AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 8367
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 2023”.

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. Joint Intelligence Community Council.
Sec. 304. Required policy for minimum insider threat standards.
Sec. 305. Timely submission of classified intelligence budget justification materials.
Sec. 306. Unfunded priorities of the intelligence community.
Sec. 307. Submission of classified annexes to executive orders and other documents.
Sec. 308. Improvements to program on recruitment and training.
Sec. 309. Measures to mitigate counterintelligence threats from proliferation and use of foreign commercial spyware.
Sec. 310. Expansion of treatment of moving expenses.
Sec. 311. Personnel vetting performance measures.
Sec. 312. Proactive cybersecurity.
Sec. 313. Limitation on availability of funds for Intelligence Community Management Account pending submission of report on domestic activities of intelligence community.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

Sec. 401. Modifications to responsibilities and authorities of Director of National Intelligence.
Sec. 402. Annual submission to Congress of National Intelligence Priorities Framework.
Sec. 403. Disposition of records of Office of the Director of National Intelligence.

Subtitle B—Central Intelligence Agency

Sec. 411. Authority of Central Intelligence Agency to provide protection for certain personnel.
Sec. 412. Notification of use of certain expenditure authorities.
Sec. 413. Clarification of authorities relating to security personnel at Office of Director of National Intelligence facilities and installations.
Sec. 414. Office of Workforce Support of Central Intelligence Agency.
Sec. 415. Establishment of External Advisory Board for Talent for the Central Intelligence Agency.
Sec. 416. Study on relationship between Central Intelligence Agency and Congress.
Sec. 417. Historical Advisory Panel of Central Intelligence Agency.

Subtitle C—Elements of the Defense Intelligence Enterprise

Sec. 421. Deputy Director for Defense Intelligence responsible for warfighter support.
Sec. 422. Cover enhancement authorities.
Sec. 423. Authority of Army counterintelligence agents to execute warrants and make arrests.
Sec. 424. Inclusion of Space Force as element of intelligence community.
Sec. 425. Military intelligence collection and analysis partnerships.
Sec. 426. Intelligence assessment of effects of counterterrorism strikes.
Sec. 427. Submission of certain legislative proposals.
Sec. 428. Oversight of Defense Intelligence Agency culture.
Sec. 429. Cyber intelligence surveillance reconnaissance information.
Sec. 430. Information on cover activities of Department of Defense.

Subtitle D—Other Elements

Sec. 441. Authorization relating to certain intelligence and counterintelligence activities of Coast Guard.
Sec. 442. Study on personnel under Strategic Intelligence Partnership Program.
Sec. 443. Assessment of handling of certain information relating to deliberations of Bureau of Industry and Security.

TITLE V—MATTERS RELATING TO EMERGING TECHNOLOGIES
Subtitle A—General Matters

Sec. 501. Definitions.
Sec. 502. Officials responsible for artificial intelligence policies of the intelligence community.

Subtitle B—Improvements Relating to Procurement

Sec. 511. Additional transaction authority.
Sec. 512. Offices of Commercial Integration.
Sec. 513. Pilot program for designation of certain SBIR and STTR projects as Entrepreneurial Innovation Projects.
Sec. 514. Reduction of barriers relating to contracts for artificial intelligence and other emerging technologies.
Sec. 515. Compliance by the intelligence community with requirements of the Federal Acquisition Regulation relating to commercially available off-the-shelf items and commercial services.
Sec. 516. Policy on required user adoption metrics in certain contracts for artificial intelligence software products.
Sec. 517. Assessments relating to information technology and software systems.

Subtitle C—Reports

Sec. 521. Reports on integration of artificial intelligence within intelligence community.
Sec. 522. Report on potential benefits of establishment of ICWERX.
Sec. 523. Requirements and report on workforce needs of intelligence community relating to science, technology, engineering, and math, and related areas.

Subtitle D—Other Matters

Sec. 531. Improvements to use of commercial software products.
Sec. 532. Improvements to employees and managers relating to emerging technologies, software development, acquisition, and sustainment.

TITLE VI—MATTERS RELATING TO FOREIGN COUNTRIES

Subtitle A—Miscellaneous Authorities, Requirements, and Limitations

Sec. 601. Notice of deployment or transfer of containerized missile systems by Russia, China, or Iran.
Sec. 602. Intelligence community coordinator for Russian atrocities accountability.
Sec. 603. Lead intelligence community coordinator for countering and neutralizing proliferation of Iran-origin unmanned aircraft systems.
Sec. 604. Collaboration between intelligence community and Department of Commerce to counter foreign commercial threats.
Sec. 605. Intelligence assessment on foreign weaponization of advertisement technology data.
Sec. 606. Intelligence community assessment regarding Russian gray zone assets.
Sec. 607. Intelligence assessment on effects of sanctions on Russia.

Subtitle B—Reports and Other Matters

Sec. 611. Report on assessing will to fight.
Sec. 612. Report on impact of Russia invasion of Ukraine on global food security.
Sec. 613. Report on threat from hypersonic weapons.
Sec. 615. Report on activities of China and Russia targeting Latin America and the Caribbean.
Sec. 616. Report on support provided by China to Russia.
Sec. 617. Report on global CCP investment in port infrastructure.
Sec. 618. Sense of Congress on provision of support by intelligence community for atrocity prevention and accountability.

TITLE VII—REPORTS AND OTHER MATTERS

Sec. 701. Repeal of certain report requirements.
Sec. 702. Increased intelligence-related engineering, research, and development capabilities of minority institutions.
Sec. 703. Annual report on response to Government Accountability Office recommendations to intelligence community.
Sec. 704. Annual report on efforts of the Federal Bureau of Investigation to identify and promote diverse candidates.
Sec. 705. Reports on personnel vetting processes and progress under Trusted Workforce 2.0 initiative.
Sec. 706. Reports relating to programs of record of National Geospatial-Intelligence Agency.
Sec. 707. Plan regarding Social Media Data and Threat Analysis Center.
Sec. 708. Report on use of publicly available social media information in personnel vetting determinations.
Sec. 709. Report on strengthening workforce diversity planning and oversight.
Sec. 710. Report on improving opportunities for women and minorities for promotions in the intelligence community.
Sec. 711. Report on transition of National Reconnaissance Office to digital engineering environment.
Sec. 713. Report on declassification efforts of Central Intelligence Agency.
Sec. 714. Report on National Space Intelligence Center.
Sec. 715. Report on implementation of Executive Order 13556, regarding controlled unclassified information.
Sec. 716. Comptroller General of the United States compilation of unidentified aerospace-undersea phenomena records.
Sec. 717. National Museum of Intelligence and Special Operations.
Sec. 718. Technical corrections.

1 SEC. 2. DEFINITIONS.

2 In this Act:

3 (1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term “congressional intelligence committees” has the meaning given such term in section

(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 2023 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.
(17) The Space Force.

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) Specifications of Amounts.—The amounts authorized to be appropriated under section 101 for the conduct of the intelligence activities of the elements listed in paragraphs (1) through (16) of section 101, are those specified in the classified Schedule of Authorizations prepared to accompany this Act.

(b) Availability of Classified Schedule of Authorizations.—

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

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

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

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

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

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2023 the sum of $665,800,000.

(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 Ac-
TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund $514,000,000 for fiscal year 2023.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

SEC. 301. RESTRICTION ON CONDUCT OF INTELLIGENCE ACTIVITIES.

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

SEC. 302. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY LAW.

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

SEC. 303. JOINT INTELLIGENCE COMMUNITY COUNCIL.

(a) MEMBERSHIP.—Subsection (b) of section 101A
of the National Security Act of 1947 (50 U.S.C. 3022)
is amended—

(1) by redesignating paragraph (8) as para-
graph (9); and

(2) by inserting after paragraph (7) the fol-
lowing new paragraph:

“(8) The Director of the Central Intelligence
Agency.”.

(b) FUNCTIONS.—Subsection (c) of such section is
amended—

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

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

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

“(3) ensuring that the intelligence community
has efficient and effective mechanisms to receive and
prioritize the intelligence needs of the departments
and agencies of the United States Government that
are not part of the intelligence community or the
Department of Defense.”.

(c) MEETINGS.—Subsection (d) of such section is
amended by striking “as the Director considers appro-
priate” and inserting “on an annual basis, or more fre-
fquently as the Director determines appropriate”.

SEC. 304. REQUIRED POLICY FOR MINIMUM INSIDER
THREAT STANDARDS.

(a) REQUIREMENT.—Section 102A(f) of the National
Security Act of 1947 (50 U.S.C. 3024(f)) is amended—
(1) by redesignating paragraphs (8) and (9) as
paragraphs (9) and (10), respectively; and
(2) by inserting after paragraph (7) the fol-
lowing new paragraph:
“(8)(A) The Director of National Intelligence shall
ensure there is established a policy for minimum insider
threat standards that is consistent with the Presidential
memorandum of November 21, 2012, titled ‘National In-
sider Threat Policy and Minimum Standards for Executive
Branch Insider Threat Programs’, or any successor there-
to.
“(B) The head of each element of the intelligence
community shall implement the policy under subparagraph
(A) within that element, and, concurrent with the submis-
son to Congress of budget justification materials in sup-
port of the budget of the President for a fiscal year that
is submitted to Congress under section 1105(a) of title
31, United States Code, shall submit to Congress a certifi-
cation as to whether the element is in compliance with
such policy.

“(C) The Director shall conduct periodic audits to de-
termine whether each element of the intelligence commu-
nity is in compliance with the policy under subparagraph
(A). The Director may refer any audit under this subpara-
graph to the Inspector General of the Intelligence Commu-
nity, who shall conduct such audit on behalf of the Direc-
tor.”.

(b) CONFORMING AMENDMENT.—Section 102A(x)(3)
of such Act (50 U.S.C. 3024(x)(3)) is amended by insert-
ing “, including the policy under subsection (f)(8),” after
“policies of the intelligence community”.

SEC. 305. TIMELY SUBMISSION OF CLASSIFIED INTEL-
LIGENCE BUDGET JUSTIFICATION MATE-
RIALS.

Title V of the National Security Act of 1947 (50
U.S.C. 3091 et seq.) is amended by inserting after section
506I the following new section (and conforming the table
of contents at the beginning of such Act accordingly):
"SEC. 506J. CLASSIFIED INTELLIGENCE BUDGET JUSTIFICATION MATERIALS.

"(a) TIMELY SUBMISSION.—At the same time as the President submits to Congress the budget for each fiscal year, the Director of National Intelligence shall submit to the congressional intelligence committees the classified intelligence budget justification materials for the element for that budget.

"(b) DEFINITIONS.—In this section:

“(1) The term ‘budget’ has the meaning given the term ‘budget of the President’ in section 506A.

“(2) The term ‘classified intelligence budget justification materials’ means, with respect to a fiscal year, the materials submitted to Congress by the Director of National Intelligence in support of the budget for that fiscal year that are classified or otherwise protected from public disclosure.”.

SEC. 306. UNFUNDED PRIORITIES OF THE INTELLIGENCE COMMUNITY.

Title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.), as amended by section 305, 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. 514. UNFUNDED PRIORITIES OF THE INTELLIGENCE COMMUNITY: ANNUAL REPORT.

“(a) ANNUAL REPORT.—Not later than 10 days after the date on which the budget of the President for a fiscal year is submitted to Congress pursuant to section 1105 of title 31, United States Code, the head of each element of the intelligence community shall submit to the Director of National Intelligence and to the congressional intelligence committees a report on the unfunded priorities of the programs under the jurisdiction of such head.

“(b) ELEMENTS.—

“(1) IN GENERAL.—Each report under subsection (a) shall specify, for each unfunded priority covered by such report, the following:

“(A) A summary description of such priority, including the objectives to be achieved if such priority is funded (whether in whole or in part).

“(B) Whether such priority will satisfy a covert action or support collection against requirements identified in the National Intelligence Priorities Framework of the Office of the Director of National Intelligence (or any successor mechanism established for the prioritization of programs and activities), in-
cluding a description of such requirements and the related prioritization level.

“(C) The additional amount of funds recom-
ommended in connection with the objectives under subparagraph (A).

“(D) Budget information with respect to the unfunded priority, including—

“(i) the appropriation account;
“(ii) the expenditure center; and
“(iii) the project and, if applicable, subproject.

“(2) PRIORITIZATION OF PRIORITIES.—Each report shall present the unfunded priorities covered by such report in overall order of urgency of priority among unfunded priorities.

“(c) UNFUNDED PRIORITY DEFINED.—In this sec-
tion, the term ‘unfunded priority’, in the case of a fiscal year, means a program, activity, or mission requirement of an element of the intelligence community that—

“(1) is not funded in the budget of the Presi-
dent for the fiscal year as submitted to Congress pursuant to section 1105 of title 31, United States Code;

“(2) is necessary to fulfill a covert action or to satisfy an information requirement associated with
the collection, analysis, or dissemination of intelligence that has been documented within the National Intelligence Priorities Framework; and

“(3) would have been recommended for funding by the head of the element of the intelligence community if—

“(A) additional resources had been available for the budget to fund the program, activity, or mission requirement; or

“(B) the program, activity, or mission requirement has emerged since the budget was formulated.”.

SEC. 307. SUBMISSION OF CLASSIFIED ANNEXES TO EXECUTIVE ORDERS AND OTHER DOCUMENTS.

(a) REQUIREMENT.—Title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.), as amended by section 306, 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. 515. SUBMISSION OF CLASSIFIED ANNEXES TO EXECUTIVE ORDERS AND OTHER DOCUMENTS.

“(a) REQUIREMENT.—Not later than 7 days after the date on which the President issues or amends a covered document, the Director of National Intelligence shall submit to the congressional intelligence committees any classi-
fied annex accompanying that document if such annex contains a reference to any element of the intelligence community.

“(b) COVERED DOCUMENT DEFINED.—In this section, the term ‘covered document’ means any executive order, memorandum, or policy directive issued by the President, including national security Presidential memoranda and Presidential policy directives, or such successor memoranda and directives.”.

(b) INITIAL SUBMISSION.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees each classified annex required under section 515 of the National Security Act, as added by subsection (a), in effect as of the date of enactment of this Act.

SEC. 308. IMPROVEMENTS TO PROGRAM ON RECRUITMENT AND TRAINING.

Section 1022 of the National Security Act of 1947 (50 U.S.C. 3222) is amended to read as follows:

“SEC. 1022. PROGRAM ON RECRUITMENT AND TRAINING.

“(a) PROGRAM.—

“(1) REQUIREMENT.—The Director of National Intelligence, in consultation with the heads of the elements of the intelligence community, shall carry
out a program to ensure that selected individuals are provided funds for academic training (including with respect to both undergraduate and postgraduate education), or to reimburse for academic training previously obtained—

“(A) in capabilities, missions, or skillsets, especially in the fields of science, technology, math, and engineering, to address workforce requirements in which the intelligence community is deficient or likely to be deficient in the future; or

“(B) for such individuals who have backgrounds or experiences that the Director has identified as being underrepresented in the intelligence community or likely to be underrepresented in the future.

“(2) COMMITMENT.—An individual selected for participation in the program shall commit to employment with an element of the intelligence community for a period that the Director determines is commensurate with the amount of funding provided to the individual under the program and under such terms and conditions as the Director considers appropriate.
“(3) DESIGNATION.—The program shall be known as the Pat Roberts Intelligence Scholars Program.

“(4) OUTREACH.—The Director, in consultation with the heads of the elements of the intelligence community, shall maintain a publicly available internet website on the program that describes—

“(A) the intent of the program;

“(B) the conditions and requirements for selection and participation;

“(C) application instructions;

“(D) the areas covered by the program pursuant to the review conducted under subsection (b)(2); and

“(E) any other details the Director determines appropriate.

“(b) ELEMENTS.—In carrying out the program under subsection (a), the Director shall—

“(1) establish such requirements relating to the academic training of participants as the Director considers appropriate to ensure that participants are prepared for employment as intelligence professionals; and

“(2) on an annual basis, review the areas that will contribute to the capabilities, missions, and
skillsets in which the intelligence community is deficient or is likely to be deficient in the future.

“(c) USE OF FUNDS.—Funds made available for the program under subsection (a) shall be used—

“(1) to provide a monthly stipend for each month that a participant is pursuing a course of study;

“(2) to pay the partial or full tuition or other appropriate education expenses of a participant for the completion of such course of study;

“(3) to reimburse a participant for tuition or other appropriate education expenses paid by the participant before becoming an employee of an element of the intelligence community, including with respect to providing payments for student loans used for such tuition and expenses;

“(4) to pay for books and materials that the participant requires or required to complete such course of study;

“(5) to pay the expenses of the participant for travel requested by an element of the intelligence community in relation to such program; or

“(6) for such other purposes the Director considers reasonably appropriate to carry out such program.”.
SEC. 309. MEASURES TO MITIGATE COUNTERINTELLIGENCE THREATS FROM PROLIFERATION AND USE OF FOREIGN COMMERCIAL SPYWARE.

(a) FINDINGS.—Congress finds the following:

(1) The proliferation of foreign commercial spyware poses an acute and emergent threat to the national security of the United States.

