEMBERSHIP.—*

*(1) NUMBER AND APPOINTMENT.—The Board shall be composed of 11 members, appointed as follows:*

*(A) 2 members appointed by the Chairman of the Permanent Select Committee on Intelligence of the House of Representatives.*

*(B) 2 members appointed by the ranking minority member of the Permanent Select Committee on Intelligence of the House of Representatives.*

*(C) 2 members appointed by the Chairman of the Select Committee on Intelligence of the Senate.*

*(D) 2 members appointed by the Vice Chairman of the Select Committee on Intelligence of the Senate.*

*(E) 3 members appointed by the Director of National Intelligence.*

*(2) CHAIRPERSON.—During the first meeting under subsection (e)(1), the members of the Board shall elect a Chairperson of the Board. In addition to meeting the criteria under paragraph (3), the Chairperson may not be an employee, or former employee, of the Agency.*

*(3) CRITERIA.—The members appointed under paragraph (1) shall meet the following criteria:*

*(A) Each member shall be a recognized expert in at least 1 medical field, as demonstrated by appropriate credentials.*

*(B) Each member shall possess significant and diverse medical experience, including clinical experience.*

*(C) Each member shall hold a security clearance at the top secret level and be able to access sensitive compartmented information.*

*(4) TERMS.—*

*(A) IN GENERAL.—Each member, including the Chairperson, shall be appointed or elected, as applicable, for the life of the Board.*

*(B) VACANCIES.—Any vacancy in the Board occurring prior to the expiration of the term under subparagraph (A) shall be filled in the manner in which the original appointment or election was made.*

*(5) COMPENSATION AND TRAVEL EXPENSES.—*

*(A) COMPENSATION.—Except as provided in subparagraph (B), each member of the Board, including the Chairperson, may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during*

*which that member is engaged in the actual performance of the duties under subsection (b).*

*(B) EXCEPTION FOR FEDERAL EMPLOYEES.—Members of the Board, including the Chairperson, who are officers or employees of the United States shall receive no additional pay by reason of the service of the member on the Board.*

*(C) TRAVEL EXPENSES.—Each member of the Board, including the Chairperson, while away from the home or regular places of business of the member in the performance of services for the Board, may be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703 of title 5, United States Code.*

*(6) DETAILEES.—*

*(A) IN GENERAL.—Upon request of the Board, the Director of National Intelligence may detail to the Board, without reimbursement from the Board, any of the personnel of the Office of the Director of National Intelligence to assist in carrying out the duties under subsection (b). Any such detailed personnel shall retain the rights, status, and privileges of the regular employment of the personnel without interruption.*

*(B) CLEARANCE.—Any personnel detailed to the Board under subparagraph (A) shall possess a security clearance in accordance with applicable laws and regulations concerning the handling of classified information.*

*(e) MEETINGS.—*

*(1) BOARD MEETINGS.—The Board shall meet not less frequently than on a quarterly basis.*

*(2) MEETINGS WITH CONGRESS.—The Board shall meet with the congressional intelligence committees on a biannual basis.*

*(f) INFORMATION ACCESS.—*

*(1) IN GENERAL.—Except as provided in paragraph (2), the Board may secure directly from any department or agency of the United States Government information necessary to enable it to carry out the duties under subsection (b) and, upon request of the Chairperson of the Board, the head of that department or agency shall furnish such information to the Board.*

*(2) EXCEPTION.—The Director (without delegation) may deny a request for information made by the Board pursuant to paragraph (1), regardless of the agency from which such information is requested.*

*(3) NOTIFICATION REQUIREMENT.—If the Director denies a request under paragraph (2), not later than 15 days after the date of such denial, the Director shall submit to the congressional intelligence committees a written notification of such denial.*

*(4) BRIEFINGS.—The Director shall ensure that the Board receives comprehensive briefings on all activities of the Office of Medical Services, including by promptly scheduling such briefings at the request of the Board.*

*(g) TERMINATION.—The Board shall terminate on the date that is 5 years after the date of the first meeting of the Board.*

*(h) DEFINITIONS.—In this section, the terms "congressional intelligence committees" and "intelligence community" have the mean-*

*ings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).*

---

## TITLE 10, UNITED STATES CODE

* * * * * * *

# SUBTITLE A—GENERAL MILITARY LAW

* * * * * * *

# PART II—PERSONNEL

* * * * * * *

## CHAPTER 81—CIVILIAN EMPLOYEES

* * * * * * *

### § 1599h. Personnel management authority to attract experts in science and engineering

(a) PROGRAMS AUTHORIZED.—

(1) LABORATORIES OF THE MILITARY DEPARTMENTS.—The Secretary of Defense may carry out a program of personnel management authority provided in subsection (b) in order to facilitate recruitment of eminent experts in science or engineering for such laboratories of the military departments as the Secretary shall designate for purposes of the program for research and development projects of such laboratories.

