AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 5412
OFFERED BY MR. SCHIFF OF CALIFORNIA

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

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

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

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—INTELLIGENCE ACTIVITIES
Sec. 101. Authorization of appropriations.
Sec. 102. Classified schedule of authorizations.
Sec. 103. Intelligence community management account.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND
DISABILITY SYSTEM
Sec. 201. Authorization of appropriations.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS
Sec. 301. Restriction on conduct of intelligence activities.
Sec. 302. Increase in employee compensation and benefits authorized by law.
Sec. 303. Temporary authority for paid leave for a serious health condition.
Sec. 304. Harmonization of whistleblower protections.
Sec. 305. Congressional oversight of certain special access programs.
Sec. 306. Clarification of requirement for authorization of funding for intelligence activities.
Sec. 307. Authorization of support by Director of National Intelligence for certain activities relating to intelligence community workforce.
Sec. 308. 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.

Sec. 310. Authority for transport of certain canines associated with force protection duties of intelligence community.

Sec. 311. Development of definitions for certain terms relating to intelligence.

Sec. 312. Support for and oversight of Unidentified Aerial Phenomena Task Force.

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.

Sec. 402. Clarification of certain responsibility of the Director of National Intelligence.

Sec. 403. Responsibility of Director of National Intelligence regarding National Intelligence Program budget concerning Federal Bureau of Investigation.

Sec. 404. Climate Security Advisory Council.

Subtitle B—Other Elements

Sec. 411. Protection of certain facilities and assets of Central Intelligence Agency from unmanned aircraft.

Sec. 412. Modification of National Geospatial-Intelligence Agency personnel management authority to attract experts in science and engineering.

Sec. 413. Requirements for termination of dual-hat arrangement for Commander of the United States Cyber Command.

Sec. 414. National Space Intelligence Center.

Sec. 415. Procurement by Federal Bureau of Investigation of Chinese products and services.

Sec. 416. Counterintelligence units at non-intelligence community Federal departments and agencies.

Sec. 417. Detection and monitoring of wildfires.

TITLE V—ANOMALOUS HEALTH INCIDENTS AND OTHER HEALTH CARE MATTERS

Sec. 501. Compensation and professional standards for certain medical officers of the Central Intelligence Agency.

Sec. 502. Medical advisory board of the Central Intelligence Agency.

Sec. 503. Report on protocols for certain intelligence community employees and dependents.

Sec. 504. Inspector General of the Central Intelligence Agency review of Office of Medical Services.

Sec. 505. Clarification of effect of certain benefits relating to injuries to the brain.

TITLE VI—MATTERS RELATING TO FOREIGN COUNTRIES

Sec. 601. National Intelligence Estimate on security situation in Afghanistan and related region.

Sec. 602. Report on likelihood of military action by countries of the South Caucasus.
Sec. 603. Report on intelligence collection posture and other matters relating to Afghanistan and related region.

Sec. 604. Report on threat posed by emerging Chinese technology companies.

Sec. 605. Report on cooperation between China and United Arab Emirates.


Sec. 607. Report on effects of sanctions by United States.

TITLE VII—REPORTS AND OTHER MATTERS

Sec. 701. Pilot program for security vetting of certain individuals.

Sec. 702. Intelligence assessment and reports on foreign racially motivated violent extremists.

Sec. 703. Periodic report on positions in the intelligence community that can be conducted without access to classified information, networks, or facilities.

Sec. 704. Biennial reports on foreign biological threats.

Sec. 705. Annual reports on domestic activities of the intelligence community.

Sec. 706. Annual reports on certain cyber vulnerabilities procured by intelligence community and foreign commercial providers of cyber vulnerabilities.

Sec. 707. Improvements to annual report on demographic data of employees of intelligence community.

Sec. 708. National Intelligence Estimate on escalation and de-escalation of gray zone activities in great power competition.

Sec. 709. Report on certain actions taken by intelligence community with respect to human rights and international humanitarian law.

Sec. 710. Briefing on trainings relating to blockchain technology.

Sec. 711. Report on prospective ability to administer COVID–19 vaccines and other medical interventions to certain intelligence community personnel.


Sec. 713. Reports relating to Inspector General of Defense Intelligence Agency.

Sec. 714. Report on rare earth elements.


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.


(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.

(13) The Drug Enforcement Administration.

(14) The National Reconnaissance Office.

(15) The National Geospatial-Intelligence Agency.


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 ap-
propriate 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 re-
ferred to in section 102(a).