(2) Foreign entities have developed and supplied foreign commercial spyware to other foreign governments that used these tools to maliciously target officials of the United States Government. Many of those foreign governments have, in service of their repressive activities, targeted journalists, businesspeople, activists, academics, and other persons.

(3) Furthermore, public reports suggest that foreign companies involved in the proliferation of foreign commercial spyware maintain close ties to foreign governments and their intelligence services. This close relationship between foreign governments and the companies selling foreign commercial spyware furthers the already substantial counterintelligence concerns for any end-user of these products, including potential end-users in the United States.
(4) To mitigate the grave counterintelligence threat posed by the rapid spread of these tools—as well as to improve the digital security of citizens of the United States, combat cyber threats, and mitigate unlawful surveillance—the United States on January 19, 2022, finalized a rule establishing controls on the export, reexport, or in-country transfer of certain items that can be used for malicious cyber activities.

(5) In furtherance of the same national security objectives, the Commerce Department on November 4, 2021, released a rule adding four foreign companies to the Entity List for engaging in activities that are contrary to the national security or foreign policy interests of the United States. This rule had the practical effect of preventing the listed companies from receiving American technologies.

(6) Subsequent public reports indicate that at least one of the four companies added to the Entity List attempted to evade these and other restrictions, and a private consultancy which oversees that company informed the European Parliament in 2022 that it could not confirm the blacklisted company is complying with all relevant laws and regulatory frameworks.
(b) SENSE OF CONGRESS.—It is the sense of Congress that the intelligence community, with its unique authorities, foreign intelligence mission, analytical capabilities, and other capabilities, is best positioned to lead the efforts of the United States Government to mitigate the counterintelligence threats posed by the rapidly expanding ecosystem of foreign commercial spyware, including by devising and implementing strategies to protect personnel of the United States Government from being maliciously targeted.

(c) STATEMENT OF POLICY.—It shall be the policy of the United States to decisively act against counterintelligence threats posed by foreign commercial spyware, as well as the individuals who lead entities selling foreign commercial spyware and who are reasonably believed to be involved, have been involved, or pose a significant risk to being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States.

(d) MEASURES TO MITIGATE COUNTERINTELLIGENCE THREATS.—Title XI of the National Security Act of 1947 (50 U.S.C. 3231 et seq.) is amended by inserting after section 1102 the following new section (and conforming the table of contents at the beginning of such Act accordingly):
"SEC. 1102A. MEASURES TO MITIGATE COUNTERINTELLIGENCE THREATS FROM PROLIFERATION AND USE OF FOREIGN COMMERCIAL SPYWARE.

“(a) ANNUAL ASSESSMENTS OF COUNTERINTELLIGENCE THREATS.—

“(1) REQUIREMENT.—Not later than March 1, 2023, and annually thereafter, the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the National Security Agency, and the Director of the Federal Bureau of Investigation, shall submit to the congressional intelligence committees a report containing an assessment of the counterintelligence threats and other risks to the national security of the United States posed by the proliferation of foreign commercial spyware. The assessment shall incorporate all credible data, including open-source information.

“(2) ELEMENTS.—Each report under paragraph (1) shall include the following, if known:

“(A) A list of the most significant foreign companies, as determined by the Director of National Intelligence, selling, leasing, or otherwise providing foreign commercial spyware, and associated foreign commercial entities, assessed
by the intelligence community to be the most
significant foreign actors in the global prolifera-
tion of foreign commercial spyware.

“(B) A description of the foreign commercial
spyware marketed by the foreign companies
identified under subparagraph (A) and an assess-
ment by the intelligence community of the
foreign commercial spyware.

“(C) An assessment of the counterintelli-
gen risk to personnel of the intelligence com-
unity posed by such spyware.

“(D) Details of where each foreign com-
pany identified under subparagraph (A) is dom-
iciled, as well as any foreign country in which
the company has subsidiaries or resellers acting
as the local agent on behalf of the foreign par-
et company.

“(E) A description of how each such for-
ign company is financed, where the foreign
company acquired its capital, and the major in-
vestors in the foreign company.

“(F) An assessment by the intelligence
community of any relationship between each
such foreign company and a foreign govern-
ment, including any export controls and processes to which the foreign company is subject.

“(G) To the extent such information is obtainable through clandestine collection or open source intelligence, a list of the foreign customers of each such foreign company, including the understanding by the intelligence community of the organizations and end-users within any foreign government that procured the spyware of that foreign company.

“(H) With respect to each foreign customer identified under subparagraph (G), an assessment by the intelligence community regarding how the foreign customer is using the spyware, including whether the spyware has been used to target personnel of the intelligence community.

“(I) With respect to the first report, a mitigation plan to reduce the exposure of personnel of the intelligence community to foreign commercial spyware.

“(J) With respect to each report following the first report, details of steps taken by the intelligence community since the previous report to implement measures to reduce the exposure
of personnel of the intelligence community to foreign commercial spyware.

“(3) FORM.—Each report under paragraph (1) shall be submitted in classified form.

“(4) DISSEMINATION.—The Director of National Intelligence shall share each report under paragraph (1) with the heads of other appropriate Federal departments and agencies, including the President, the heads of all elements of the intelligence community, the Secretary of State, the Attorney General, the Director of the Federal Bureau of Investigation, the Secretary of Commerce, and the heads of any other agencies the Director determines appropriate.

“(b) CLASSIFIED WATCHLIST.—

“(1) SUBMITTAL TO CONGRESS.—The Director of National Intelligence shall submit to the appropriate congressional committees a list of companies selling, leasing, or otherwise providing foreign commercial spyware that the Director determines are engaged in activities that pose a counterintelligence risk to personnel of the intelligence community.

“(2) UPDATES.—The Director shall update the list under paragraph (1) not less frequently than annually.
“(3) FORM.—Each list under paragraph (1) shall be submitted in classified form.

“(4) DISSEMINATION.—The Director of National Intelligence shall share each list under paragraph (1) with the heads of other appropriate Federal departments and agencies, including the President, the heads of all elements of the intelligence community, the Secretary of State, the Attorney General, the Director of the Federal Bureau of Investigation, the Secretary of Commerce, and the heads of any other agencies the Director determines appropriate.

“(e) AUTHORITY TO PROHIBIT PURCHASE OR USE BY INTELLIGENCE COMMUNITY.—

“(1) FOREIGN COMMERCIAL SPYWARE FROM FOREIGN SPYWARE COMPANY.—

“(A) IN GENERAL.—The Director of National Intelligence may prohibit any element of the intelligence community from procuring, leasing, or otherwise acquiring on the commercial market, or extending or renewing a contract to procure, lease, or otherwise acquire, foreign commercial spyware from a foreign spyware company.
“(B) CONSIDERATIONS.—In determining whether and how to exercise the authority under subparagraph (A), the Director of National Intelligence shall consider—

“(i) the assessment of the intelligence community of the counterintelligence threats or other risks to the United States posed by the foreign commercial spyware; and

“(ii) the assessment of the intelligence community of whether the foreign commercial spyware has been used to target United States Government personnel.

“(2) DOMESTIC COMPANY PROVIDING FOREIGN COMMERCIAL SPYWARE.—

“(A) AUTHORITY TO PROHIBIT PURCHASE.—The Director of National Intelligence may prohibit the purchase or use by the intelligence community of spyware from a domestic company if the Director determines that the spyware was originally sourced, in whole or in part, from a foreign company.

“(B) CONSIDERATIONS.—In considering whether and how to exercise the authority under subparagraph (A) with respect to
spyware, the Director of National Intelligence shall consider—

“(i) whether the original owner or developer retains any of the physical property or intellectual property associated with the spyware;

“(ii) whether the original owner or developer has verifiably destroyed all copies of the data collected by or associated with the spyware;

“(iii) whether the personnel of the original owner or developer retain any access to data collected by or associated with the spyware;

“(iv) whether the use of the spyware requires the user to connect to an information system of the original owner or developer or of a foreign government; and

“(v) whether the spyware poses a counterintelligence risk to the United States or any other threat to the national security of the United States.

“(3) Domestic company that has acquired foreign commercial spyware.—
“(A) AUTHORITY.—The Director of National Intelligence may prohibit any element of the intelligence community from entering into any contract or other agreement for any purpose with a domestic company that has acquired, in whole or in part, any foreign commercial spyware.

“(B) CONSIDERATIONS.—In considering whether and how to exercise the authority under subparagraph (A) with respect to domestic company that has acquired foreign commercial spyware, the Director of National Intelligence shall consider—

“(i) whether the original owner or developer of the spyware retains any of the physical property or intellectual property associated with the spyware;

“(ii) whether the original owner or developer of the spyware has verifiably destroyed all copies of the data collected by or associated with the spyware;

“(iii) whether the personnel of the original owner or developer of the spyware retain any access to data collected by or associated with the spyware;
“(iv) whether the use of the spyware requires the user to connect to an information system of the original owner or developer or of a foreign government; and

“(v) whether the spyware poses a counterintelligence risk to the United States or any other threat to the national security of the United States.

“(4) WAIVER AUTHORITY.—

“(A) IN GENERAL.—The head of an element of the intelligence community may request from the Director of National Intelligence the waiver of a prohibition made under paragraph (1), (2), or (3). The Director may issue such a waiver in response to such a request if—

“(i) such waiver is in the national security interest of the United States; and

“(ii) the Director submits to the congressional intelligence committees the notice described in subparagraph (B).

“(B) NOTICE.—Not later than 30 days after issuing a waiver under subparagraph (A), the Director of National Intelligence shall submit to the congressional intelligence committees notice of the waiver. Such notice shall include—
“(ii) the rationale for issuing the waiver; and

“(iii) the considerations that informed the ultimate determination of the Director to issue the waiver.

“(5) TERMINATION OF PROHIBITION.—The Director of National Intelligence may terminate a prohibition made under paragraph (1), (2), or (3) at any time.

“(d) NOTIFICATIONS.—

“(1) IN GENERAL.—Not later than 30 days after the date on which the Director of National Intelligence exercises the authority to issue a prohibition under subsection (c), the Director of National Intelligence shall notify the congressional intelligence committees of such exercise of authority. Such notice shall include—

“(A) a description of the circumstances under which the prohibition was issued;

“(B) an identification of the company or product covered by the prohibition;
“(C) any information that contributed to the decision of the Director to exercise the authority, including any information relating to counterintelligence or other risks to the national security of the United States posed by the company or product, as assessed by the intelligence community; and

“(D) an identification of each element of the intelligence community to which the prohibition has been applied.

“(2) COUNTERINTELLIGENCE NOTIFICATIONS.—Not later than 30 days after the date on which an element of the intelligence community becomes aware that a Government-issued mobile device was targeted or compromised by foreign commercial spyware, the Director of National Intelligence, in coordination with the Director of the Federal Bureau of Investigation, shall notify the congressional intelligence committees of such determination, including—

“(A) the component of the element and the location of the personnel whose device was targeted or compromised;

“(B) the number of devices compromised or targeted;
“(C) an assessment by the intelligence community of the damage to national security of the United States resulting from any loss of data or sensitive information;

“(D) an assessment by the intelligence community of any foreign government, or foreign organization or entity, and, to the extent possible, the foreign individuals, who directed and benefitted from any information acquired from the targeting or compromise; and

“(E) as appropriate, an assessment by the intelligence community of the capacity and will of such governments or individuals to continue targeting personnel of the United States Government.

“(e) DEFINITIONS.—In this section:

“(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ‘appropriate congressional committees’ means—

“(A) the Committee on Foreign Affairs, the Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives; and
“(B) the Committee on Foreign Relations, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate.

“(2) DOMESTIC COMPANY.—The term ‘domestic company’ means a commercial entity, or any subsidiary or affiliate of the entity, incorporated or domiciled in the United States that—

“(A) sells, leases, or otherwise provides foreign commercial spyware, including by reason of—

“(i) taking ownership, in whole or in part, of a foreign spyware company; or

“(ii) entering into a partnership with a foreign spyware company; or

“(B) otherwise owns, leases, or has access to foreign commercial spyware.

“(3) FOREIGN COMMERCIAL SPYWARE.—The term ‘foreign commercial spyware’ means a tool (or set of tools) sold, leased, marketed, or otherwise provided as an end-to-end system originally developed or owned by a foreign spyware company that provides a purchaser remote access to information stored on or transiting through an electronic device connected to the internet, including end-to-end systems that—
“(A) allow malign actors to infect mobile
and internet-connected devices with malware
over both wireless internet and cellular data
connections, including without any action re-
quired by the user of the device;

“(B) can record telephone calls and other
audio;

“(C) track the location of the device; or

“(D) access and retrieve information on
the device, including text messages, files, e-
mails, transcripts of chats, contacts, photos,
and browsing history.

“(4) FOREIGN SPYWARE COMPANY.—The term
‘foreign spyware company’ means an entity that is—

“(A) incorporated or domiciled outside the
United States; and

“(B) not subject to the laws and regula-
tions of the United States regulating the sur-
veillance of citizens of the United States and
foreign citizens.

“(5) GOVERNMENT-ISSUED MOBILE DEVICE.—
The term ‘Government-issued mobile device’ means
a smartphone, tablet, or laptop, or similar portable
computing device, that is issued to personnel if the
intelligence community by a department or agency of
the United States Government for official use by the personnel.

“(6) UNITED STATES PERSON.—The term ‘United States person’ has the meaning given that term in Executive Order 12333 (50 U.S.C. 3001 note), or any successor order.”.

(e) GOVERNMENT-ISSUED MOBILE DEVICES.—

(1) REQUIREMENT.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall—

(A) issue standards, guidance, best practices, and policies for elements of the intelligence community to protect Government-issued mobile devices from being compromised by foreign commercial spyware;

(B) survey elements of the intelligence community regarding the processes used by the elements to routinely monitor Government-issued mobile devices for known indicators of compromise associated with foreign commercial spyware; or

(C) submit to the appropriate congressional committees a report on the sufficiency of the measures in place to routinely monitor Government-issued mobile devices of appropriate
personnel of the intelligence community for known indicators of compromise associated with foreign commercial spyware.

(2) FORM.—The report under subparagraph (B) may be submitted in classified form.

(3) PRIVATE SECTOR PARTNERSHIPS.—Section 904(d)(7) of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3383(d)(7)) is amended by adding at the end the following new paragraph:

“(E) VULNERABILITIES FROM FOREIGN COMMERCIAL SPYWARE.—

“(i) CONSULTATION.—In carrying out efforts to secure Government-issued mobile devices, to consult with the private sector of the United States and reputable third-party researchers to identify vulnerabilities from foreign commercial spyware and maintain effective security measures for such devices.

“(ii) DEFINITIONS.—In this subparagraph, the terms ‘Government-issued mobile devices’ and ‘foreign commercial spyware’ have the meaning given those terms in section 1102A of the National Security Act of 1947.”.
(f) Imposition of Sanctions Against Certain Persons Engaged in Proliferation or Use of Foreign Commercial Spyware.—

(1) Discretionary sanctions.—The President may impose the sanctions described in paragraph (2) with respect to—

(A) a foreign company the President determines, based on credible evidence, to pose a counterintelligence or other risk to the national security of the United States, such as a company included on the watchlist required by subsection (b) of section 1102A of the National Security Act of 1947, as added to subsection (d).

(B) any foreign individual who—

(i) is a current or former senior executive officer employed by a company described in subparagraph (A); and

(ii) is responsible for or complicit in, or has directly or indirectly engaged in, the proliferation of foreign commercial spyware that could enable the targeting of United States Government officials or personnel of the intelligence community;

(C) any foreign individual who—
(i) is a current or former official of a foreign government or is acting for or on behalf of such official; and

(ii) is responsible for or complicit in, or has directly or indirectly engaged in, the targeting of United States Government officials or personnel of the intelligence community through the use of foreign commercial spyware; or

(D) any foreign person that has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of—

(i) a foreign company selling, leasing, or otherwise providing foreign commercial spyware; or

(ii) the targeting of United States Government officials or personnel of the intelligence community through the use of foreign commercial spyware.

(2) Sanctions described.—The sanctions described in this paragraph are the following:

(A) Blocking of property.—The President shall exercise all of the powers granted to the President under the International Emer-
gency Economic Powers Act (50 U.S.C. 1701 et seq.) (except that the requirements of section 202 of such Act (50 U.S.C. 1701) shall not apply) to the extent necessary to block and prohibit all transactions in property and interests in property of a person determined by the President to be subject to paragraph (1) if such property and interests in property are in the United States, come within the United States, or come within the possession or control of a United States person.

(B) **Inadmissibility to the United States and Revocation of Visa or Other Documentation.**

(i) **Ineligibility for visa, admission, or parole.**—In the case of a foreign person determined by the President to be subject to paragraph (1) who is an individual, the foreign person is—

(I) inadmissible to the United States;

(II) ineligible to receive a visa or other documentation to enter the United States; and
(III) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(ii) CURRENT VISA REVOKED.—In the case of a foreign person determined by the President to be subject to paragraph (1) who is an individual, the visa or other entry documentation of the person shall be revoked, regardless of when such visa or other entry documentation is or was issued. A revocation under this subparagraph shall take effect immediately and automatically cancel any other valid visa or entry documentation that is in the person’s possession.