(2) DARPA.—The Director of the Defense Advanced Research Projects Agency may carry out a program of personnel management authority provided in subsection (b) in order to facilitate recruitment of eminent experts in science or engineering for research and development projects and to enhance the administration and management of the Agency.

(3) DOTE.—The Director of the Office of Operational Test and Evaluation may carry out a program of personnel management authority provided in subsection (b) in order to facilitate recruitment of eminent experts in science or engineering to support operational test and evaluation missions of the Office.

(4) STRATEGIC CAPABILITIES OFFICE.—The Director of the Strategic Capabilities Office may carry out a program of personnel management authority provided in subsection (b) in order to facilitate recruitment of eminent experts in science or engineering for the Office.

(5) DIU.—The Director of the Defense Innovation Unit may carry out a program of personnel management authority provided in subsection (b) in order to facilitate recruitment of eminent experts in science or engineering for the Unit.

(6) JOINT ARTIFICIAL INTELLIGENCE CENTER.—The Director of the Joint Artificial Intelligence Center may carry out a program of personnel management authority provided in subsection (b) in order to facilitate recruitment of eminent experts in science or engineering for the Center. The authority to carry

out the program under this paragraph shall terminate on December 31, 2024.

(7) NGA.—The Director of the National Geospatial-Intelligence Agency may carry out a program of personnel management authority provided in subsection (b) in order to facilitate recruitment of eminent experts in science or engineering for research and development projects and to enhance the administration and management of the Agency.

(7) SDA.—The Director of the Space Development Agency may carry out a program of personnel management authority provided in subsection (b) in order to facilitate recruitment of eminent experts in science or engineering for research and development projects and to enhance the administration and management of the Agency. The authority to carry out the program under this paragraph shall terminate on December 31, 2025.

(8) UNITED STATES CYBER COMMAND.—The Commander of United States Cyber Command may carry out a program of personnel management authority provided in subsection (b) in order to facilitate the recruitment of eminent experts in computer science, data science, engineering, mathematics, and computer network exploitation within the headquarters of United States Cyber Command and the Cyber National Mission Force.

(b) PERSONNEL MANAGEMENT AUTHORITY.—Under a program under subsection (a), the official responsible for administration of the program may—

(1) without regard to any provision of title 5 governing the appointment of employees in the civil service—

(A) in the case of the laboratories of the military departments designated pursuant to subsection (a)(1), appoint scientists and engineers to a total of not more than 40 scientific and engineering positions in such laboratories;

(B) in the case of the Defense Advanced Research Projects Agency, appoint individuals to a total of not more than 140 positions in the Agency, of which not more than 5 such positions may be positions of administration or management of the Agency;

(C) in the case of the Office of Operational Test and Evaluation, appoint scientists and engineers to a total of not more than 10 scientific and engineering positions in the Office;

(D) in the case of the Strategic Capabilities Office, appoint scientists and engineers to a total of not more than 5 scientific and engineering positions in the Office;

(E) in the case of the Defense Innovation Unit, appoint scientists and engineers to a total of not more than 5 scientific and engineering positions in the Unit;

(F) in the case of the Joint Artificial Intelligence Center, appoint scientists and engineers to a total of not more than 5 scientific and engineering positions in the Center;

(G) in the case of the National Geospatial-Intelligence Agency, appoint individuals to a total of not more than 7 positions in the Agency, of which not more than 2 such po-

sitions may be positions of administration or management in the Agency;

(G) [3] in the case of the Space Development Agency, appoint individuals to a total of not more than 10 positions in the Agency, of which not more than 3 such positions may be positions of administration or management of the Agency; and