TITLE II—CENTRAL INTEL-
LIGENCE AGENCY RETIRE-
MENT AND DISABILITY SYS-
TEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Cen-
tral Intelligence Agency Retirement and Disability Fund
$514,000,000 for fiscal year 2022.

TITLE III—GENERAL INTEL-
LIGENCE COMMUNITY MAT-
TERS

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 notwith-
standing 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 condi-
tion.

“(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 ac-
commodate an employee’s leave schedule request under
subsection (b), including a request to use such leave inter-
mittently or on a reduced leave schedule, to the extent that
the requested leave schedule does not unduly disrupt agen-
cy 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 intel-
ligence 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 direc-
tive 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. Paid serious health condition leave.”.
(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 insert “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”.

(c) 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 su-
pervisor 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 subpara-
graph (B) 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 (e)(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 (B) 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 (e) the following:

“(d) RULE OF CONSTRUCTION.—Consistent with the protection of sources and methods, nothing in subsection (b) or (e) 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 SUB-COMPARTMENTS.—

“(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 commu-
nity 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 sub-compartments of covered special access programs active as of the date of the report.

“(B) A list of all compartments and sub-compartments 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 ac-
cess programs, and the compartments and
subcompartments within each, are substan-
tiated and justified based on the informa-
tion required by clause (ii); and

“(ii) for each certification—

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

“(II) the identification of a con-
trol officer for each covered special ac-
cess program; and

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

“(e) COVERED SPECIAL ACCESS PROGRAM DE-
FINED.—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).


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 ac-
cepting 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 em-
ployee of such element occupying a covered intel-
ligence position to sign a written agreement requir-
ing the regular reporting of covered post-service em-
ployment to the head of such element pursuant to
paragraph (1).

“(c) PENALTIES.—

“(1) CRIMINAL PENALTIES.—A former em-
ployee who knowingly and willfully violates sub-
section (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 impris-
oned for not more than 5 years, or both. Each re-
port 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 sub-
section (b) to employees of that element who occupy
a covered intelligence position.

“(2) Written Notice.—The head of each ele-
ment 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 com-
mittees a report on covered post-service employment
occurring during the year covered by the report.

“(2) Elements.—Each report under para-
graph (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 ac-
tivities 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 mak-
ing 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 spe-
cific foreign individual, agency, or entity, for whom
the covered post-service employment is being per-
formed.

“(4) As applicable, a description of—

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

“(B) the activities that may violate Fed-
eral 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 occu-
pying such position to information regarding sen-
sitive intelligence sources or methods or other excep-
tionally 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 na-
tional 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, con-
trolled, 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 intel-
ligence 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 ap-
propriations 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 intel-
ligence community shall be treated as being listed in sub-
section (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 con-
sultation 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.

(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 “con- 
gressional intelligence committees” and “intelligence com- 
munity” have the meanings given such terms in section 

SEC. 312. SUPPORT FOR AND OVERSIGHT OF UNIDENTI- 
IFIED AERIAL PHENOMENA TASK FORCE.

(a) AVAILABILITY OF DATA ON UNIDENTIFIED AER- 
IAL PHENOMENA.—The Director of National Intelligence 
shall ensure that each element of the intelligence commu- 
nity 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 Unidenti- 
fied Aerial Phenomena Task Force, or successor en- 
tity, shall submit to the appropriate congressional 
committees a report on the findings of the Unidenti- 
fied Aerial Phenomena Task Force, or successor en- 
tity.

(2) CONTENTS.—Each report submitted under 
paragraph (1) shall include, at a minimum, the fol- 
lowing:
(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 BIO-SECURITY 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 pre-vent” 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 paragraph:
“(2) 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).
(c) 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 RESPONSIBILITY OF THE 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”.

September 30, 2021 (1:00 p.m.)
SEC. 413. REQUIREMENTS FOR TERMINATION OF DUAL-HAT ARRANGEMENT FOR COMMANDER OF THE UNITED STATES CYBER COMMAND.


(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 (e) 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 rel-
levant 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 Con-
gress 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 Bu-
reau conducts a security assessment under subsection (a),
the Director shall submit to the congressional intelligence
committees a copy of such assessment and the rec-
ommendation 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 govern-
ment 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 sub-
section (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 THE 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 THE 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, 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 Director 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 top-
ies 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 (e), 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 (e).

(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 (e) 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 re-
quired 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 THE 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.
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 re-
spect 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 classi-
fied 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 POS-
TURE 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 In-
telligence, in consultation with the heads of elements of
the intelligence community determined relevant by the Di-
rector, shall submit to the congressional intelligence com-
mittees a report on the collection posture of the intel-
ligence community and other matters relating to Afghan-
istan 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 de-
scribed in paragraph (1)(A), including by filling any
gaps identified pursuant to such paragraph.