(iii) EXCEPTION TO COMPLY WITH INTERNATIONAL OBLIGATIONS.—Sanctions under this paragraph shall not apply with respect to a foreign person if admitting or paroling the person into the United States is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations,
signed at Lake Success June 26, 1947,
and entered into force November 21, 1947,
between the United Nations and the
United States, or other applicable inter-
national obligations.

(3) IMPLEMENTATION; PENALTIES.—

(A) IMPLEMENTATION.—The President
may exercise all authorities provided under sec-
tions 203 and 205 of the International Emer-
and 1704) to carry out this subsection and shall
issue such regulations, licenses, and orders as
are necessary to carry out this subsection.

(B) PENALTIES.—Any person that vio-
lates, attempts to violate, conspires to violate,
or causes a violation of this subsection or any
regulation, license, or order issued to carry out
subparagraph (A) shall be subject to the pen-
alties provided for in subsections (b) and (c) of
section 206 of the International Emergency
Economic Powers Act (50 U.S.C. 1705) to the
same extent as a person that commits an un-
lawful act described in subsection (a) of that
section.
(4) Exception relating to importation of goods.—

(A) In general.—The authorities to impose sanctions authorized under this subsection shall not include the authority to impose sanctions on the importation of goods.

(B) Good defined.—In this paragraph, the term “good” means any article, natural or man-made substance, material, supply or manufactured product, including inspection and test equipment, and excluding technical data.

(5) Termination.—The President may terminate the application of sanctions under this subsection at any time.

(g) Report on harmonization among Five Eyes partnership.—

(1) Requirement.—Not later than 30 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 potential for the United States to lead an effort to devise and implement a common approach with the Five Eyes Partnership to mitigate the counterintelligence risks posed by the proliferation of foreign commercial spyware, including by seeking commit-
ments from partner countries of the Five Eyes Partnership to implement measures similar to the requirements under this section and section 1102A of the National Security Act of 1947 (50 U.S.C. 3231 et seq.), as added by this section.

(2) FORM.—The report under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex, consistent with the protection of intelligence sources and methods.

(h) DEFINITIONS.—In this section:

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

(A) the Committee on Foreign Affairs, the Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives; and

(B) the Committee on Foreign Relations, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate.

(2) FOREIGN COMMERCIAL SPYWARE; FOREIGN SPYWARE COMPANY; GOVERNMENT-ISSUED MOBILE DEVICE.—The terms “foreign commercial spyware”, “foreign spyware company”, and “Government-issued mobile device” have the meanings given those
terms in section 1102A of the National Security Act of 1947 (50 U.S.C. 3231 et seq.), as added by this section.

(3) Five Eyes Partnership.—The term “Five Eyes Partnership” means the intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

(4) Foreign person.—The term “foreign person” means a person that is not a United States person.

(5) Person.—The term “person” means an individual or an entity (including a company).

SEC. 310. EXPANSION OF TREATMENT OF MOVING EXPENSES.

(a) Deduction.—Section 217(k) of the Internal Revenue Code of 1986 is amended by inserting “or an employee or new appointee of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) (other than a member of the Armed Forces of the United States) who moves pursuant to a change in assignment that requires relocation” after “to whom subsection (g) applies”.

(b) Exclusion for Qualified Moving Expense Reimbursements.—Section 132(g)(2) of the Internal Revenue Code of 1986 is amended by inserting “or an em-
ployee or new appointee of the intelligence community (as
defined in section 3 of the National Security Act of 1947
(50 U.S.C. 3003)) (other than a member of the Armed
Forces of the United States) who moves pursuant to a
change in assignment that requires relocation” after
“change of station”.

(c) EFFECTIVE DATE.—The amendments made by
this section shall apply to taxable years beginning after
December 31, 2021.

SEC. 311. PERSONNEL VETTING PERFORMANCE MEASURES.

(a) MEASURES.—Not later than 180 days after the
date of the enactment of this Act, the Director of National
Intelligence, acting as the Security Executive Agent, and
in coordination with the Chair and other principals of the
Council, shall develop performance measures to assess the
vetting of personnel, including measures to assess contin-
uous vetting and the quality of each phase of the security
clearance process, including the initiation, investigation,
and adjudication phases.

(b) REPORT.—

(1) REQUIREMENT.—Not later than 180 days
after the date of the enactment of this Act, the Di-
rector of National Intelligence shall submit to the
congressional intelligence committees a report de-
scribing the performance measures developed under subsection (a).

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

(A) A description of how departments and agencies of the United States Government have implemented Security Executive Agent Directive 6 titled “Continuous Evaluation” and related personnel vetting performance measures to ensure that implementation is efficient and effective, including the resources expended by each department or agency for continuous vetting and whether departments and agencies are identifying security-relevant information in a timely manner.

(B) A description of the performance measures the Director of National Intelligence and the Secretary of Defense use to assess the quality of each phase of the security clearance process, including initiation, investigation, adjudication, reinvestigation, and continuous vetting.

(C) How such performance measures meet key attributes for successful performance measures as described in the report of the Comp-
troller General of the United States titled “Per-
sonnel Vetting: Actions Needed to Implement
Reforms, Address Challenges, and Improve
Planning” (GAO–22–104093).

(D) Any impediments or constraints relat-
ing to the implementation of Security Executive
Agent Directive 6 or the development of such
performance measures to assess the quality of
the clearance process.

(c) DEFINITIONS.—The terms “continuous vetting”,
“Council”, and “Security Executive Agent” have the
meanings given those terms in section 6601 of the Damon
Paul Nelson and Matthew Young Pollard Intelligence Au-
thorization Act for Fiscal Years 2018, 2019, and 2020
(50 U.S.C. 3352).

SEC. 312. PROACTIVE CYBERSECURITY.
(a) SURVEY OF ELEMENTS.—Pursuant to section
103G(b)(1) of the National Security Act (50 U.S.C.
3032(b)(1)), not later than 1 year after the date of the
enactment of this Act, the Chief Information Officer of
the Intelligence Community shall conduct a survey of each
element of the intelligence community on the use by that
element of proactive cybersecurity initiatives, continuous
monitoring, and active defense techniques.

(b) REPORT BY CHIEF INFORMATION OFFICER.—
(1) REPORT.—Not later than 1 year after the date of the completion of the survey under subsection (a), the Chief Information Officer of the Intelligence Community shall submit to the congressional intelligence committees a report on proactive cybersecurity initiatives, continuous monitoring, and active defense techniques. Such report shall include the following:

(A) The results of the survey of each element of the intelligence community conducted under subsection (a), including—

(i) examples of any successes against attackers who unlawfully breached an information system of an element of the intelligence community; and

(ii) concerns, limitations, and associated recommendations relating to innovative uses of proactive cybersecurity initiatives.

(B) An analysis of the feasibility, costs, and benefits of consolidating oversight and implementation of such methods within the intelligence community, including whether such consolidation would significantly enhance defense.
(C) An analysis of any statutory or policy limitations on the ability of the Director of National Intelligence, or the head of any element of the intelligence community, to carry out such methods on behalf of an element of the intelligence community or multiple such elements.

(D) An analysis of the relationships between and among the intelligence community, the Department of Defense, the Cybersecurity and Intelligence Security Agency of the Department of Homeland Security, national laboratories, and the private sector, and whether such relationships should be enhanced to protect national security systems of the intelligence community through proactive cybersecurity measures.

(E) With respect to active defense techniques, a discussion of the effectiveness of such techniques to protect the information systems of the elements of the intelligence community, any constraints that hinder such techniques, and associated recommendations.

(F) With respect to continuous monitoring, a discussion of—
(i) how an information system operates under normal and intended use, compared to how such system operates under a variety of adverse conditions and scenarios; and

(ii) the feasibility of the adoption of continuous monitoring among the intelligence community.

(G) Recommendations for legislative action and further resources relating to the successful use of proactive cybersecurity initiatives, deception environments, and continuous monitoring.

(2) FORM.—The report under paragraph (1) may be submitted in classified form.

(c) DEFINITIONS.—In this section:

(1) ACTIVE DEFENSE TECHNIQUE.—The term “active defense technique” means an action taken on an information system of an element of the intelligence community to increase the security of such system against an attacker, including—

(A) the use of a deception technology or other purposeful feeding of false or misleading information to an attacker accessing such system; or
(B) proportional action taken in response
to an unlawful breach.

(2) CONTINUOUS MONITORING.—The term
“continuous monitoring” means continuous experi-
mentation conducted by an element of the intel-
ligence community on an information system of such
element to evaluate the resilience of such system
against a malicious attack or condition that could
compromise such system for the purpose of improv-
ing design, resilience, and incident response with re-
spect to such system.

(3) DECEPTION TECHNOLOGY.—The term “de-
ception technology” means an isolated digital envi-
ronment, system, or platform containing a replica-
tion of an active information system with realistic
data flows to attract, mislead, and observe an
attacker.

(4) INTELLIGENCE COMMUNITY INFORMATION
ENVIRONMENT.—The term “intelligence community
information environment” has the meaning given the
term in Intelligence Community Directive 121, or
any successor document.

(5) NATIONAL LABORATORY.—The term “na-
tional laboratory” has the meaning given that term
in section 2 of the Energy Policy Act of 2005 (42


(7) NATIONAL SECURITY SYSTEM.—The term “national security system” has the meaning given that term in section 3552 of title 44, United States Code.

(8) PROACTIVE CYBERSECURITY INITIATIVES.—The term “proactive cybersecurity initiatives” means actions performed periodically and continuously within an organization, focused on identifying and eliminating vulnerabilities within the network infrastructure, preventing security breaches, and evaluating the effectiveness of the business security posture in real-time, including threat hunting, endpoint and network monitoring, and cybersecurity awareness and training.
SEC. 313. LIMITATION ON AVAILABILITY OF FUNDS FOR INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT PENDING SUBMISSION OF REPORT ON DOMESTIC ACTIVITIES OF INTELLIGENCE COMMUNITY.

Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2023 for the Intelligence Community Management Account, 5 percent may not be obligated or expended until the date on which the Director of National Intelligence submits the report required by section 505(c) of the Intelligence Authorization Act for Fiscal Year 2022 (division X of Public Law 117–103; 50 U.S.C. 3112 note).

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

SEC. 401. MODIFICATIONS TO RESPONSIBILITIES AND AUTHORITIES OF DIRECTOR OF NATIONAL INTELLIGENCE.

Section 102A of the National Security Act of 1947 (50 U.S.C. 3024), as amended by section 304, is further amended—

(1) in subsection (c)—
(A) in paragraph (1)(A), by striking “guidance” and inserting “specific requirements”; 

(B) in paragraph (3)(B), by inserting “establish specific requirements and” after “shall”; 

and 

(C) in paragraph (5)(C), by striking “may” and inserting “shall”; 

(2) in subsection (h)—

(A) in paragraph (1)(A)—

(i) by striking “encourage” and inserting “require”; and

(ii) by inserting “and apolitical” after “sound”; and

(B) by amending paragraph (3) to read as follows; 

“(3) ensure that substantial differences in analytic judgment are fully considered, brought to the attention of policymakers, and documented in analytic products; and”;

(3) in subsection (i)—

(A) in paragraph (1), by inserting “establish and enforce policies to” after “shall”; 

(B) in paragraph (2), by striking “guidelines” and inserting “requirements”; and
(C) by adding at the end the following new paragraph:

“(4) Each head of an element of the intelligence community shall ensure that any congressionally mandated report submitted to Congress by the head, other than such a report submitted solely to the congressional intelligence committees, shall be consistent with the protection of intelligence sources and methods in accordance with the policies established by the Director under paragraph (1), regardless of whether the provision of law mandating the report explicitly requires such protection.”; and

(4) in subsection (x)—

(A) in the matter preceding paragraph (1), by striking “the head of each department of the Federal Government that contains an element of the intelligence community and the Director of the Central Intelligence Agency” and inserting “the heads of the elements of the intelligence community”; and

(B) in paragraph (1)—

(i) in subparagraph (A), by striking “; and” and inserting a semicolon;

(ii) in subparagraph (B), by striking the semicolon and inserting “; and”; and
(iii) by adding at the end the following new subparagraph:

“(C) each contract awarded by an element of the intelligence community includes provisions granting consent for the network monitoring by the element of any information technology network used to perform work under such contract, regardless of the classification level of such network.”.

SEC. 402. ANNUAL SUBMISSION TO CONGRESS OF NATIONAL INTELLIGENCE PRIORITIES FRAMEWORK.

(a) Annual Submission.—Section 102A(p) of the National Security Act of 1947 (50 U.S.C. 3023(p)) is amended by inserting at the end the following new paragraph:

“(3) Not later than October 1 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees a copy of the most recently updated National Intelligence Priorities Framework of the Office of the Director of National Intelligence (or any such successor mechanism).”.

(b) Limitation on Availability of Funds for Intelligence Community Management Account.—Of the funds authorized to be appropriated by this Act
or otherwise made available for fiscal year 2023 for the
Intelligence Community Management Account, 5 percent
may not be obligated or expended until the date on which
the Director of National Intelligence submits the first copy
required under paragraph (3) of such section 102A(p), as
added by subsection (a).

SEC. 403. DISPOSITION OF RECORDS OF OFFICE OF THE DI-
RECTOR OF NATIONAL INTELLIGENCE.

Section 1096(a) of the Intelligence Reform and Ter-
orism Prevention Act of 2004 (Public Law 108–458; 50
U.S.C. 3001 note) is amended—

(1) by inserting “(1)” before “Upon”;

(2) by adding at the end the following new sen-
tence: “Any records of the Office of the Director of
National Intelligence that are maintained by the
agency as a service for the Office of the Director of
National Intelligence under section 1535 of title 31,
United States Code, (popularly known as the ‘Econ-
omy Act’) may be treated as the records of the agen-
cy when dispositioned as required by law, and any
disclosure of such records between the two agencies
shall not be subject to any otherwise applicable legal
consent requirements or disclosure accounting re-
quirements.”; and
(3) by adding at the end the following new paragraph:

“(2) The records of the Office of the Director of National Intelligence may not be dispositioned pursuant to paragraph (1) without the authorization of the Director of National Intelligence.”.

Subtitle B—Central Intelligence Agency

SEC. 411. AUTHORITY OF CENTRAL INTELLIGENCE AGENCY TO PROVIDE PROTECTION FOR CERTAIN PERSONNEL.

(a) Authority.—Paragraph (4) of section 5(a) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3506(a)) is amended to read as follows:

“(4) Authorize personnel designated by the Director to carry firearms to the extent necessary for the performance of the Agency’s authorized functions, except that, within the United States, such authority shall be limited to the purposes of—

“(A) the training of Agency personnel and other authorized persons in the use of firearms;

“(B) the protection of classified materials and information;

“(C) the protection of installations and property of the Agency;
“(D) the protection of—

“(i) current and former Agency personnel and their immediate families;

“(ii) individuals nominated by the President to the position of Director (including with respect to an individual whom a President-elect (as defined in section 3(e) of the Presidential Transition Act of 1963 (3 U.S.C. 102 note) has declared an intent to nominate) and their immediate families; and

“(iii) defectors and their immediate families, and other persons in the United States under Agency auspices; and

“(E) with respect to the Office of the Director of National Intelligence, the protection of—

“(i) installations and property of the Office of the Director of National Intelligence pursuant to section 15(a)(1);

“(ii) the Director of National Intelligence;

“(iii) current and former personnel of the Office of the Director of National Intelligence and their immediate families as the Director of National Intelligence may designate; and

“(iv) individuals nominated by the President to the position of Director of National In-
telligence (including with respect to an individual whom a President-elect has declared an intent to nominate) and their immediate families;”.

(b) CONFORMING AMENDMENT.—Section 15(d)(1) of such Act (50 U.S.C. 3515(d)(1)) is amended by striking “designated by the Director under section 5(a)(4) to carry firearms for the protection of current or former Agency personnel and their immediate families, defectors and their immediate families, and other persons in the United States under Agency auspices,” and inserting the following: “designated by the Director to carry firearms under subparagraph (D) of section 5(a)(4) or clause (ii), (iii), or (iv) of subparagraph (E) of such section,”.

(c) TECHNICAL AMENDMENT.—Paragraphs (7) and (8) of section 5(a) of such Act (50 U.S.C. 3506(a)) are amended by adjusting the margins to conform with the other paragraphs in such section.

SEC. 412. NOTIFICATION OF USE OF CERTAIN EXPENDITURE AUTHORITIES.

(a) CIA.—Section 8 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3510) is amended by adding at the end the following new subsection:

“(c) NOTIFICATION.—Not later than 30 days after the date on which the Director makes a novel or signifi-
cant expenditure pursuant to subsection (a), the Director shall notify the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate of such expenditure.”.