(H) in the case of United States Cyber Command, appoint computer scientists, data scientists, engineers, mathematicians, and computer network exploitation specialists to a total of not more than 10 scientific and engineering positions in the Command;

(2) notwithstanding any provision of title 5 governing the rates of pay or classification of employees in the executive branch, prescribe the rates of basic pay for positions to which employees are appointed under paragraph (1)—

(A) in the case of employees appointed pursuant to ⟦paragraph (1)(B)⟧ *subparagraph (B) of paragraph (1)* to any of 5 positions designated by the Director of the Defense Advanced Research Projects Agency for purposes of this subparagraph *or employees appointed pursuant to the first subparagraph (G) of such paragraph to any of 2 positions of administration or management designated by the Director of the National Geospatial-Intelligence Agency for purposes of this subparagraph*, at rates not in excess of a rate equal to 150 percent of the maximum rate of basic pay authorized for positions at Level I of the Executive Schedule under section 5312 of title 5; and

(B) in the case of any other employee appointed pursuant to paragraph (1), at rates not in excess of the maximum rate of basic pay authorized for senior-level positions under section 5376 of title 5; and

(3) pay any employee appointed under paragraph (1), other than an employee appointed to a position designated as described in paragraph (2)(A), payments in addition to basic pay within the limit applicable to the employee under subsection (d).

(c) LIMITATION ON TERM OF APPOINTMENT.—

(1) IN GENERAL.—Except as provided in paragraph (2), the service of an employee under an appointment under subsection (b)(1) may not exceed four years.

(2) EXTENSION.—The official responsible for the administration of a program under subsection (a) may, in the case of a particular employee under the program, extend the period to which service is limited under paragraph (1) by up to two years if the official determines that such action is necessary to promote the efficiency of a laboratory of a military department, the Defense Advanced Research Projects Agency, the Office of Operational Test and Evaluation, the Strategic Capabilities Office, the Defense Innovation Unit, the Joint Artificial Intelligence Center, or the National Geospatial-Intelligence Agency, as applicable.

(d) MAXIMUM AMOUNT OF ADDITIONAL PAYMENTS PAYABLE.—Notwithstanding any other provision of this section or section 5307 of title 5, no additional payments may be paid to an employee under

subsection (b)(3) in any calendar year if, or to the extent that, the employee's total annual compensation in such calendar year will exceed the maximum amount of total annual compensation payable at the salary set in accordance with section 104 of title 3.

* * * * * * *

---

**NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2017**

* * * * * * *

# DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

* * * * * * *

# TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

* * * * * * *

## Subtitle C—Cyberspace-Related Matters

* * * * * * *

**SEC. 1642. LIMITATION ON TERMINATION OF DUAL-HAT ARRANGEMENT FOR COMMANDER OF THE UNITED STATES CYBER COMMAND.**

[(a) LIMITATION ON TERMINATION OF DUAL-HAT ARRANGEMENT.—The Secretary of Defense may not terminate the dual-hat arrangement until the date on which the Secretary and the Chairman of the Joint Chiefs of Staff jointly certify to the appropriate committees of Congress that—

[(1) the Secretary and the Chairman carried out the assessment under subsection (b);

[(2) each of the conditions described in paragraph (2)(C) of such subsection has been met; and

[(3) termination of the dual-hat arrangement will not pose risks to the military effectiveness of the United States Cyber Command that are unacceptable to the national security interests of the United States.

[(b) ASSESSMENT.—

[(1) IN GENERAL.—The Secretary and the Chairman shall jointly assess the military and intelligence necessity and benefit of the dual-hat arrangement.

[(2) ELEMENTS.—The assessment under paragraph (1) shall include the following elements:

[(A) An evaluation of the operational dependence of the United States Cyber Command on the National Security Agency.

[(B) An evaluation of the ability of the United States Cyber Command and the National Security Agency to

carry out their respective roles and responsibilities independently.

[(C) A determination of whether the following conditions have been met:

[(i) Robust operational infrastructure has been deployed that is sufficient to meet the unique cyber mission needs of the United States Cyber Command and the National Security Agency, respectively.

[(ii) Robust command and control systems and processes have been established for planning, deconflicting, and executing military cyber operations and national intelligence operations.

[(iii) The tools, weapons, and accesses used in and available for military cyber operations are sufficient for achieving required effects and United States Cyber Command is capable of acquiring or developing such tools, weapons, and accesses.