(3) An assessment of the effect of publicly doc-
umenting abuses engaged in by the Taliban, and a
description of the efforts of the intelligence commu-
nity to support other departments and agencies in
the Federal Government with respect to the collec-
tion and documentation of such abuses.

(4) An assessment of the relationship between
the intelligence community and countries in the cov-
ered region, including an assessment of the fol-
lowing:

(A) Intelligence and information sharing

with such countries.

(B) Any change in the collection posture of
the intelligence community with respect to the
uclear 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 intel-
ligence community with respect to the presence
of such countries in Afghanistan (including fi-
nancial 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 commu-
nity to use the airspace of any such countries.

(5) An assessment of any financial contribu-
tions to the Taliban from foreign countries (particu-
larly from China, Iran, Russia, and any other for-
eign 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 unclassi-
fied summary.

(d) BIANNUAL UPDATES.—On a biannual basis dur-
ing the 5-year period following the date of the submission
of the report under subsection (a), the Director of Na-
tional Intelligence, in consultation with the heads of the
elements of the intelligence community determined rel-
evant 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 sub-
section (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 re-
spect 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 re-
spect 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 in-
clude 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 classi-

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 In-
telligence, 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 sub-
section (a) shall include the following:

(1) An assessment of whether sanctions im-
posed 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 Bu-
reau 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 associ-
ated with foreign racially motivated violent extremist organizations.

(2) ELEMENTS.—The report under paragraph 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 Lib-
entities 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.

(e) 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 Secu-
rity, 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 Gov-
ernmental Affairs, the Committee on Foreign
Relations, and the Committee on the Judiciary
of the Senate.

(2) TERRORISM INFORMATION.—The term “ter-
rorism 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

SEC. 703. PERIODIC REPORT ON POSITIONS IN THE INTEL-
LIGENCE COMMUNITY THAT CAN BE CON-
DUCTED WITHOUT ACCESS TO CLASSIFIED
INFORMATION, NETWORKS, OR FACILITIES.

Section 6610 of the Damon Paul Nelson and Mat-
thew 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
116 of the National Security Act of 1947, as added by subsection (a).

SEC. 705. ANNUAL REPORTS ON DOMESTIC ACTIVITIES OF THE 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 in-
formation 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 sub-
section (a).

SEC. 706. ANNUAL REPORTS ON CERTAIN CYBER
VULNERABILITIES PROCURED BY INTEL-
LIGENCE COMMUNITY AND FOREIGN COM-
MERCIAl PROVIDERS OF CYBER

VULNERABILITIES.

(a) REQUIREMENT.—Title XI of the National Secu-

rity 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 INTEL-
LIGENCE COMMUNITY AND FOREIGN COM-
MERCIAl 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 com-
mittees a report containing information on foreign com-
mercial 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 ac-
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, par-
ticularly in the context of Ukrainian gas pipe-
lines, to coerce its neighbors into compliance
with its policies.

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

(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 attempts by Russia to poison Sergei Skripal in London.

(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 oper-
ations, 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 deni-
able adversary operations.

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

(G) The extent to which gray zone activi-
ties 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 opportu-
nities for strengthening those norms.

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

(J) Opportunities to strengthen the resil-
ience 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
corresponding definitions for such terms) for

concepts associated with gray zone activities.

(2) CONSIDERATIONS.—In developing the lexi-

con 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 al-

ternative definition)—


(A) more accurately describes a concept as-

associated with gray zone activities; or


(B) is preferable for any other reason.

(3) REPORT.—

(A) PUBLICATION.—The Director of Na-

tional Intelligence shall publish a report con-

taining the lexicon developed under paragraph

(1).

(B) FORM.—The report under subpara-

graph (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”.


(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 (e).

(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; and
(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 Secu-
rity 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.

(e) 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 re-
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.—


(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 ac-
cess 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 min-
ing, 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 commu-
nity with respect to rare earth elements;

(B) any relevant planning or efforts by the
intelligence community to assure secured access
to rare earth magnets;
(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 de-
partments and agencies of the United States
Government that are not elements of the intel-
ligence 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 sec-
tion 6306 of the Damon Paul Nelson and Mat-
thew Young Pollard Intelligence Authorization
Act for Fiscal Years 2018, 2019, and 2020 (50
U.S.C. 3370) with respect to rare earth ele-
ments.

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

(d) RARE EARTH ELEMENTS DEFINED.—In this sec-
tion, 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 collec-
tion 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.

(e) 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).