(b) OTHER ELEMENTS.—Section 102A of the National Security Act of 1947 (50 U.S.C. 3024), as amended by section 402, is further amended—

(1) in subsection (m)(1), by inserting before the period at the end the following: “, including with respect to the notification requirement under section 8(c) of such Act (50 U.S.C. 3510(c))”;

(2) in subsection (n), by adding at the end the following new paragraph:

“(5) Any authority provided to the Director of National Intelligence or the head of an element of the intelligence community pursuant to this subsection to make an expenditure referred to in subsection (a) of section 8 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3510) is subject to the notification requirement under subsection (c) of such section. If the Director of National Intelligence is required to make a notification for a specific expenditure pursuant to both this paragraph and paragraph (4)(G), the Director may make a single notification.”.
SEC. 413. CLARIFICATION OF AUTHORITIES RELATING TO
SECURITY PERSONNEL AT OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE FACILITIES AND INSTALLATIONS.

(a) Authority of Central Intelligence Agency Security Personnel.—

(1) Authority.—Section 15(a)(1) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3515(a)(1)) is amended—

(A) in subparagraph (C), by striking “; and” and inserting a semicolon;

(B) by redesignating subparagraph (D) as subparagraph (E);

(C) by inserting after subparagraph (C) the following new subparagraph:

“(D) within any facility or installation operated by the Director of National Intelligence; and”;

(D) in subparagraph (E), as redesignated by subparagraph (B), by striking “subparagraph (C)” and inserting “subparagraph (C) or (D),”.

(2) Rules and Regulations.—Section 15(a)(4) of such Act (50 U.S.C. 3515(a)(4)) is amended—
(A) by striking “The rules” and inserting
“(A) Except as provided in subparagraph (B),
the rules”; and
(B) by adding at the end the following new
subparagraph:
“(B) With respect to the areas referred to in subpara-
graph (D) of paragraph (1), the rules and regulations en-
forced by such personnel and applicable to such areas shall
be the rules and regulations prescribed by the Director,
in coordination with the Director of National Intel-
ligence.”.

(3) Conforming Amendment.—Section
15(a)(2) of such Act (50 U.S.C. 3515(a)(2)) is
amended by striking “(D)” and inserting “(E)”.
(b) Authority of Office of Director of Na-
tional Intelligence Security Personnel.—Section
102A(m) of the National Security Act of 1947 (50 U.S.C.
3024(m)), as amended by section 412(b)(1), is further
amended by adding at the end the following new para-
graph:
“(3) In addition to the authority provided to the Di-
rector of the Central Intelligence Agency to authorize se-
curity personnel of the Central Intelligence Agency within,
and in certain streets, sidewalks, and open areas with re-
spect to, a facility or installation operated by the Director
of National Intelligence under section 15(a) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3515(a)), the Director of National Intelligence may exercise with respect to the security personnel of the Office of the Director of National Intelligence such authority to the same extent, and subject to the same conditions and limitations, that the Director of the Central Intelligence Agency may exercise such authority with respect to security personnel of the Central Intelligence Agency.”.

SEC. 414. OFFICE OF WORKFORCE SUPPORT OF CENTRAL INTELLIGENCE AGENCY.

(a) ESTABLISHMENT.—Not later than 120 days after the date of the enactment of this Act, the Director shall establish an office, to be known as the “Office of Workforce Support”, to provide independent support and advocacy for the physical and mental health and well-being of current and former officers, employees, and contractors of the Agency.

(b) DEPUTY DIRECTOR; ASSIGNED OFFICERS.—

(1) DEPUTY DIRECTOR.—The Director shall appoint a Deputy Director for Workforce Support as the head of the Office of Workforce Support, who shall report directly to the Director.

(2) FULL-TIME ASSIGNED OFFICERS.—To assist in performing the functions under subsection...
(c), the Director shall ensure there is assigned to the Office of Workforce Support not fewer than 10 officers of the Agency, who shall have no official duties other than duties related to such Office while so assigned.

(e) FUNCTIONS.—The functions of the Office of Workforce Support shall be, with respect to eligible individuals under subsection (e), as follows:

(1) Providing to such individuals independent and confidential advice and assistance, and advocating on behalf of such individuals, on matters relating to health and well-being, including with respect to physical health, mental health, retirement benefits, disability compensation, and other related programs and benefits for which the individual may be eligible (without regard to whether such programs and benefits are administered or funded by the United States Government or the private sector).

(2) Maintaining, and making available to such individuals, the following:

(A) A list of physicians and mental health care providers (including from the private sector, as applicable), who hold an appropriate security clearance, or are eligible to hold an appropriate security clearance, and are qualified
to provide confidential services and support to such individuals.

(B) A list of private attorneys who hold an appropriate security clearance and are qualified to provide to such individuals confidential legal advice, including with respect to physical health, mental health, retirement benefits, disability compensation, and other related matters.

d) Provision of Services to Former Officers, Employees, and Contractors.—In the case of an individual specified in subsection (e)(2), services under the Office of Workforce Support shall be provided upon the request of the individual.

e) Eligibility.—An individual is eligible for receiving a service under the Office of Workforce Support if the individual is—

(1) an officer, employee, or contractor of the Agency; or

(2) a former officer, employee, or contractor of the Agency whose employment or contract with the Agency, as the case may be, concluded not more than 10 years prior to the date on which the individual seeks the service.

f) Briefings.—On a biannual basis until the date of termination under subsection (g), the Director shall
provide to the congressional intelligence committees a briefing on the status of the Office of Workforce Support, including on—

(1) the number of officers assigned to such Office pursuant to subsection (b)(2); and

(2) the number of eligible individuals under subsection (e) who have received services under such Office, and the type of services so received.

(g) TERMINATION.—The Office of Workforce Support shall terminate on the date that is 3 years after the date on which such Office is established.

SEC. 415. ESTABLISHMENT OF EXTERNAL ADVISORY BOARD FOR TALENT FOR THE CENTRAL INTELLIGENCE AGENCY.

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

(1) the Central Intelligence Agency plays one of the most critical roles in national defense;

(2) the intelligence provided by the officers of the Agency protects the United States;

(3) to carry out this mission, the Agency needs to attract, train, lead, and retain the most talented and diverse workforce possible;

(4) therefore, the Director must ensure the Agency is incorporating best practices from the pri-
vate sector to hire, lead, manage, and retain the most important element of the organization, Agency personnel; and

(5) An External Advisory Board for Talent will provide the Agency an important mechanism to improve how the Agency recruits, leads, and manages Agency personnel.

(b) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall establish an advisory board for the Central Intelligence Agency, to be known as the “External Advisory Board for Talent” (in this section referred to as the “Board”).

(e) DUTIES.—The duties of the Board shall be to advise the Director and the head of the Talent Center of the Agency, or such successor organizational element, on—

(1) the most up-to-date best practices and innovations in the areas of hiring, leadership, management practices, and talent retention; and

(2) the fostering of a culture of continuous improvement within the Agency, whereby each successive generation of officers of the Agency become more effective leaders and improve the mission performance of the Agency organically and from within.
(d) MEMBERSHIP.—

(1) COMPOSITION.—The Board shall be composed of at least 7 members selected from a diverse range of private sector industries, each of whom shall be, in the determination of the Director, a highly accomplished executive or thought leader in the field of human resource management with a demonstrated history of leading, or advising, high-functioning organizations.

(2) PAY.—Each member of the Board shall be compensated at a rate prescribed by the Director for each day (including travel time) during which the member is engaged in the actual performance of duties vested in the Board.

(3) TRAVEL EXPENSES.—Each member of the Board may receive travel expenses, including per diem in lieu of subsistence, in accordance with applicable provisions under subchapter I of chapter 57 of title 5, United States Code, for travel between the residence of the member and the metropolitan Washington, D.C., area.

(e) MEETINGS.—On a basis that is at least quarterly until the date of termination under subsection (h), the Board shall hold a meeting with the Director to provide the views of the Board on the state of the Agency work-
force, a summary of the minutes of which shall be distrib-
uted among the Agency workforce to ensure transparency.

(f) IMPLEMENTATION OF RECOMMENDATIONS.—

(1) ASSISTANCE FROM TALENT CENTER.—The
head of the Talent Center of the Agency, or such
successor organizational element, shall assist the
Board in carrying out any studies necessary for the
fulfilment of the duties of the Board and shall assist
the Director in implementing any recommendations
of the Board.

(2) AUTHORITY OF DIRECTOR.—The Director
shall retain final authority with respect to the imple-
mentation of any such recommendations.

(g) REPORTS AND BRIEFINGS.—

(1) ANNUAL REPORTS.—On an annual basis
until the date of termination under subsection (h),
the Board shall submit to the Director and the con-
gressional intelligence committees a report on the
state of the Agency workforce.

(2) PERIODIC BRIEFINGS.—On a regular basis
until the date of termination under subsection (h),
the members of the Board shall provide briefings to
the congressional intelligence committees, and the
staff members of such committees.
(h) TERMINATION.—The Board shall terminate on
the date that is 3 years after the date on which the Board
is established.

(i) DEFINITIONS.—In this section, the terms “Agency” and “Director” have the meaning given those terms
in section 1 of the Central Intelligence Agency Act of 1949

SEC. 416. STUDY ON RELATIONSHIP BETWEEN CENTRAL IN-
TELLIGENCE AGENCY AND CONGRESS.

(a) FINDINGS.—Congress finds the following:

(1) In 2008, the Center for the Study of Intel-
ligence of the Central Intelligence Agency published
an unclassified manuscript of a study titled “The
Agency and the Hill: CIA’s Relationship with Con-
gress, 1946-2004”.

(2) The study, organized thematically, provides
a valuable primer for officials of the Agency, mem-
bers of Congress, congressional staff, and the gen-
eral public about the necessarily secret business of
intelligence oversight.

(b) STUDY.—

(1) REQUIREMENT.—Not later than 2 years
after the date of the enactment of this Act, the Di-
rector of the Central Intelligence Agency, acting
through the Center for the Study of Intelligence,
shall prepare a study, in book form, describing the relationship between the Central Intelligence Agency and Congress between the 2004 and 2022. The Director shall ensure that the study is modeled on the manuscript described in subsection (a)(1), including with respect to the organizational structure.

(2) ELEMENTS.—The study under paragraph (1) shall document the following:

(A) Major legislation affecting the Agency.

(B) Programs and budget.

(C) Oversight of analysis.

(D) Oversight of collection.

(E) Oversight of covert action.

(F) Oversight of security and personnel matters.

(G) The process by which officials of the Agency are appointed by the President, by and with the advice and consent of the Senate.

(H) For each of the elements specified in subparagraphs (A) through (G), highlights of the principal issues before Congress and a discussion of how those issues were handled.

(I) Any other matters the Director determines appropriate.
(3) **Submission.**—The Director shall submit to the congressional intelligence committees the study prepared under paragraph (1).

(4) **Form.**—The study under paragraph (1) shall be made in unclassified form, but the Director may submit to the congressional intelligence committees a classified annex.

**SEC. 417. HISTORICAL ADVISORY PANEL OF CENTRAL INTELLIGENCE AGENCY.**

(a) **Sense of Congress.**—It is the sense of Congress that Congress expresses its appreciation—

   (1) to the Director of the Central Intelligence Agency for reconstituting the Historical Advisory Panel; and

   (2) for the important work of the Historical Advisory Panel, especially for—

   (A) the efforts of the Panel to aid with the declassification of materials that enrich the historical national security record; and

   (B) the assistance of the Panel in liaison with the scholarly community.

(b) **Reporting Requirement.**—The Historical Advisory Panel shall report directly to the Director of the Central Intelligence Agency.
(c) **Historical Advisory Panel Defined.**—The term “Historical Advisory Panel” means the panel of the Central Intelligence Agency, regardless of the name of the panel, that assists in conducting declassification reviews and providing other assistance with respect to matters of historical interest.

**Subtitle C—Elements of the Defense Intelligence Enterprise**

**SEC. 421. DEPUTY DIRECTOR FOR DEFENSE INTELLIGENCE RESPONSIBLE FOR WARFIGHTER SUPPORT.**

Section 137 of title 10, United States Code, is amended by adding at the end the following new subsection:

“(e) The Secretary of Defense shall ensure that not fewer than one of the Deputy Directors for Defense Intelligence (or such successor positions) is responsible for warfighter support. An individual appointed to that position shall be a general or flag officer serving in a joint duty assignment.”.

**SEC. 422. COVER ENHANCEMENT AUTHORITIES.**

Part II of title 10, United States Code, is amended by inserting after chapter 88 the following new chapter (and conforming the table of chapters at the beginning of such part accordingly):
CHAPTER 89—COVER ENHANCEMENT

AUTHORITIES

§ 1801. Definitions

In this chapter:

“(1) The term ‘designated employee’ means an employee of the Department of Defense designated by the Secretary of Defense under section 1802(b).

“(2) The term ‘designated member’ means a member of the armed forces designated by the Secretary of Defense under section 1802(b).

“(3) The term ‘Federal retirement system’ includes the Federal Employees’ Retirement System (including the Thrift Savings Plan).

“(4) The term ‘military retirement system’ includes military retired pay programs under chapters 61, 63, 65, and 67 of this title and the Survivor Benefit Plan established by chapter 73 of this title.

§ 1802. Cover enhancement authority

“(a) AUTHORITY.—Notwithstanding any other provision of law, the Secretary of Defense may exercise the au-
thorities under this chapter to protect from unauthorized disclosure—

“(1) intelligence operations of the Department of Defense;

“(2) the identities of undercover officers;

“(3) intelligence sources and methods; or

“(4) cover mechanisms.

“(b) Designation of Employees and Members.—(1) Subject to paragraph (2), the Secretary of Defense may designate any employee of the Department of Defense or member of the armed forces who is under cover to be an employee or a member to whom this chapter applies.

“(2) The Secretary of Defense may not designate more than 15 persons under paragraph (1) in a fiscal year unless the Secretary provides notice of the intent to designate more than 15 persons in such fiscal year to the congressional defense committees and the congressional intelligence committees (as such term is defined in section 3 of the National Security Act of 1957 (50 U.S.C. 3003)).

“(3) A designation may be made under this subsection with respect to any or all authorities exercised under this chapter.

“(c) Interagency Coordination and Support.— Establishment of any such cover enhancement authority
for intelligence operations of the Department of Defense shall be pre-coordinated using processes and procedures for intelligence community deconfliction mutually agreed upon by the Secretary of Defense and the Director of the Central Intelligence Agency.

“§ 1803. Compensation

“The Secretary of Defense may pay a designated employee or designated member salary, allowances, and other benefits in an amount and in a manner consistent with the cover of that employee or member, without regard to any limitation that is otherwise applicable to a Federal employee or member of the armed forces. A designated employee or designated member may accept, use, and, to the extent authorized by regulations prescribed under this chapter, retain any salary, allowances, and other benefits provided under this chapter.

“§ 1804. Retirement benefits

“(a) Establishment of Retirement System.—The Secretary of Defense may establish, administer, contract for, or implement through another Federal department or agency, a cover retirement system for designated employees and designated members (and the spouse, former spouses, and survivors of such designated employees and designated members). A designated employee or designated member may not receive credit for service
under the retirement system established under this para-


graph and another Federal retirement system for the same
time period.

“(b) CONVERSION TO OTHER FEDERAL RETIRE-


MENT SYSTEM.—A designated employee or designated


member participating in the retirement system established


under subsection (a) may convert to coverage under the


Federal retirement system or military retirement system


that would otherwise apply to such employee or member


at any appropriate time determined by the Secretary of


Defense (including at the time of separation of service by


reason of retirement), if the Secretary of Defense deter-


mines that the participation of the employee or member


in the retirement system established under this subsection


is no longer necessary to protect from unauthorized disclo-


sure—


“(1) intelligence operations;


“(2) the identities of undercover officers;


“(3) intelligence sources and methods; or


“(4) cover mechanisms.


“(c) CONVERSION TREATMENT.—Upon a conversion


under subsection (b)—


“(1) all periods of service under the retirement


system established under this section shall be

deemed periods of creditable service under the appli-
cable Federal retirement system or military retirement system;

“(2) the Secretary of Defense shall transmit an amount for deposit in any applicable fund of that Federal retirement system or military retirement system that—

“(A) is necessary to cover all employee or member and agency contributions including—

“(i) interest as determined by the head of the agency administering the Federal retirement system or military retirement system into which the employee or member is converting; or

“(ii) in the case of an employee or member converting into the Federal Employee’s Retirement System or military retirement system, interest as determined under chapter 84 of title 5 or chapter 74 of this title, as the case may be; and

“(B) ensures that such conversion does not result in any unfunded liability to that fund; and

“(3) in the case of a designated employee or designated member who participated in an employee or member investment retirement system established
under subsection (a) and is converted to coverage
under the Federal retirement system or military re-
tirement system, the Secretary of Defense may
transmit any or all amounts of that designated em-
ployee or designated member in that employee or
military investment retirement system (or similar
part of that retirement system) to the Thrift Sav-
ings Fund.

“(d) TRANSMITTED AMOUNTS.—(1) Amounts de-
scribed under subsection (c)(2) shall be paid from any
fund the Secretary of Defense deems appropriate.

“(2) The Secretary of Defense may use amounts con-
tributed by the designated employee or designated member
to a retirement system established under subsection (a)
to offset amounts paid under paragraph (1).