[(iv) Capabilities have been established to enable intelligence collection and operational preparation of the environment for cyber operations.

[(v) Capabilities have been established to train cyber operations personnel, test cyber capabilities, and rehearse cyber missions.

[(vi) The Cyber Mission Force has achieved full operational capability and has demonstrated the capacity to execute the cyber missions of the Department, including the following:

[(I) Execution of national-level missions through cyberspace, including deterrence and disruption of adversary cyber activity.

[(II) Defense of the Department of Defense Information Network.

[(III) Support for other combatant commands, including targeting of adversary military assets.

[(c) BIANNUAL BRIEFING.—

[(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this subsection and biannually thereafter, the Secretary of Defense and the Director of National Intelligence shall provide to the appropriate committees of Congress briefings on the nature of the National Security Agency and United States Cyber Command's current and future partnership. Briefings under this subsection shall not terminate until the certification specified in subsection (a) is issued.

[(2) ELEMENTS.—Each briefing under this subsection shall include status updates on the current and future National Security Agency-United States Cyber Command partnership efforts, including relating to the following:

[(A) Common infrastructure and capability acquisition.

[(B) Operational priorities and partnership.

[(C) Research and development partnership.

[(D) Executed documents, written memoranda of agreements or understandings, and policies issued governing such current and future partnership.

[(E) Projected long-term efforts.]

*(a) LIMITATION ON TERMINATION OF DUAL-HAT ARRANGEMENT.—The Secretary of Defense may not terminate the dual-hat arrangement until the date on which the Secretary submits to the appropriate committees of Congress the certification under subsection (b)(1). The Secretary shall implement such termination by not later than the first day of the fiscal year following the fiscal year in which the Secretary submits such certification.*

*(b) ANNUAL SUBMISSION OF INFORMATION.—Together with the defense budget materials for fiscal year 2023, and annually thereafter until the termination of the dual-hat arrangement, the Secretary of Defense, in coordination with the Director of National Intelligence, shall submit to the appropriate committees of Congress a report containing either of the following:*

*(1) A certification that the United States Cyber Command has met each of the following conditions:*

*(A) Sufficient operational infrastructure has been deployed to meet the unique cyber mission needs of the United States Cyber Command.*

*(B) Sufficient command and control systems and processes have been established for planning, deconflicting, and executing military cyber operations.*

*(C) Capabilities have been established to enable intelligence collection and operational preparation of the environment for cyber operations consistent with the United States Cyber Command reaching full operational status.*

*(D) Mechanisms have been established to train cyber operations personnel, test cyber capabilities, and rehearse cyber missions.*

*(E) The United States Cyber Command has achieved full operational capability.*

*(2) If the Secretary, in coordination with the Director, is not able to make the certification under paragraph (1)—*

*(A) an identification of the items contained in the defense budget materials that are related to meeting the conditions specified in such paragraph; and*

*(B) an assessment of the funding required to meet such conditions during the period covered by the future-years defense program under section 221 of title 10, United States Code.*

[(d)] *(c)* DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means—

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

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

(2) DUAL-HAT ARRANGEMENT.—The term "dual-hat arrangement" means the arrangement under which the Commander of the United States Cyber Command also serves as the Director of the National Security Agency.

*(3) DEFENSE BUDGET MATERIALS.—The term "defense budget materials" has the meaning given that term in section 231(f) of title 10, United States Code.*

* * * * * * *

---

## SECTION 901 OF TITLE IX OF DIVISION J OF THE FURTHER CONSOLIDATED APPROPRIATIONS ACT, 2020

**SEC. 901. SPECIAL RULES FOR CERTAIN MONTHLY WORKERS' COMPENSATION PAYMENTS AND OTHER PAYMENTS FOR DEPARTMENT OF STATE PERSONNEL UNDER CHIEF OF MISSION AUTHORITY.**

(a) ADJUSTMENT OF COMPENSATION FOR CERTAIN INJURIES.—

(1) INCREASE.—The Secretary of State or the head of any other Federal agency may pay an additional monthly monetary benefit, provided that the covered employee is receiving benefits under section 8105 or 8106 of title 5, United States Code, and may determine the amount of each monthly monetary benefit amount by taking into account—

(A) the severity of the qualifying injury;

(B) the circumstances by which the covered employee became injured; and

(C) the seniority of the covered employee, particularly for purposes of compensating for lost career growth.

(2) MAXIMUM.—Notwithstanding chapter 81 of title 5, United States Code, the total amount of monthly compensation increased under paragraph (1) may not exceed the monthly pay of the maximum rate of basic pay for GS-15 of the General Schedule under section 5332 of such title.

(b) COSTS FOR TREATING QUALIFYING INJURIES.—The Secretary of State may pay the costs of or reimburse for diagnosing and treating—

(1) a qualifying injury of a covered employee for such costs, that are not otherwise covered by chapter 81 of title 5, United States Code, or other provision of Federal law; or

(2) a covered individual, or a covered dependent, for such costs that are not otherwise covered by Federal law.

(c) INFORMATION EXCHANGE.—To avoid duplicate or otherwise improper payments under this subsection, the Secretary of Labor, the Secretary of State, and, as appropriate, the head of any other Federal agency paying benefits under this section shall exchange information about the amounts paid for treatment of qualifying injuries.

(d) REGULATIONS.—Not later than 120 days after the date of the enactment of this Act, the Secretary of State shall—

(1) prescribe regulations ensuring the fair and equitable implementation of this section; and

(2) submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives such regulations.

(e) DEFINITIONS.—In this section:

(1) COVERED DEPENDENT.—The term "covered dependent" means a family member (as defined by the Secretary of State) of a employee who, on or after January 1, 2016—

(A) accompanies the employee to an assigned duty station in a foreign country under chief of mission authority; and

(B) becomes injured by reason of a qualifying injury.

(2) COVERED EMPLOYEE.—The term "covered employee" means an employee of the Federal Government who, on or after January 1, 2016, becomes injured by reason of a qualifying injury and was assigned to a duty station in the Republic of Cuba, the People's Republic of China, or another foreign country designated by the Secretary of State pursuant to subsection (f), but does not include an individual receiving compensation under section 19A of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b).

(3) COVERED INDIVIDUAL.—The term "covered individual" means an individual who, on or after January 1, 2016, becomes injured by reason of a qualifying injury and is—

(A) detailed to a duty station in the Republic of Cuba, the People's Republic of China, or another foreign country designated by the Secretary of State pursuant to subsection (f); or

(B) affiliated with the Department of State, as determined by the Secretary of State.

(4) QUALIFYING INJURY.—The term "qualifying injury" means the following:

(A) With respect to a covered dependent, an injury incurred—

(i) during a period in which the covered dependent is accompanying an employee to an assigned duty station in the Republic of Cuba, the People's Republic of China, or another foreign country designated by the Secretary of State pursuant to subsection (f);

(ii) in connection with war, insurgency, hostile act, terrorist activity, or other incident designated by the Secretary of State; and

(iii) that was not the result of the willful misconduct of the covered dependent.

(B) With respect to a covered employee or a covered individual, an injury incurred—

(i) during a period of assignment to a duty station in the Republic of Cuba, the People's Republic of China, or another country designated by the Secretary of State pursuant to subsection (f);

(ii) in connection with war, insurgency, hostile act, terrorist activity, or other incident designated by the Secretary of State; and

(iii) that was not the result of the willful misconduct of the covered employee or the covered individual.

(f) DESIGNATION BY THE SECRETARY OF STATE OF ANOTHER FOREIGN COUNTRY OR DUTY STATION.—The Secretary of State may designate another foreign country for the purposes of this section, provided that the Secretary reports such designation to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives, and includes in such report a rationale for each such designation. The Secretary of State may not designate an added foreign country or duty station for purposes

of providing additional monetary benefit pursuant to subsection (a), (b), or (i) for a qualifying injury to covered employees, covered dependents, or covered individuals under this section unless the Secretary of State—

(1) provides to the Committees on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives 30 days' notice of the designation of a particular additional country or duty station and the rationale for such addition; and

(2) provides no such additional monetary benefit pursuant to subsection (a), (b), or (i) to covered employees, covered dependents, or covered individuals for a qualifying injury until the 30-day notice period expires, unless there is written agreement by both the Chair and Ranking Members of both the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives that there is no objection to proceeding with provision of such monetary benefit compensation in less than 30 days.