“(e) RECORDS.—The Secretary of Defense shall
transmit all necessary records relating to a designated em-
ployee or designated member who converts to a Federal
retirement system or military retirement system under
subsection (b) (including records relating to periods of
service which are deemed to be periods of creditable serv-
ice under subsection (c)(1)) to the head of the agency ad-
ministering that Federal retirement system or military re-
tirement system.
§ 1805. Health insurance benefits

“(a) IN GENERAL.—The Secretary of Defense may establish, administer, contract for, or implement through another Federal agency, a cover health insurance program for designated employees and designated members and eligible family members. A designated employee or designated member may not participate in the health insurance program established under this section and the program under chapter 89 of title 5 or chapter 55 of this title at the same time.

“(b) CONVERSION TO FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM.—A designated employee participating in the health insurance program established under subsection (a) may convert to coverage under the program under chapter 89 of title 5, and a designated member participating in the program established under subsection (a) may convert to coverage under the program under chapter 55 of this title or chapter 17 of title 38, at any appropriate time determined by the Secretary of Defense (including at the time of separation of service by reason of retirement), if the Secretary of Defense determines that the participation of the employee or member in the health insurance program established under this subsection is no longer necessary to protect from unauthorized disclosure—

“(1) intelligence operations;
“(2) the identities of undercover officers;
“(3) intelligence sources and methods; or
“(4) cover mechanisms.
“(c) CONVERSION TREATMENT.—Upon a conversion
of a designated employee under subsection (b)—
“(1) the employee (and family, if applicable)
shall be entitled to immediate enrollment and cov-
erage under chapter 89 of title 5;
“(2) any requirement of prior enrollment in a
health benefits plan under chapter 89 of title 5 for
continuation of coverage purposes shall not apply;
“(3) the employee shall be deemed to have had
coverage under chapter 89 of title 5 from the first
opportunity to enroll for purposes of continuing cov-
erage; and
“(4) the Secretary of Defense shall transmit an
amount for deposit in the Employees’ Health Bene-
fits Fund that is necessary to cover any costs of
such conversion.
“(d) TRANSMITTED AMOUNTS.—Any amount de-
scribed under subsection (c)(4) shall be paid from any
fund the Secretary of Defense deems appropriate.
“(e) ELIGIBLE FAMILY MEMBER DEFINED.—In this
section, the term ‘eligible family member’ means—
“(1) with respect to an employee, a member of a family as defined in section 8901 of title 5; and
“(2) with respect to a member of the armed forces, a dependent as defined in section 1072 of this title.

§ 1806. Life insurance benefits

“(a) IN GENERAL.—The Secretary of Defense may establish, administer, contract for, or implement through another Federal agency, a cover life insurance program for designated employees and designated members (and the family of such designated employees or designated members). A designated employee or designated member may not participate in the life insurance program established under this section and the program under chapter 87 of title 5 for the same time period.

“(b) CONVERSION TO FEDERAL EMPLOYEES GROUP LIFE INSURANCE PROGRAM.—A designated employee participating in the life insurance program established under subsection (a) may convert to coverage under the program under chapter 87 of title 5, and a designated member participating in the life insurance program established under subsection (a) may convert to coverage under the program under chapter 19 of title 38, at any appropriate time determined by the Secretary of Defense (including at the time of separation of service by reason of retirement), if
the Secretary of Defense determines that the participation of the employee or member in the life insurance program established under this section is no longer necessary to protect from unauthorized disclosure—

“(1) intelligence operations;

“(2) the identities of undercover officers;

“(3) intelligence sources and methods; or

“(4) cover mechanisms.

“(e) CONVERSION TREATMENT.—Upon a conversion of a designated employee under subsection (b)—

“(1) the employee (and family, if applicable) shall be entitled to immediate coverage under chapter 87 of title 5;

“(2) any requirement of prior enrollment in a life insurance program under chapter 87 of title 5 for continuation of coverage purposes shall not apply;

“(3) the employee shall be deemed to have had coverage under chapter 87 of title 5 for the full period of service during which the employee would have been entitled to be insured for purposes of continuing coverage; and

“(4) the Secretary of Defense shall transmit an amount for deposit in the Employees’ Life Insurance
Fund that is necessary to cover any costs of such conversion.

“(d) TRANSMITTED AMOUNTS.—Any amount described under subsection (c)(4) shall be paid from any fund the Secretary of Defense deems appropriate.

“§ 1807. Exemption from certain requirements

“The Secretary of Defense may exempt a designated employee or designated member from mandatory compliance with any Federal regulation, rule, standardized administrative policy, process, or procedure that the Secretary of Defense determines—

“(1) would be inconsistent with the cover of that employee or member; and

“(2) could expose that employee to detection as a Federal employee or that member as a member of the armed forces.

“§ 1808. Taxation and social security

“(a) IN GENERAL.—Notwithstanding any other provision of law, a designated employee or designated member—

“(1) shall file a Federal or State tax return as if that employee or member is not a Federal employee or member of the armed forces and may claim and receive the benefit of any exclusion, deduction, tax credit, or other tax treatment that
would otherwise apply if that designated employee
was not a Federal employee or that designated mem-
ber was not a member of the armed forces, if the
Secretary of Defense determines that taking any ac-
tion under this subsection is necessary to protect
from unauthorized disclosure—

“(A) intelligence operations;
“(B) the identities of undercover officers;
“(C) intelligence sources and methods; or
“(D) cover mechanisms; and

“(2) shall receive social security benefits based
on the social security contributions made.

“(b) COMPENSATION FOR CERTAIN INCREASED TAX
LIABILITY.—In the case of a designated employee or des-
ignated member who files a tax return as provided in sub-
section (a)(1), the Secretary may increase (on a grossed-
up basis) the compensation of such employee or member
under section 1803 to account for any increased income
tax liability attributable to having so filed.

“(c) INTERNAL REVENUE SERVICE REVIEW.—The
Secretary of Defense shall establish procedures to carry
out this section. The procedures shall be subject to peri-
odic review by the Internal Revenue Service.
"§ 1809. Regulations

“The Secretary of Defense shall prescribe regulations to carry out this chapter. The regulations shall ensure that the combination of salary, allowances, and benefits that an employee or member designated under this chapter may retain does not significantly exceed, except to the extent determined by the Secretary of Defense to be necessary to exercise the authority in this chapter, the combination of salary, allowances, and benefits otherwise received by employees or members not designated under this chapter.

"§ 1810. Finality of decisions

“Any determinations authorized by this chapter to be made by the Secretary of Defense or a designee of the Secretary shall be final and conclusive and may not be subject to review by any court.

"§ 1811. Subsequently enacted laws

“No law enacted after the effective date of this chapter shall affect the authorities and provisions of this chapter unless such law specifically refers to this chapter.”

SEC. 423. AUTHORITY OF ARMY COUNTERINTELLIGENCE AGENTS TO EXECUTE WARRANTS AND MAKE ARRESTS.

(a) Authority to Execute Warrants and Make Arrests.—Section 7377 of title 10, United States Code, is amended—
(1) in the section heading, by inserting “AND

   **ARMY COUNTERINTELLIGENCE COMMAND**” before the colon; and

(2) in subsection (b)—

   (A) by striking “any employee of the Depart-
   ment of the Army who is a special agent”
   and inserting the following: “any employee of
   the Department of the Army who is—

   “(1) a special agent”;

   (B) in paragraph (1), as designated by
   subparagraph (A), by striking the period at the
   end and inserting “; or”; and

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

   “(2) a special agent of the Army Counterintel-
   ligence Command (or a successor to that command)
   whose duties include conducting, supervising, or co-
   ordinating counterintelligence investigations involv-
   ing potential or alleged violations punishable under
   chapter 37, 113B, or 115 of title 18, and similar of-
   fenses punishable under this title.”.

(b) CLERICAL AMENDMENT.—The table of sections
at the beginning of chapter 747 of such title is amended
by striking the item relating to section 7377 and inserting
the following new item:
SEC. 424. INCLUSION OF SPACE FORCE AS ELEMENT OF INTELLIGENCE COMMUNITY.

Section 3(4)(H) of the National Security Act of 1947 (50 U.S.C. 3003(4)(H)) is amended by inserting “the Space Force,” after “the Marine Corps,”.

SEC. 425. MILITARY INTELLIGENCE COLLECTION AND ANALYSIS PARTNERSHIPS.

(a) USE OF APPROPRIATED FUNDS.—The Director of the Defense Intelligence Agency may use not more than $10,000,000 of appropriated funds available to the Defense Intelligence Agency for each fiscal year to pay for the expenses of partnerships with foreign countries, regional organizations with defense, intelligence, or security components, and security alliances of which the United States is a member for military intelligence collection and analysis activities.

(b) USE OF FUNDS OTHER THAN APPROPRIATED FUNDS.—Notwithstanding any other provision of law, the Director may use funds other than appropriated funds to pay for the expenses of partnerships with foreign countries, regional organizations with defense or security components, and security alliances of which the United States is a member for military intelligence collection and analysis activities, except that—
(1) no such funds may be expended, in whole
or in part, by or for the benefit of the Defense Intel-
ligence Agency for a purpose for which Congress had
previously denied funds;

(2) proceeds from the sale of military intel-
ligence collection and analysis items may be used
only to purchase replacement items similar to the
items that are sold; and

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

(c) LOGISTIC SUPPORT, SUPPLIES, AND SERVICES.—
Notwithstanding any other provision of law, the Director
may exercise the authority under this section to pay for,
or otherwise facilitate, the logistic support, supplies, and
services associated with partnerships with foreign coun-
tries, regional organizations with defense or security com-
ponents, and security alliances of which the United States
is a member.

(d) COORDINATION WITH SECRETARY OF STATE.—
The Director of the Defense Intelligence Agency shall co-
ordinate the military intelligence collection and analysis
activities funded pursuant to this section with the Sec-
retary of State.
(c) **Coordination With Director of National Intelligence.**—The Director of the Defense Intelligence Agency shall coordinate the military intelligence collection and analysis activities funded pursuant to this section with the Director of National Intelligence.

(f) **Budget Exhibit.**—With respect to each fiscal year in which this section is carried out, the Secretary of Defense shall ensure that the defense budget materials include a budget exhibit detailing the receipt and disbursements of funds to be used by the Director of the Defense Intelligence Agency under subsections (a) and (b).

(g) **Sunset.**—

(1) **In general.**—Subject to paragraph (2), the authority to carry out this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(2) **Exception.**—A military intelligence collection and analysis activity for which funds have been obligated under this section before the date on which the authority to carry out this section terminates under paragraph (1) may continue until the completion of the activity.

(h) **Definitions.**—In this section:

(1) **Defense budget materials.**—The term “defense budget materials” has the meaning given
that term in section 231 of title 10, United States Code.

(2) MILITARY INTELLIGENCE COLLECTION AND ANALYSIS ACTIVITY.—The term “military intelligence collection and analysis activity” means—

(A) the conduct of a combined human intelligence and counterintelligence activity;

(B) the collection, processing, exploitation, analysis, and dissemination of all-source intelligence;

(C) the conduct of a foreign defense intelligence liaison relationship or defense intelligence exchange program; or

(D) the research, development, acquisition, and sustainment of an information technology system or telecommunication capability in support of an activity described in subparagraph (A), (B), or (C).

SEC. 426. INTELLIGENCE ASSESSMENT OF EFFECTS OF COUNTERTERRORISM STRIKES.

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

(1) the intelligence community is responsible for ensuring that products compliant with analytic
tradecraft are available to the operational elements of the Department of Defense;

(2) such products must be prepared with the rigor necessary to determine the status of a potential terrorist target, the role of the target, how critical the target is to the operations of a terrorist group, and the effect removing that individual would have on the strategic threat to the United States, United States persons overseas, members of the United States Armed Forces overseas, or facilities of the United States overseas; and

(3) the intelligence community is also responsible for assessing the strategic impact of counterterrorism strikes to determine whether the anticipated or desired impact on the terrorist group or network was achieved.

(b) INTELLIGENCE ASSESSMENT.—The Director of the Defense Intelligence Agency, in coordination with the directorates of intelligence of the combatant commands, shall produce an intelligence assessment of the effects of counterterrorism strikes conducted by the Armed Forces on targets outside of areas of active hostilities during the 5-year period preceding the date of the enactment of this Act.
(c) ELEMENTS.—The assessment under subsection (b) shall include the following:

(1) With respect to the counterterrorism strikes covered by the assessment—

(A) the short- and long-term effects of the strike on the planned external operations of the respective terrorist group, particularly the operations targeting the United States, United States persons overseas, members of the United States Armed Forces overseas, or facilities of the United States overseas;

(B) the effects of the strike on the intent of the respective terrorist group to conduct external operations, particularly the operations targeting the United States, United States persons overseas, members of the United States Armed Forces overseas, or facilities of the United States overseas;

(C) the effects of the strike on the recruitment of the respective terrorist group;

(D) the effects of the strike on the local perception of the respective terrorist group, the host country, and the United States; and
(E) the effects of the strike on the capabilities of the host country to conduct operations against the targeted group.

(2) An identification of the number and quality of finished intelligence products that assessed the effects that a counterterrorism strike of the United States would have, or did have, against specific terrorist individuals or groups.

(3) Recommendations to improve the efficacy, accuracy, and timeliness of intelligence analysis to increase the strategic effect of counterterrorism strikes.

(d) REPORT.—

(1) REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, the Director shall submit to the appropriate congressional committees a report containing the intelligence assessment under subsection (b) and the judgments under paragraph (2).

(2) JUDGMENTS.—The report shall include the following judgments:

(A) What percentage of counterterrorism strikes covered by the intelligence assessment under subsection (b) had a short-term effect on the planned external operations of the respec-
tive terrorist group, particularly the operations targeting the United States, United States persons overseas, members of the United States Armed Forces overseas, or facilities of the United States overseas.

(B) What percentage of counterterrorism strikes covered by the intelligence assessment under subsection (b) had a long-term effect on the planned external operations of the respective terrorist group, particularly the operations targeting the United States, United States persons overseas, members of the United States Armed Forces overseas, or facilities of the United States overseas.

(C) A qualitative assessment of the effects of the counterterrorism strikes.

(3) Form.—The report under paragraph (1) may be submitted in classified form, except that the judgments under paragraph (2) shall be in unclassified form.

(e) Definitions.—In this section:

(1) Appropriate congressional committees.—The term “appropriate congressional committees” means the following:
(A) The congressional intelligence committees.

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

(2) COUNTERTERRORISM STRIKE.—The term “counterterrorism strike” means an air strike conducted by the United States Armed Forces targeting a specific individual that is not a defensive strike conducted to reduce imminent danger to the United States Armed Forces or specifically designated partner forces of the United States.

(3) EXTERNAL OPERATIONS.—The term “external operations”, with respect to a terrorist groups, means violent or lethal operations conducted outside the country or region of origin of the terrorist group.

SEC. 427. SUBMISSION OF CERTAIN LEGISLATIVE PROPOSALS.

(a) REQUIREMENT.—In submitting a covered legislative proposal, the Secretary of Defense shall also simultaneously submit to the congressional intelligence committees the proposal, including a brief explanation of the proposal.
(b) FORM.—A covered legislative proposal submitted under subsection (a) shall be submitted in unclassified form, but may contain a classified annex.

(c) COVERED LEGISLATIVE PROPOSAL DEFINED.—In this section, the term “covered legislative proposal” means a provision of legislation proposed by the Secretary of Defense to Congress that is approved by the Office of Management and Budget and involves the grant, expansion, modification, or cessation of authority involving the intelligence, intelligence-related, or tactical intelligence activities of the Department of Defense.

SEC. 428. OVERSIGHT OF DEFENSE INTELLIGENCE AGENCY CULTURE.

(a) FINDINGS.—Congress finds the following:

(1) The Defense Intelligence Agency has not taken sufficient steps to address an unhealthy culture at the Agency.

(2) In the report of the Permanent Select Committee on Intelligence of the House of Representatives accompanying H.R. 5412 of the 117th Congress (H. Rept. 117–156), the Committee mandated several reports and briefings for which the Defense Intelligence Agency failed to respond in a timely manner.
(3) The Agency has committed to improving Agency culture and leadership; however, actions taken to date fall short of addressing the permissive environment for management abuses.

(b) Mandatory Provision of Exit Survey or Interview.—

(1) In general.—The Director of the Defense Intelligence Agency shall ensure that each employee of such Agency who leaves employment with such Agency (but not including any detail assignment) completes an exit survey or exit interview prior to such departure, to the extent practicable.

(2) Annual Submissions to Congress.—On an annual basis during the 3-year period beginning on the date of the enactment of this Act, the Director of the Defense Intelligence Agency shall submit to the congressional intelligence committees a written analysis of the results of the exit surveys or exit interviews completed pursuant to paragraph (1) during the year covered by the report together with a plan of the Director to address any issues identified pursuant to such results to improve retention and culture.

(c) Congressional Oversight Relating to Workforce Climate Surveys.—
(1) **Notifications of Ad-hoc Workforce Climate Surveys.**—Not later than 14 days after the date on which the Director of the Defense Intelligence Agency conducts an ad-hoc workforce climate survey (including in response to a specific incident or concern), the Director shall notify the congressional intelligence committees.