(g) TREATMENT OF AMOUNTS.—For purposes of section 104 of the Internal Revenue Code of 1986, amounts paid pursuant to this section shall be treated as amounts described in subsection (a)(5) of such section.

(h) APPLICATION.—

(1) ADJUSTMENT OF COMPENSATION PROVISION.—Subsections (a) and (b) shall apply with respect to—

(A) payments made to covered employees (as defined in such section) under section 8105 or 8106 of title 5, United States Code, beginning on or after January 1, 2016; and

(B) diagnosis or treatment described in subsection (b) occurring on or after January 1, 2016.

(2) OTHER PAYMENT PROVISION.—Payment under subsection (i) may be made available for a qualifying injury (as defined in such subsection) that occurs before, on, or after the date of the enactment of the Helping American Victims Afflicted by Neurological Attacks Act of 2021.

(3) RULE OF CONSTRUCTION.—Nothing in this section shall limit, modify, or otherwise supersede chapter 81 of title 5, United States Code, the Defense Base Act (42 U.S.C. 1651 et seq.), or section 19A of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b). Monetary benefits and treatment expenses paid under this section shall not be considered payments under any workers' compensation law.

(i) OTHER INJURIES.—

(1) DEFINITIONS.—In this subsection:

(A) COVERED DEPENDENT.—The term "covered dependent" has the meaning given such term in subsection (e), except that the assigned duty station need not be in the Republic of Cuba, the People's Republic of China, or another foreign country.

(B) COVERED EMPLOYEE.—The term "covered employee" has the meaning given such term in subsection (e), except that the assigned duty station need not be in the Republic of Cuba, the People's Republic of China, or another foreign country.

(C) COVERED INDIVIDUAL.—The term "covered individual" has the meaning given such term in subsection (e), except that the assigned duty station need not be in the Republic of Cuba, the People's Republic of China, or another foreign country.

(D) QUALIFYING INJURY.—The term "qualifying injury" has the meaning given such term in subsection (e), except that the assigned duty station need not be in the Republic of Cuba, the People's Republic of China, or another foreign country.

(2) AUTHORITY.—Notwithstanding any other provision of law but subject to paragraph (3), the Secretary of State or other agency head with an employee may provide payment to a covered dependent, a dependent of a former employee, a covered employee, a former employee, and a covered individual for a qualifying injury to the brain.

(3) LIMITATIONS.—

(A) APPROPRIATIONS REQUIRED.—Payment under paragraph (2) in a fiscal year may only be made using amounts appropriated in advance specifically for payments under such paragraph in such fiscal year.

(B) MATTER OF PAYMENTS.—Payments under paragraph (2) using amounts appropriated for such purpose shall be made on a first come, first serve, or pro rata basis.

(C) AMOUNTS OF PAYMENTS.—The total amount of funding obligated for payments under paragraph (2) may not exceed the amount specifically appropriated for providing payments under such paragraph during its period of availability.

(4) REGULATIONS.—

(A) IN GENERAL.—The Secretary or other agency head described in paragraph (2) that provides payment under such paragraph shall prescribe regulations to carry out this subsection.

(B) ELEMENTS.—The regulations prescribed under subparagraph (A) shall include regulations detailing fair and equitable criteria for payment under paragraph (2).

*(5) NO EFFECT ON OTHER BENEFITS.—Payments made under paragraph (2) are supplemental to any other benefit furnished by the United States Government for which a covered dependent, dependent of a former employee, covered employee, former employee, or covered individual is entitled, and the receipt of such payments may not affect the eligibility of such a person to any other benefit furnished by the United States Government.*

* * * * * * *

---

## DAMON PAUL NELSON AND MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018, 2019, AND 2020

* * * * * * *

# DIVISION E—INTELLIGENCE AUTHORIZATIONS FOR FISCAL YEARS 2018, 2019, AND 2020

* * * * * * *

## SUBDIVISION 1

* * * * * * *

# TITLE LVII—REPORTS AND OTHER MATTERS

## Subtitle A—Reports and Briefings

* * * * * * *

**SEC. 5704. COLLECTION, ANALYSIS, AND DISSEMINATION OF WORKFORCE DATA.**

(a) MODIFICATION OF REQUIREMENT FOR ANNUAL REPORT ON HIRING AND RETENTION OF MINORITY EMPLOYEES.—

(1) EXPANSION OF PERIOD OF REPORT.—Subsection (a) of section 114 of the National Security Act of 1947 (50 U.S.C. 3050) is amended by inserting "and the preceding 5 fiscal years" after "fiscal year".