(2) **Reports on Final Results.**—Not later than 90 days after the date on which the Director of the Defense Intelligence Agency concludes the conduct of any workforce climate survey, the Director shall submit to the congressional intelligence committees a report containing the final results of such workforce climate survey. Such report shall include the following:

(A) The topic of the workforce climate survey, and the workforce level surveyed.

(B) The rationale for conducting the workforce climate survey.

(C) The measures in place to ensure the accessibility of the workforce climate survey.

(D) The lead official or entity conducting the workforce climate survey.
(E) Any actions the Director intends to take, or is considering, in response to the results of the workforce climate survey.

(3) ACCESSIBILITY OF WORKFORCE CLIMATE SURVEYS.—The Director of the Defense Intelligence Agency shall ensure that, to the extent practicable, and consistent with the protection of intelligence sources and methods, workforce climate surveys are accessible to employees of such Agency on classified and unclassified systems.

(d) FEASIBILITY REPORT.—Not later than 270 days after the date of enactment of this Act, the Director of the Defense Intelligence Agency shall submit to the congressional intelligence committees a report containing an analysis of the feasibility (including the anticipated cost, personnel requirements, necessary authorities, and such other matters as may be determined appropriate by the Director for purposes of analyzing feasibility) of—

(1) conducting 360-degree performance reviews among employees of the Defense Intelligence Agency; and

(2) including leadership suitability assessments (including personality evaluations, communication style assessments, and emotional intelligence aptitude assessments) for promotions of such employees
to a position within grade GS–14 or above of the General Schedule.

(c) WORKFORCE CLIMATE SURVEY DEFINED.—In this section, the term “workforce climate survey”—

(1) means a workforce engagement or climate survey conducted at the agency, directorate, career field, or integrated intelligence center level, without regard to whether the survey is conducted on an annual or ad-hoc basis; and

(2) does not include an exit survey specified in subsection (b).

SEC. 429. CYBER INTELLIGENCE SURVEILLANCE RECONNAISSANCE INFORMATION.

(a) QUARTERLY BRIEFINGS.—On a quarterly basis, the Secretary of Defense shall provide to the appropriate congressional committees a briefing on, with respect to the period covered by the briefing, the intelligence activities occurring in cyberspace in support of current and future offensive cyberspace operations or defensive cyberspace operations.

(b) ANNUAL CERTIFICATIONS.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter for 5 years, the Secretary of Defense shall certify to the appropriate congressional committees that, with respect to the period covered by the certification, the
Secretary has reported to such committees all intelligence activities occurring in cyberspace in support of current and future offensive cyberspace operations or defensive cyberspace operations.

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term “appropriate congressional committees” means the following:

(1) The congressional intelligence committees.

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

SEC. 430. INFORMATION ON COVER ACTIVITIES OF DEPARTMENT OF DEFENSE.

(a) INFORMATION.—Not less frequently than quarterly, the Secretary of Defense shall provide to the appropriate congressional committees information on the cover activities of the Department of Defense.

(b) ELEMENTS.—The Secretary shall ensure that the information provided under subsection (a) includes, with respect to the period covered by the information, the following:

(1) A detailed description of each cover activity or cover support activity provided by an element of the Department of Defense to an activity, operation, or other initiative of the Department of Defense or
other department or agency of the United States Government, including—

(A) a description of the specific activity; and

(B) when such activity was approved or decommissioned.

(2) Any other matters the Secretary determines appropriate.

(e) FORM.—The information under subsection (a) may be provided in classified form.

(d) 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).

Subtitle D—Other Elements

SEC. 441. AUTHORIZATION RELATING TO CERTAIN INTELLIGENCE AND COUNTERINTELLIGENCE ACTIVITIES OF COAST GUARD.

(a) AUTHORIZATION.—Subject to subsection (b), and consistent with the policies, procedures, and coordination required pursuant to section 811 of the Counterintell-
eligence and Security Enhancements Act of 1994 (50 U.S.C. 3381) and section 902 of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3382), the Com-
mmandant of the Coast Guard may expend amounts made available for the intelligence and counterintelligence activi-
ties of the Coast Guard to conduct such an activity with-
out regard to any other provision of law or regulation re-
ating to the expenditure of Government funds, if—

(1) the object of the activity is of a confidential, extraordinary, or emergency nature; and

(2) following each such expenditure, the Com-
mandant submits to the congressional intelligence committees a certification that the object of the ac-
tivity conducted was of a nature described in para-
graph (1).

(b) LIMITATION.—Of the funds made available for a fiscal year for the intelligence and counterintelligence ac-
tivities of the Coast Guard, not more than 5 percent may be expended during the fiscal year under subsection (a) to conduct such activities in accordance with such sub-
section unless, for each intended expenditure in excess of such percentage—

(1) the Commandant submits to the congres-
sional intelligence committees a notification of the intent to expend the amounts; and
(2) a period of 30 days has elapsed following
the date on which the Commandant submits such
notification.

(c) ANNUAL REPORT.—

(1) SUBMISSION.—Not later than December 1
of each year, the Commandant shall submit to the
congressional intelligence committees a report on all
expenditures during the preceding fiscal year under
subsection (a).

(2) MATTERS.—Each report under paragraph
(1) shall include, for each individual expenditure cov-
ered by such report that is in excess of the percent-
age specified in subsection (b) for the relevant fiscal
year, the following:

(A) A detailed description of the purpose
of such expenditure.

(B) The amount of such expenditure.

(C) An identification of the approving au-
thority for such expenditure.

(D) A justification as to why other au-
thorities available to the Coast Guard could not
be used for such expenditure.

(E) Any other matters the Commandant
considers appropriate.
(d) CONGRESSIONAL INTELLIGENCE COMMITTEES DEFINED.—In this section, 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).

(e) SUNSET.—This section shall cease to have effect on the date that is 3 years after the date of the enactment of this Act.

SEC. 442. STUDY ON PERSONNEL UNDER STRATEGIC INTELLIGENCE PARTNERSHIP PROGRAM.

(a) STUDY.—The Director of National Intelligence and the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, in consultation with the National Laboratories Directors’ Council, shall jointly conduct a study of the skills, recruitment, and retention of the personnel at the national laboratories who carry out projects under the Strategic Intelligence Partnership Program.

(b) ELEMENTS.—The study under subsection (a) shall address the following:

(1) The degree to which the personnel at the national laboratories who carry out projects under the Strategic Intelligence Partnership Program have the requisite training, skillsets, or expertise in critical science, technology, and engineering areas to
support ongoing and anticipated projects under such Program, and the sufficiency of such personnel.

(2) Whether such personnel have compensation, benefits, and pay scales that are competitive with comparable roles in the private sector in the geographic market in which the relevant national laboratory is located.

(3) Any challenges associated with the retention of such personnel.

(4) The talent composition of such personnel, broken down by career phase and degree status, to include any relevant exit survey data.

(5) A description of current or previous programs to enabling such personnel to rotate between elements of the intelligence community and the national laboratories, including the number of personnel on nonreimbursable or reimbursable assignment to an element of the intelligence community.

(6) The degree to which such projects and personnel support or augment other ongoing mission areas and capacities at the national laboratories.

(c) RECOMMENDATIONS.—Upon completing the study under subsection (a), the Directors shall jointly develop findings and recommendations based on the results of the study regarding the recruitment and retention of
personnel at the national laboratories who carry out projects under the Strategic Intelligence Partnership Program, including with respect to the following:

(1) New or alternative business models, sponsorship arrangements, or work scope agreements.

(2) Extending eligibility for existing, or establishing new, recruitment, retention, or other career incentive programs, including student loan repayment and forgiveness programs, to such personnel.

(3) Initiating geographically flexible or remote work arrangements for such personnel.

(4) Enabling such personnel to participate in training at elements of the intelligence community, or obtain academic training at the National Intelligence University.

(5) Establishing new, or enhancing existing, opportunities for detailee or rotational programs among the intelligence community and the national laboratories.


(7) Any other recommendations the Directors determine relevant.

(d) REPORT.—
(1) REQUIREMENT.—Not later than one year after the date of the enactment of this Act, the Directors shall jointly submit to the congressional intelligence committees a report containing the study under subsection (a) and the recommendations under subsection (c).

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

(e) NATIONAL LABORATORIES DEFINED.—In this section, the term “national laboratories” means—

(1) each national security laboratory (as defined in section 3281(1) of the National Nuclear Security Administration Act (50 U.S.C. 2471(1))); and

(2) each national laboratory of the Department of Energy.

SEC. 443. ASSESSMENT OF HANDLING OF CERTAIN INFORMATION RELATING TO DELIBERATIONS OF BUREAU OF INDUSTRY AND SECURITY.

(a) INSPECTORS GENERAL ASSESSMENT.—

(1) REQUIREMENT.—Not later than 270 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community, in coordination with the Inspector General of the Department of Commerce, shall submit to the appro-
priate congressional committees an assessment of practices for handling covered information that may, in isolation or in aggregate, cause harm to the national security of the United States.

(2) MITIGATION.—The report under paragraph (1) shall include recommended steps, should any be necessary, to improve the secure handling of covered information, including with respect to whether the decisions and deliberations of the Bureau of Industry and Security of the Department of Commerce that involve covered information should be solely conducted on classified networks.

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

(b) DIRECTOR OF NATIONAL INTELLIGENCE ASSESSMENT.—

(1) REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall conduct an assessment of how covered information is transmitted, stored, and secured.

(2) MATTERS INCLUDED.—The assessment under paragraph (1) shall include—
(A) the projected cost of installing classified information systems for use by the Bureau of Industry and Security; and

(B) the feasibility of identifying secured office space for such systems.

(3) SUBMISSION.—Not later than 210 days after the date of enactment of this Act, the Director shall submit to the appropriate congressional committees the findings of the assessment under paragraph (1).

(c) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees;

(B) the Committee on Energy and Commerce of the House of Representatives; and

(C) the Committee on Commerce, Science, and Transportation of the Senate.

(2) COVERED INFORMATION.—The term “covered information” means information provided by an element of the intelligence community to the Bureau of Industry and Security of the Department of Commerce as part of decisions or deliberations by the
Bureau or information or material derived from classified deliberative or decisional interagency policy documents.

TITLE V—MATTERS RELATING TO EMERGING TECHNOLOGIES
Subtitle A—General Matters

SEC. 501. DEFINITIONS.

In this title:

(1) EMERGING TECHNOLOGY COMPANY.—The term "emerging technology company" means a company that is in the business of maturing and selling technology that is in a developmental stage, or that may be developed during the 10-year period beginning on January 1, 2022, including with respect to biotechnology, quantum information science, future generation wireless technology, advanced materials, artificial intelligence, nanotechnology, microelectronics, space technology, renewable energy generation and storage, advanced computing, and human-machine interfaces.

(2) SMALL- OR MEDIUM-SIZED EMERGING TECHNOLOGY COMPANY.—The term "small- or medium-sized emerging technology company" means an emerging technology company with fewer than 1,000 employees.
SEC. 502. OFFICIALS RESPONSIBLE FOR ARTIFICIAL INTELLIGENCE POLICIES OF THE INTELLIGENCE COMMUNITY.

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

(1) the intelligence community must rapidly adopt artificial intelligence into its workflows to compete with United States adversaries, and keep pace with and leverage commercial cutting-edge technologies;

(2) while pockets of success are present across the intelligence community, Congress is concerned that artificial intelligence has not scaled appropriately and continues to lag behind industry;

(3) broadly, Congress believes that the Director of National Intelligence should be primarily responsible for setting the policies and procedures as they relate to artificial intelligence adoption, acquiring any necessary common infrastructure such as training data, intelligence community-wide contracts for data labelers, cloud storage and compute capabilities, and other infrastructure necessary for intelligence community elements rapidly to adopt artificial intelligence; and

(4) the heads of the elements of the intelligence community should be primarily responsible for ac-
quiring and developing agency-specific artificial intelligence applications, in coordination with the Director and the heads of the elements of the intelligence community, and assisting the Director with preparing the necessary infrastructure such as data, hardware, and software for the intelligence community to adopt artificial intelligence applications.

(b) REQUIREMENT TO DEVELOP DEFINITION.—Section 309(a) of the Intelligence Authorization Act for Fiscal Year 2022 (50 U.S.C. 3316c(a)) is amended—

(1) by redesignating paragraphs (3) through (24) as paragraphs (4) through (25), respectively; and

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

“(3) Artificial intelligence.”.

(c) DIRECTOR OF NATIONAL INTELLIGENCE.—Section 102A(n) of the National Security Act of 1947 (50 U.S.C. 3024(n)), as amended by section 412(b)(2), is further amended by adding at the end the following new paragraph:

“(6) The Director of National Intelligence, in consultation with the heads of the elements of the intelligence community and the Director of Science and Technology, shall establish policies and procedures relating to the ac-
quisition and use of artificial intelligence by the intelligence community, including with respect to data, computing, storage, and models necessary for the intelligence community to leverage, incorporate, adopt, and maintain artificial intelligence applications.”.

(d) DIRECTOR OF SCIENCE AND TECHNOLOGY.—

(1) DUAL-HATTED AS CHIEF TECHNOLOGY OFFICER.—Subsection (a) of section 103E of such Act (50 U.S.C. 3030) is amended by inserting at the end the following new sentence: “The Director of Science and Technology shall also serve as the Chief Technology Officer of the Office of the Director of National Intelligence.”.

(2) APPOINTMENT.—Subsection (b) of such section is amended to read as follows:

“(b) REQUIREMENT RELATING TO APPOINTMENT.—An individual appointed as Director of Science and Technology shall have a professional background and experience appropriate for the duties of the Director of Science and Technology. In making such appointment, the Director of National Intelligence shall give preference to an individual with varied professional experiences, including experience outside of the United States Government.”.

(3) POLICIES.—Such section is amended—
(A) by redesignating subsection (d) as subsection (f); and

(B) by inserting after subsection (c) the following new subsection:

“(d) POLICIES.—The Director of Science and Technology shall—

“(1) recommend to the Director of National Intelligence policies and procedures for the intelligence community relating to incorporating artificial intelligence in accordance with section 102A(n);

“(2) conduct reviews of the policies and procedures of the intelligence community relating to the adoption and integration of technology into the intelligence community, including with respect to, as appropriate—

“(A) incentives and policies relating to human resources;

“(B) incentives and policies relating to acquisition and contracting;

“(C) incentives and policies relating to financial management and budgeting; and

“(D) technology standards and policies;

“(3) make recommendations to the Director of National Intelligence with respect to the budgets of the elements of the intelligence community regarding
the matters covered by this section, including with
respect to reprogramming funds to carry out the in-
telligence community-wide artificial intelligence mis-
ion of the Director of National Intelligence;

“(4) coordinate with the Under Secretary of
Defense for Research and Engineering on initiatives,
policies, and programs carried out jointly between
the intelligence community and the Department of
Defense;

“(5) coordinate with the Director of the Office
of Science and Technology Policy to promote intel-
ligence community-specific requirements and per-
spectives within the initiatives of the Office of
Science and Technology Policy; and

“(6) for purposes of integrating the priorities
and requirements of the intelligence community into
a broader national strategy on technology, coordi-
nate with the heads of—

“(A) the National Institute for Standards
and Technology;

“(B) the National Science Foundation; and

“(C) any other department or agency of
the United States Government, federally funded
research and development center, or other enti-
(4) CLARIFICATION OF ROLE.—Such section is amended by inserting after subsection (d), as added by paragraph (3), the following new subsection:

“(e) CLARIFICATION OF ROLE.—The Director of Science and Technology may not have operational control over any program directly managed by an element of the intelligence community other than the Office of the Director of National Intelligence.”.

(e) CHIEF DATA OFFICER.—

(1) IN GENERAL.—The National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended by inserting after section 103J the following new section (and conforming the table of contents at the beginning of such Act accordingly):

“SEC. 103K. CHIEF DATA OFFICER.

“(a) DIRECTOR OF SCIENCE AND TECHNOLOGY.—There is a Chief Data Officer within the Office of the Director of National Intelligence who shall be appointed by the Director of National Intelligence. The Chief Data Officer is the Chief Data Officer of the Office of the Director of National Intelligence for purposes of section 3520 of title 44, United States Code.
“(b) REQUIREMENT RELATING TO APPOINTMENT.—

An individual appointed as the Chief Data Officer shall have a professional background and experience appropriate for the duties of the Chief Data Officer. In making such appointment, the Director of National Intelligence shall give preference to an individual with varied professional experiences, including experience outside of the United States Government.

“(c) DUTIES.—In addition to any other functions and responsibilities specified in section 3520 of title 44, United States Code, the Chief Data Officer—

“(1) shall recommend to the Director of National Intelligence policies and procedures for the intelligence community regarding the acquisition and use of artificial intelligence with respect to the data needs of the intelligence community in support of adopting emerging technologies, in accordance with section 102A(n) and subject to the approval by the Director of National Intelligence, the Director of Science and Technology, and the Chief Information Officer;

“(2) shall conduct reviews of the policies and procedures of the intelligence community relating to data, including with respect to data curation, data labeling, data acquisition, data security, data inter-
operability, and data accessibility, except with respect to such policies and procedures established pursuant to a provision of law or executive order relating to the control, use, retention, collection, or dissemination of data;

“(3) shall conduct ongoing reviews of the data policies of the intelligence community, including to ensure that such policies promote interoperability and accessibility with commercial software providers, including by the promotion of open application programming interfaces;

“(4) shall coordinate with the Chief Data Officer of the Department of Defense and other relevant officials of the Department to ensure consistent data policies and, to the extent practicable and advisable, consistent standards and policies that ensure data is accessible between relevant elements of the intelligence community and the Department;

“(5) may make recommendations to the Director of National Intelligence, acting through the Chief Technology Officer, with respect to the budgets of the elements of the intelligence community regarding data, if such recommendations are—

“(A) consistent with the policies established by the Director; and
“(B) made in furtherance of accelerating the transition to digital business practices across the intelligence community, including with respect to the acquisition, curation, dissemination, and other data practices necessary to adopt artificial intelligence capabilities and other emerging technologies within the intelligence community; and

“(6) shall perform other such duties as may be prescribed by the Director of National Intelligence, the Director of Science and Technology, or specified by law.

“(d) IDENTIFICATION OF CONFLICTS.—Not later than 60 days after the date on which the Chief Data Officer identifies a policy of the intelligence community, including with respect to policies governing the access to data, that restricts the Chief Data Officer from carrying out subsection (c), the Chief Data Officer shall notify the Director of National Intelligence and the congressional intelligence committees of such policy and restriction.”.

(2) INCUMBENT.—The individual serving in the position of Chief Data Officer of the Office of the Director of National Intelligence as of the date of the enactment of this Act may continue to serve in such position without further appointment pursuant
to section 103K of the National Security Act of 1947, as added by paragraph (1).

Subtitle B—Improvements Relating to Procurement

SEC. 511. ADDITIONAL TRANSACTION AUTHORITY.

(a) ADDITIONAL TRANSACTION AUTHORITY.—The National Security Act of 1947 (50 U.S.C. 3001 et seq.), as amended by section 502, is further amended by inserting after section 102A the following new section (and conforming the table of contents at the beginning of such Act accordingly):

“SEC. 102B. ADDITIONAL TRANSACTION AUTHORITY.

“(a) IN GENERAL.—In addition to other acquisition authorities, the head of an element of the intelligence community may exercise the authorities under subsections (b), (c), and (d).

“(b) COOPERATIVE AGREEMENTS AND GRANTS.—The head of an element of the intelligence community may use cooperative agreements and grants, in accordance with chapter 63 of title 31, United States Code, to carry out basic, applied, and advanced research and development, and prototype projects in support of intelligence activities.

“(c) OTHER TRANSACTION AUTHORITY.—The head of an element of the intelligence community may enter into transactions (other than contracts, cooperative agree-
ments, and grants) under the authority of this subsection to carry out basic, applied, and advanced research projects in support of intelligence activities.

“(d) AUTHORITY OF ELEMENTS OF THE INTELLIGENCE COMMUNITY TO CARRY OUT CERTAIN PROTOTYPE PROJECTS.—

“(1) AUTHORITY.—The head of an element of the intelligence community may, under the authority of subsection (e), enter into a transaction to carry out a prototype project in support of intelligence activities only if each party to the transaction, other than the Federal Government, is a covered contractor.

“(2) FOLLOW-ON PRODUCTION CONTRACTS OR TRANSACTIONS.—

“(A) IN GENERAL.—A transaction entered into under this subsection for a prototype project may provide for the award of a follow-on production contract or a follow-on production transaction to the participants in the transaction. A transaction includes all individual prototype subprojects awarded under the transaction to a consortium of United States industry and academic institutions.
“(B) FOLLOW-ON PRODUCTION CONTRACTS.—A follow-on production contract provided for in a transaction under subparagraph (A) may be awarded to the participants in the transaction without the use of any competitive procedure that would otherwise apply if the following criteria are satisfied:

“(i) The authorizing official of the relevant element of the intelligence community determines that Government users of the proposed production product or production service have been consulted.

“(ii) In the case of a proposed production product that is software, there are mechanisms in place for Government users to provide feedback to participants to the follow-on production contract.

“(iii) In the case of a proposed production product that is software, the follow-on production contract includes a requirement that, for the duration of such contract (or such other period of time as may be agreed to as a term of such contract)—
“(I) the participants provide to the head of the relevant element of the intelligence community the most up-to-date version of the production product that is available in the commercial marketplace; and

“(II) there are mechanisms in place for the participants to provide real-time updates to the production product.

“(C) FOLLOW-ON PRODUCTION TRANSACTIONS.—A follow-on production transaction provided for in a transaction under subparagraph (A) may be awarded to the participants in the transaction without the use of any competitive procedure that would otherwise apply.

“(e) RECOVERY OF FUNDS.—

“(1) IN GENERAL.—A cooperative agreement authorized by subsection (a) and a transaction authorized by subsection (c) or (d) may include a clause that requires a person to make payments to the Office of the Director of National Intelligence or any other element of the intelligence community as a condition for receiving support under the agreement or other transaction.
“(2) ACCOUNTING FOR RECOVERED FUNDS.—

The amount of any payment received by the Federal Government pursuant to a requirement imposed under paragraph (1) may be credited to the appropriate account for research and development or procurement. Amounts so credited shall be merged with other funds in the account and shall be available for the same purposes and the same period for which other funds in such account are available.

“(f) EDUCATION.—The Director of National Intelligence and the heads of the elements of the intelligence community shall ensure that management, technical, and contracting personnel of the elements of the intelligence community who are involved in the award or administration of transactions under subsection (c) or (d), or alternative acquisition pathways, are afforded opportunities for adequate education and training relating to such award or administration.

“(g) AGREEMENTS OFFICERS.—To ensure adequate availability of staff warranted as Agreements Officers, by not later than October 1, 2024, at least 50 percent of the contracting staff within the intelligence community that hold at least some responsibility for buying technology shall have received the appropriate training to become warranted as Agreements Officers, who are given author-
ity to execute and administer the agreements, grants, and transactions authorized by this section.

“(h) DELEGATION REQUIRED.—The Director of National Intelligence and the heads of the elements of the intelligence community shall, to the maximum extent practicable, delegate the authority to make a determination or decision referred to in this section to the official responsible for technology adoption in the relevant element of the intelligence community, regardless of whether such official serves in an acquisition position.

“(i) DEFINITIONS.—In this section:

“(1) COMMERCIAL PRODUCT.—The term ‘commercial product’ has the meaning given that term in section 103 of title 41, United States Code.

“(2) COMMERCIAL SERVICE.—The term ‘commercial service’ has the meaning given that term in section 103a of title 41, United States Code.

“(3) COVERED CONTRACTOR.—The term ‘covered contractor’ means a contractor of an element of the intelligence community that is a small- or medium-sized emerging technology company.

“(4) EMERGING TECHNOLOGY COMPANY.—The term ‘emerging technology company’ means a company that is in the business of maturing and selling technology that is in a developmental stage, or that
may be developed during the 10-year period begin-
ning on January 1, 2022, including with respect to
biotechnology, quantum information science, future
generation wireless technology, advanced materials,
artificial intelligence, nanotechnology, microelec-
tronics, space technology, renewable energy genera-
tion and storage, advanced computing, and human-
machine interfaces.

“(5) Production Product.—The term ‘pro-
duction product’ means any commercial product that
is not a prototype or development product and is in-
tended to provide capability to the United States
Government at scale as determined by the author-
izing official of the relevant element of the intel-
ligence community.

“(6) Production Service.—The term ‘pro-
duction service’ means any commercial service that
is not a prototype or development service and is in-
tended to provide capability to the United States
Government at scale as determined by the author-
izing official of the relevant element of the intel-
ligence community.

“(7) Small- or Medium-Sized Emerging
Technology Company.—The term ‘small- or me-
dium-sized emerging technology company’ means an
emerging technology company with fewer than 1,000 employees.”.

(b) GUIDANCE.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall issue guidance for carrying out the amendments made by subsection (a).

SEC. 512. OFFICES OF COMMERCIAL INTEGRATION.

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

(1) Congress is concerned that the administrative and technical burdens on small- and medium-sized emerging technology companies to do business with the intelligence community is inadvertently precluding the most cutting-edge, advanced companies from contracting with the United States Government;

(2) this dynamic has significant negative consequences for United States national security, including United States global technological competitiveness in the fields of artificial intelligence, quantum computing, and advanced manufacturing, among others;

(3) some such companies have attempted still to contract with the intelligence community by spending valuable capital and time on government affairs
experts to navigate the challenges of integrating into the intelligence community, yet, the administrative and technical burdens of contracting with the intelligence community are often too high even for the companies that are able to afford this consulting;

(4) Congress believes that the United States Government has both an obligation and an opportunity to assist these technology companies navigate the hurdles it takes to work with the intelligence community to ensure that the Federal Government benefits from the best that the private sector has to offer; and

(5) doing so will help cultivate an ecosystem of cutting-edge technology companies that can provide products and services that are essential to the missions of the intelligence community, and advance the goal of ensuring United States adversaries do not outpace the United States in these critical fields.

(b) PLAN FOR ESTABLISHMENT.—

(1) SUBMISSION.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the heads of the elements of the intelligence community, shall submit to the congressional intelligence committees a plan for the establishment of an office
within each element, to be known as the “Office of Commercial Integration” of that element, for the purpose of providing administrative assistance to covered contractors.

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

(A) A proposal for the designation of a senior official of the Office of the Director of National Intelligence who shall be responsible for the coordination across the Offices of Commercial Integration.

(B) Guidelines requiring each Director of Commercial Integration to share best practices and other information, and coordinate, with the other Directors of Commercial Integration.

(C) A timeline of the steps necessary to establish each Office of Commercial Integration by the date that is not later than 2 years after the date of the enactment of this Act.

(D) An assessment of the personnel requirements, and any other resource requirements, necessary to establish each Office of Commercial Integration by such date, including an identification of—
(i) each Director of Commercial Integration;

(ii) the amount of personnel necessary for the establishment of each Office of Commercial Integration; and

(iii) the necessary qualifications of any such personnel.

(E) Policies regarding the types of administrative assistance that may be provided to covered contractors by each Office of Commercial Integration, taking into account the role of such assistance as an incentive for emerging technology companies to enter into contracts with the heads of the elements of the intelligence community. In developing such policies, the Director of National Intelligence shall prioritize assistance to reduce administrative burdens faced by preferred contractors.

(F) Eligibility criteria for determining the types of covered contractors that may receive administrative assistance provided by each Office of Commercial Integration.

(G) Guidelines that outline, with respect to a contract, at what stage covered contractors determined eligible pursuant to the criteria
specified in subparagraph (F) may receive such administrative assistance.

(H) Policies regarding outreach efforts to be conducted by each Director of Commercial Integration with respect to such eligible covered contractors.

(I) Policies regarding how the intelligence community will coordinate with the Director of the Federal Bureau of Investigation to provide proactive counterintelligence risk analysis and assistance to private entities.

(J) Such other intelligence community-wide policies as the Director of National Intelligence may prescribe relating to the improvement of commercial integration (and the coordination of such improvements) by and among the elements of the intelligence community.

(c) **Deadline for Establishment.**—Not later than 2 years after the date of the enactment of this Act, each head of an element of the intelligence community shall establish within that element, in accordance with the plan under subsection (b), an Office of Commercial Integration of that element.

(d) **Staff; Detaillees.**—
(1) **STAFF.**—Each Director of Commercial Integration may appoint personnel as the Director determines appropriate.

(2) **DETAILEES.**—Upon request of a Director of Commercial Integration, the head of any Federal department of agency may detail, on a reimbursable basis, any of the personnel of such department or agency to the Office of Commercial Integration concerned.

(3) **EXPERTISE.**—In appointing personnel under paragraph (1) and accepting detailed personnel pursuant to paragraph (2), each Director of Commercial Integration shall seek to appoint and accept personnel with expertise in a range of disciplines necessary for the accelerated integration of commercial technologies into the intelligence community (as determined by the Director), including expertise in the administrative burdens associated with the following:

(A) Authorization to operate certifications.

(B) Contracting.

(C) Facility clearances.

(D) Security clearances.

(c) **REPORTS REQUIRED.**—
(1) REPORTS.—Not later than 2 years after the date of the enactment of this Act, and annually thereafter for 3 years, each Director of Commercial Integration shall submit to the congressional intelligence committees a report on the status of the Office of Commercial Integration concerned, including the following, with respect to the year covered by the report:

(A) A description of the assistance offered by the Director.

(B) A description of the methods by which the Director advertised such assistance.

(C) Any updates to the policies of such Office.

(D) Statistics on the types of covered contractors that received administrative assistance provided by such Office, and the extent of the use of the assistance by such covered contractors.

(E) A summary of any successes relating to administrative assistance provided by such Office.

(F) Recommendations on how to improve the efficiency or effectiveness of such Office.
(G) An identification of any additional resources or authorities necessary for such Office to fulfill the duties of the Office.

(2) COORDINATION.—In carrying out paragraph (1), each Director of Commercial Integration shall coordinate with the senior official designated pursuant to subsection (b)(2)(A).

(f) DEFINITIONS.—In this section:

(1) COVERED CONTRACTOR.—The term “covered contractor” has the meaning given that term in section 514(c).

(2) DIRECTOR OF COMMERCIAL INTEGRATION.—The term “Director of Commercial Integration” means the head of an Office of Commercial Integration.

(3) OFFICE OF COMMERCIAL INTEGRATION CONCERNED.—The term “Office of Commercial Integration concerned”, with respect to a Director of Commercial Integration, means the Office of Commercial Integration of which that Director is head.

(4) PREFERRED CONTRACTOR.—The term “preferred contractor” means a contractor described in section 514(c)(4).
SEC. 513. PILOT PROGRAM FOR DESIGNATION OF CERTAIN SBIR AND STTR PROJECTS AS ENTREPRENEURIAL INNOVATION PROJECTS.

(a) Pilot Program.—The Director of National Intelligence shall carry out a pilot program to more effectively transition eligible projects that present the potential to meet the operational needs of covered elements of the intelligence community to Phase III through the designation of eligible projects as Entrepreneurial Innovation Projects.

(b) Designation.—

(1) In General.—Under the pilot program under subsection (a), each head of a covered element of the intelligence community, in consultation with the Director of National Intelligence, shall designate not fewer than 5 eligible projects per year as Entrepreneurial Innovation Projects.

(2) Required Criteria.—The head of a covered element of the intelligence community may designate an eligible project as an Entrepreneurial Innovation Project under paragraph (1) if the head determines the eligible project meets the following criteria:

(A) The eligible project demonstrates the potential to—
(i) advance the national security capabilities of the United States;

(ii) provide new technologies or processes, or new applications of existing technologies, that will enable new alternatives to existing programs, systems, and initiatives of the intelligence community;

(iii) provide future cost savings; or

(iv) significantly reduce the time to deliver capabilities to the intelligence community.

(B) Any other criteria that the head determines appropriate.

(3) MITIGATION OF CONFLICTS OF INTEREST.—Each head of a covered element of the intelligence community, in consultation with the Director of National Intelligence, shall establish procedures designed to mitigate, to the greatest extent practicable, organizational conflicts of interest relating to the designation of projects under paragraph (1), including conflicts of interest from within a department or agency of the United States Government for which the designation and successful completion of an Entrepreneurial Innovation Project may represent a competing alternative to an existing or pro-
posed program or other activity of such department or agency.

(4) APPLICATIONS.—An eligible project seeking a designation under paragraph (1) shall submit to the head of the covered element of the intelligence community from which such designation is sought an application containing—

(A) an explanation as to how the eligible project meets the criteria specified in paragraph (2); and

(B) such other information as the head, in consultation with the Director of National Intelligence, considers appropriate.

(5) REVOCATION OF DESIGNATION.—If the head of a covered element of the intelligence community that previously designated a project under paragraph (1) determines such project no longer meets the required criteria specified in paragraph (2), or that the technology that is the subject of such project has become irrelevant, such head may revoke the Entrepreneurial Innovation Project designation for such project.

(e) BENEFITS OF DESIGNATION.—

(1) INCLUSION IN MULTIYEAR NATIONAL INTELLIGENCE PROGRAM PLAN.—The Director of Na-
tional Intelligence shall include in the relevant
multiyear national intelligence program plan sub-
mitted to Congress under section 1403 of the Na-
tional Defense Authorization Act for Fiscal Year
1991 (50 U.S.C. 3301) the estimated expenditures
of each designated project.

(2) INCLUSION UNDER SEPARATE HEADING.—
The designating head shall ensure that each des-
ignated project is included under a separate heading
in the relevant multiyear national intelligence pro-
gram plan submitted to Congress under such section
1403 of the National Defense Authorization Act for

(3) CONSIDERATION IN PROGRAMMING AND
BUDGETING.—Each designated project shall be
taken into consideration by the designating head in
the programming and budgeting phases of the intel-
ligence planning, programming, budgeting, and eval-
uation process.

(d) REPORTS TO CONGRESS.—

(1) ANNUAL REPORTS.—On an annual basis for
each fiscal year during which the pilot program
under subsection (a) is carried out, concurrently
with the submission of the budget of the President
for that fiscal year under section 1105(a) of title 31,
United States Code, the Director of National Intelligence shall submit to the appropriate congressional committees a report that includes the following:

(A) A description of each designated project.