(2) CLARIFICATION ON DISAGGREGATION OF DATA.—Subsection (b) of such section is amended, in the matter before paragraph (1), by striking "disaggregated data by category of covered person from each element of the intelligence community" and inserting "data, disaggregated by category of covered person and by element of the intelligence community,".

(b) INITIAL REPORTING.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and subject to paragraph (3), the Director of National Intelligence shall make available to the public, the appropriate congressional committees, and the workforce of the intelligence community a report which includes aggregate demographic data and other information regarding the diversity and inclusion efforts of the workforce of the intelligence community.

(2) CONTENTS.—A report made available under paragraph (1)—

(A) shall include unclassified reports and barrier analyses relating to diversity and inclusion efforts;

(B) shall include aggregate demographic data—

(i) by segment of the workforce of the intelligence community and grade or rank;

(ii) relating to attrition and promotion rates;

(iii) that addresses the compliance of the intelligence community with validated inclusion metrics, such as the New Inclusion Quotient index score; and

(iv) that provides demographic comparisons to the relevant nongovernmental labor force and the relevant civilian labor force;

(C) shall include an analysis of applicant flow data, including the percentage and level of positions for which data are collected, and a discussion of any resulting policy changes or recommendations;

(D) shall include demographic data relating to participants in professional development programs of the intelligence community and the rate of placement into senior positions for participants in such programs;

(E) shall include any voluntarily collected demographic data relating to the membership of any external advisory committee or board to which individuals in senior positions in the intelligence community appoint members; and

(F) may include data in proportions or percentages to account for concerns relating to the protection of classified information.

(c) UPDATES.—[After making available a report under subsection (b), the Director of National Intelligence shall annually provide a report] *Not later than March 31 of each year, the Director of National Intelligence shall provide a report* (which may be provided as part of an annual report required under another provision of law) to the workforce of the intelligence community (including senior leadership), the public, and the appropriate congressional committees that includes—

[(1) demographic data and information on the status of diversity and inclusion efforts of the intelligence community;]

*(1) demographic data and information on the status of diversity and inclusion efforts of the intelligence community, including demographic data relating to—*

*(A) the average years of service;*

*(B) the average number of years of service for each level in the General Schedule, Senior Executive Service, Senior Intelligence Service, or equivalent; and*

*(C) career categories;*

(2) an analysis of applicant flow data, including the percentage and level of positions for which data are collected, and a discussion of any resulting policy changes or recommendations; and

(3) demographic data relating to participants in professional development programs of the intelligence community and the rate of placement into senior positions for participants in such programs.

(d) EXPAND THE COLLECTION AND ANALYSIS OF VOLUNTARY APPLICANT FLOW DATA.—

(1) IN GENERAL.—The Director of National Intelligence shall develop a system to collect and analyze applicant flow data for as many positions within the intelligence community as practicable, in order to identify areas for improvement in attracting diverse talent, with particular attention to senior and management positions.

(2) PHASED IMPLEMENTATION.—The collection of applicant flow data may be implemented by the Director of National In-

telligence in a phased approach commensurate with the resources available to the intelligence community.

(e) IDENTIFY ADDITIONAL CATEGORIES FOR VOLUNTARY DATA COLLECTION OF CURRENT EMPLOYEES.—

(1) IN GENERAL.—The Director of National Intelligence may submit to the Office of Management and Budget and to the appropriate congressional committees a recommendation regarding whether the intelligence community should voluntarily collect more detailed data on demographic categories in addition to the race and ethnicity categories specified in the statistical policy directive issued by the Office of Management and Budget entitled "Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity".

(2) PROCESS.—In making a recommendation under paragraph (1), the Director of National Intelligence shall—

(A) engage in close consultation with internal stakeholders, such as employee resource or affinity groups;

(B) ensure that there is clear communication with the workforce of the intelligence community—

(i) to explain the purpose of the potential collection of such data; and

(ii) regarding legal protections relating to any anticipated use of such data; and

(C) ensure adherence to relevant standards and guidance issued by the Federal Government.

(f) DEFINITIONS.—In this section:

(1) APPLICANT FLOW DATA.—The term "applicant flow data" means data that tracks the rate of applications for job positions among demographic categories.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Committee on Foreign Relations, the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Armed Services, the Committee on Homeland Security, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(3) DIVERSITY.—The term "diversity" means diversity of persons based on gender, race, ethnicity, disability status, veteran status, sexual orientation, gender identity, national origin, and other demographic categories.

* * * * * * *

# SUBDIVISION 2

* * * * * * *

# TITLE LXVI—SECURITY CLEARANCES

* * * * * * *

**SEC. 6610. PERIODIC REPORT ON POSITIONS IN THE INTELLIGENCE COMMUNITY THAT CAN BE CONDUCTED WITHOUT ACCESS TO CLASSIFIED INFORMATION, NETWORKS, OR FACILITIES.**

Not later than 180 days after the date of the enactment of [this Act and not less frequently than once every 5 years thereafter,] *this Act, and biennially thereafter,* the Director of National Intelligence shall submit to the congressional intelligence committees a report that reviews the intelligence community for which positions can be conducted without access to classified information, networks, or facilities, or may only require a security clearance at the secret level. *Such report shall take into account the potential effect of maintaining continuity of operations during a covered national emergency (as defined by section 303 of the Intelligence Authorization Act for Fiscal Year 2021 (division W of Public Law 116–260)) and the assessed needs of the intelligence community to maintain such continuity of operations.*

* * * * * * *

## MINORITY VIEWS

The Republican Members of the Committee are increasingly concerned about the Administration's use of the Intelligence Community (IC) for purposes outside of the collection, exploitation, and dissemination of foreign intelligence as defined in the National Security Act. Longstanding bipartisan support for the IC's mission is jeopardized by the blurring of lines between U.S. Government entities responsible for domestic activities, including law enforcement, and those responsible for the collection of intelligence against foreign adversaries.

Congress authorizes and funds the development of powerful tools for use by America's spy agencies. We do so with the understanding, reflected in both law and policy, that the purpose of the IC is to acquire information on foreign threats. This singular focus enhances our confidence that we'll avoid a reoccurrence of the dark days in which the Central Intelligence Agency and National Security Agency were used by the Executive Branch to target Americans based on their political views. This focus is also necessitated by the complexity and magnitude of the threats faced by the United States from our foreign adversaries.

As Members of the Committee, we recognize that limitations on domestic activities can make the mission of the IC more challenging. We also understand that the tools and capabilities of the IC could potentially enhance the domestic missions of the U.S. Government, such as the prosecution of domestic violent extremists. However, unlike our authoritarian adversaries—such as the People's Republic of China—the efficiency of domestic surveillance is not the objective of the U.S. Government. First and foremost, we must ensure the rights of the American people are not infringed.

While we support the vigorous prosecution of all criminal acts carried out by domestic violent extremists, the IC cannot be involved in tracking, investigating, or analyzing such threats other than when law enforcement identifies a potential foreign nexus to those criminal acts. If federal law enforcement agencies lack the resources to prevent and prosecute persistent and lethal domestic threats, the Executive Branch should request those resources from the appropriate Congressional committees of jurisdiction rather than improperly utilizing National Intelligence Program funds for this purpose.

In order for Congress to conduct rigorous oversight and to ensure that the IC's resources are not being improperly used, we must obtain the information we need from the Executive Branch. That is why Section 705 of this Act creates a permanent, annual requirement for every IC element to report to this Committee about every domestic activity it engaged in during the prior fiscal year. Such reports will likely include many mundane and unobjectionable activities, such as conducting security clearance investigations, run-

ning insider threat programs, or other administrative functions. But the annual reports may also shed light on activities that are improper for elements of the IC. This will allow the Committee to make yearly decisions, as part of our annual Intelligence Authorization Act process, about which domestic Intelligence Community activities should be authorized and to identify those that should be prohibited.

Sincerely,

DEVIN NUNES.
MICHAEL TURNER.
BRAD WENSTRUP.
CHRIS STEWART.
RICK CRAWFORD.
ELISE STEFANIK.
MARKWAYNE MULLIN.
TRENT KELLY.
DARIN LAHOOD.
BRIAN FITZPATRICK.

○