(B) A summary of the potential of each designated project, as specified in subsection (b)(2)(A).

(C) For each designated project, a description of the progress made toward delivering on such potential.

(D) A description of the progress made toward inclusion of the designated project in the future-years intelligence program.

(E) Such other information on the status of such pilot program as the Director considers appropriate.

(2) Final report.—In the final report submitted under paragraph (1) prior to the date of termination under subsection (e), the Director of National Intelligence shall include a recommendation on whether to extend the pilot program under subsection (a) and the appropriate duration of such extension, if any.
(e) **Termination Date.**—The authority to carry out the pilot program under subsection (a) shall terminate on December 31, 2027.

(f) **Definitions.**—In this section:

1. **Appropriate Congressional Committees.**—The term “appropriate congressional committees” means—
   - (A) the congressional intelligence committees;
   - (B) the Committee on Small Business of the House of Representatives; and
   - (C) the Committee on Small Business and Entrepreneurship of the Senate.

2. **Covered Element of the Intelligence Community.**—The term “covered element of the intelligence community” means the following:
   - (A) The Office of the Director of National Intelligence.
   - (B) The Central Intelligence Agency.
   - (C) The National Security Agency.
   - (D) The National Geospatial-Intelligence Agency.
   - (E) The National Reconnaissance Office.

3. **Designated Project.**—The term “designated project” means a project that has been des-
designated as an Entrepreneurial Innovation Project under the pilot program under subsection (a) and for which such designation has not been revoked under subsection (b)(5).

(4) DESIGNATING HEAD.—The term “designating head” means, with respect to the designation of a project as an Entrepreneurial Innovation Project under the pilot program under subsection (a), the head of the covered element of the intelligence community making such designation.

(5) ELIGIBLE PROJECT.—The term “eligible project” means a project for which a small business concern has completed a Phase II SBIR or STTR award.

(6) PHASE II; PHASE III; SBIR; STTR.—The terms “Phase II”, “Phase III”, “SBIR”, and “STTR” have the meanings given such terms in section 9(e) of the Small Business Act (15 U.S.C. 638(e)).

(7) SMALL BUSINESS CONCERN.—The term “small business concern” has the meaning given such term under section 3 of the Small Business Act (15 U.S.C. 632).
SEC. 514. REDUCTION OF BARRIERS RELATING TO CONTRACTS FOR ARTIFICIAL INTELLIGENCE AND OTHER EMERGING TECHNOLOGIES.

(a) FINDINGS; SENSE OF CONGRESS.—

(1) FINDINGS.—Congress finds the following:

(A) Authorizations to operate are essential to maintaining network and system security.

(B) However, Congress is concerned that the executive branch does not have a user-friendly platform or process to adjudicate and review authority to operate applications.

(C) Nor is the executive branch resourced to meet the demand for authority to operate certifications from commercial vendors, leading to lengthy delays to bring commercial solutions into government networks and systems.

(D) These barriers handicap the executive branch when contracting for cutting-edge technologies.

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

(A) the intelligence community and the Secretary of Defense should develop a resourcing plan to address these issues, including developing common platforms for applications and requirements to be shared with indus-
148

try, and a process for authority to operate cer-
tification reciprocity across the Department of
Defense and the intelligence community, with
the appropriate safeguards;

(B) easing these administrative costs and
burdens helps cultivate an ecosystem that
incentivizes small- and medium-sized emerging
technology companies to work with the Federal
Government, which is essential for the United
States to compete globally for technology su-
premacy;

(C) sensitive compartmented information
facilities are often requirements for companies
that wish to conduct business with the intel-
ligence community;

(D) unfortunately, the process to accredit
and certify a facility as a sensitive compart-
mented information facility is time consuming
and expensive, which further raises the barriers
to entry for small- and medium-sized emerging
technology companies; and

(E) lowering those barriers is an important
function of the intelligence community to gain
access to the cutting-edge technology offered by
such companies.
(b) Protocol on Authority to Operate Certifications.—

(1) Protocol.—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 Defense, shall develop and submit to the appropriate congressional committees a protocol setting forth policies and procedures relating to authority to operate certifications held by commercial providers.

(2) Elements.—The protocol under paragraph (1) shall include, at a minimum, the following:

(A) A policy that ensures reciprocal recognition among the elements of the intelligence community and the Department of Defense of authority to operate certifications held by commercial providers. Such reciprocal recognition shall be limited to authority to operate certifications for systems that store or provide access to data classified at an equal or higher classification level.

(B) Procedures under which a commercial provider that is a contractor of an element of the intelligence community or the Department of Defense and holds an authority to operate
certification for a system that relates to the contract concerned may provide to head of such element or the Secretary of Defense, as the case may be, the most recently updated version of any software, data, or application under such system without being required to submit an application for a new or renewed authority to operate certification.

(C) Procedures for the automated review, renewal, and revocation of authority to operate certifications held by commercial providers, subject to such conditions as may be prescribed by the Director of National Intelligence, in coordination with the Secretary of Defense.

(D) Standard documentation requirements for commercial providers submitting applications for authority to operate certifications. Such requirements shall be—

(i) established jointly by the Director of National Intelligence and the Secretary of Defense; and

(ii) except as provided in paragraph (3), uniform across the Department of Defense and the elements of the intelligence
community for each appropriate level of security.

(E) A requirement to establish a joint portal of the Office of the Director of National Intelligence and the Department of Defense for the maintenance of records, applications, and system requirements for authority to operate certifications. Such portal shall be designed to store unclassified information, but may provide for the storage of classified information to the extent determined necessary by the Director of National Intelligence and the Secretary of Defense.

(F) A workforce plan that addresses the shortage of personnel of the intelligence community who are authorized to grant an authority to operate certification, including recommendations by the Director of National Intelligence for increased pay and other incentives to recruit and retain such personnel.

(G) Policies and procedures to ensure coordination across the elements of the intelligence community with respect to the protocol under paragraph (1), including a requirement for—
(i) the Director of National Intelligence to designate an official to lead such coordination across the intelligence community; and

(ii) the head of each element of the intelligence community to designate an official of the element to oversee the implementation of such protocol with respect to the element.

(H) Procedures to ensure data security and safety with respect to the implementation of the protocol under paragraph (1).

(I) A proposed timeline for the implementation of the protocol under paragraph (1) by the deadline specified in such paragraph.

(3) EXCEPTION TO STANDARD DOCUMENTATION REQUIREMENTS.—The Director of National Intelligence and the Secretary of Defense may jointly establish nonuniform documentation requirements for commercial providers submitting applications for authority to operate certifications, in addition to the requirements specified in paragraph (2)(D), only if, prior to such establishment, the Director and Secretary provide to the appropriate congressional com-
mittees a briefing on why such additional requirements are necessary.

(4) DEFINITIONS.—In this subsection:

(A) The term “appropriate congressional committees” means—

(i) the congressional intelligence committees; and

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

(B) The term “authority to operate certification” means, with respect to a system, a formal designation by a designated approving authority that authorizes the operation of the system by a Federal department or agency and includes an acknowledgment that the Federal department or agency accepts the risk of such operation.

(C) The term “contract concerned”, with respect to a contractor of an element of the intelligence community or the Department of Defense, means the contract entered into by that contractor with the head of the element or the Secretary of Defense, as the case may be.
(c) Plan to Expand Sensitive Compartmented Information Facility Access by Certain Contractors.—

(1) Plan; briefing.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of such other elements of the intelligence community as the Director of National Intelligence may determine appropriate, shall jointly—

(A) develop a plan to expand access by covered contractors to sensitive compartmented information facilities for the purpose of providing covered contractors with a facility to securely perform work under covered contracts; and

(B) provide to the appropriate congressional committees a briefing on such plan.

(2) Matters.—The plan under paragraph (1) shall include the following:

(A) An overview of the existing sensitive compartmented information facilities, if any, that may be repurposed for the purpose specified in paragraph (1).
(B) An assessment of the feasibility of building additional sensitive compartmented information facilities for such purpose.

(C) An assessment of the relative costs and benefits of repurposing existing, or building additional, sensitive compartmented information facilities for such purpose.

(D) The eligibility criteria for determining which covered contractors may be granted access to sensitive compartmented information facilities for such purpose.

(E) An estimate of the maximum number of covered contractors that may be provided access to sensitive compartmented information facilities for such purpose, taking into account the matters specified in subparagraphs (A) and (B).

(F) Policies to ensure the efficient and narrow use of sensitive compartmented information facilities for such purpose, including a timeline for the length of such use by a covered contractor and a detailed description of the process to terminate access to the sensitive compartmented information facility by a covered contractor upon—
(i) the expiration of the covered contract of the covered contractor; or

(ii) a determination that the covered contractor no longer has a need for such access to fulfill the terms of such contract.

(G) Pricing structures for the use of sensitive compartmented information facilities by covered contractors for the purpose specified in paragraph (1). Such pricing structures—

(i) may include free use (for the purpose of incentivizing future covered contracts), with the potential for pricing to increase dependent on the length of the covered contract, the size of the covered contractor, and the need for such use; and

(ii) shall ensure that the cumulative cost for a covered contractor to rent and independently certify a sensitive compartmented information facility for such purpose does not exceed the market average for the Director of National Intelligence or the Secretary of Defense to build, certify, and maintain a sensitive compartmented information facility.
(H) A security plan for vetting each covered contractor prior to the access of a sensitive compartmented information facility by the covered contractor for the purpose specified in paragraph (1), and an assessment of potential security concerns regarding such access.

(I) A proposed timeline for the expansion of access to sensitive compartmented information facilities in accordance with paragraph (1).

(J) Such other matters as the Director of National Intelligence or the Secretary of Defense considers relevant to such expansion.

(3) Eligibility criteria for covered contractors.—Under the eligibility criteria specified in subparagraph (D)—

(A) unless the Director of National Intelligence determines the source of the financing of a covered contractor poses a national security risk, such source of financing may not be taken into consideration in making a determination as to the eligibility of the covered contractor; and

(B) preference shall be given to any preferred contractor described in paragraph (4).
(4) PREFERRED CONTRACTORS.—A preferred contractor described in this paragraph is a covered contractor—

(A) that is a small business concern that has a Phase I or Phase II SBIR award for a project under a covered contract and demonstrates a need for access to a sensitive compartmented information facility with respect to such ongoing project; or

(B) the covered contract of which is a contract entered into with the Director of AFWERX of the Air Force (or such successor program), the Director of the Defense Innovation Unit of the Department of Defense, or the head of any other program or element of the Federal Government with a focus on technology or innovation.

(5) DEFINITIONS.—In this subsection:

(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means—

(i) the congressional intelligence committees; and
(ii) the Committees on Armed Services of the House of Representatives and the Senate.

(B) COVERED CONTRACT.—The term “covered contract” means a contract entered into by a covered contractor with the head of an element of the intelligence community or the Secretary of Defense that relates to the development of technology solutions for the intelligence community or the Department of Defense, as the case may be.

(C) COVERED CONTRACTOR.—The term “covered contractor” means a contractor of the intelligence community or the Department of Defense that the Director of National Intelligence determines is a small- or medium-sized technology company in an early stage of developing technology solutions pursuant to a covered contract.

(D) PHASE I; PHASE II; SBIR.—The terms “Phase I”, “Phase II”, and “SBIR” have the meanings given those terms in section 9(e) of the Small Business Act (15 U.S.C. 638(e)).

(E) SMALL BUSINESS CONCERN.—The term “small business concern” has the meaning

(d) REPORTS ON EXPANSION OF SECURITY CLEARANCES FOR CERTAIN CONTRACTORS.—

(1) REPORTS.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter for 3 years, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the extent to which security clearance requirements delay, limit, or otherwise disincentivize emerging technology companies from entering into contracts with the United States Government.

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

(A) Statistics on the periods of time between the submission of applications for security clearances by employees of emerging technology companies and the grant of such security clearances, disaggregated by the size of the respective company.

(B) The number of security clearances granted to employees of small- or medium-sized emerging technology companies during the period covered by the report.
(C) The number of applications for security clearances submitted by employees of emerging technology companies that have yet to be adjudicated as of the date on which the report is submitted.

(D) A projection, for the year following the date on which the report is submitted, of the number of security clearances necessary for employees of emerging technology companies to perform work on behalf of the intelligence community during such year, and an assessment of the capacity of the intelligence community to meet such demand.

(E) An identification of each occurrence, during the period covered by the report, in which an emerging technology company withdrew from or declined to accept a contract with the United States Government on the sole basis of delays, limitations, or other issues involving security clearances, and a description of the types of business the United States Government has lost as a result of such occurrences.

(F) Recommendations for expediting the grant of security clearances to employees of emerging technology companies, including with
162

respect to any additional resources, authorities,
or personnel that the Director of National In-
telligence determines may be necessary for such
expedition.

(3) FORM.—Each report under paragraph (1)
may be submitted in classified form, but if so sub-
mitted shall include an unclassified executive sum-
mary.

(4) PROPOSAL CONCURRENT WITH BUDGET
SUBMISSION.—At the time that the President sub-
mits to Congress the budget for fiscal year 2024
pursuant to section 1105 of title 31, United States
Code, the Director of National Intelligence shall sub-
mit to the congressional intelligence committees a
proposal to improve the capacity of the workforce re-
sponsible for the investigation and adjudication of
security clearances, with the goal of reducing the pe-
riod of time specified in paragraph (2)(A) to less
than 60 days. Such proposal shall include an identi-
fication of any resources the Director determines
necessary to expand the number of individuals au-
thorized to conduct polygraphs on behalf of the in-
telligence community, including by furnishing nec-
essary training to such individuals.
SEC. 515. COMPLIANCE BY THE INTELLIGENCE COMMUNITY WITH REQUIREMENTS OF THE FEDERAL ACQUISITION REGULATION RELATING TO COMMERCIALLY AVAILABLE OFF-THE-SHELF ITEMS AND COMMERCIAL SERVICES.

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

(1) parts 10 and 12 of the Federal Acquisition Regulation broadly require departments and agencies of the United States Government to conduct market research to determine whether commercially available off-the-shelf items, nondevelopmental items, or commercial services are available that could meet the requirements of the department or agency;

(2) the requirements under such parts 10 and 12, among other important goals, reduce administrative costs and allow expedited acquisition and deployment of such items and services;

(3) however, such departments and agencies too often contract for custom products, rather than buying existing commercial products and adapting those as necessary, which creates a fundamental compliance issue; and

(4) the intelligence community should adopt a culture shift to ensure better compliance with such parts 10 and 12.
(b) POLICY.—

(1) REQUIREMENT.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence shall implement a policy to ensure that each element of the intelligence community complies with parts 10 and 12 of the Federal Acquisition Regulation with respect to any procurement.

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

(A) Written criteria for an element of the intelligence community to evaluate when a procurement of a covered item or service is permissible, including—

(i) requiring the element to conduct an independent market analysis to determine whether a commercially available off-the-shelf item, nondevelopmental item, or commercial service is viable; and

(ii) a description of the offeror for such covered item or service and how the covered item or service to be acquired will be integrated into existing systems of the intelligence community.
(B) If an element of the intelligence community enters into a contract for artificial intelligence or other emerging technologies that is a covered item or service, not later than 45 days before entering into such contract, the head of the element shall notify the congressional intelligence committees in writing of the intent to enter into such contract, including a brief summary of—

(i) the justification for not using a commercially available off-the-shelf item, nondevelopmental item, or commercial service; and

(ii) the independent market analysis conducted under subparagraph (A).

(C) A detailed set of performance incentives for the acquisition personnel of the intelligence community that—

(i) prioritizes and rewards adherence to parts 10 and 12 of the Federal Acquisition Regulation; and

(ii) incentivizes reliance by the intelligence community on commercially available off-the-shelf items, nondevelopmental items, or commercial services and
incentivizes such personnel that enter into contracts for covered items or services only when necessary.

(D) Methods to ensure the coordination across the elements of the intelligence community in carrying out the policy, including by designating an official of each element to ensure implementation and incentives for elements to share best practices for entering into contracts for covered items or services.

(E) On an annual basis, the head of each element of the intelligence community shall certify in writing to the congressional intelligence committees that each contract involving software development that was awarded during the year covered by the certification was awarded in adherence to section 3453 of title 10, United States Code, and such parts 10 and 12, as applicable.

(F) Any other incentives for the acquisition personnel of the intelligence community that the Director determines appropriate to improve the use of commercially available off-the-shelf items, nondevelopmental items, and commercial services in contracts for emerging tech-
nologies, including with respect to pay incentives, time off for training, and nonmonetary awards.

(3) SUBMISSION.—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) the policy developed under paragraph (1); and

(B) a plan to implement the policy not later than 1 year after the date of such enactment.

(4) MARKET ANALYSIS.—In carrying out the independent market analysis pursuant to paragraph (1)(A)(ii), the Director may enter into a contract with an independent market research group with qualifications and expertise to find available commercially available off-the-shelf items, nondevelopmental items, or commercial services to meet the needs of the intelligence community.

(c) ANNUAL REPORTS.—

(1) REQUIREMENT.—Not later than 2 years after the date of the enactment of this Act, and annually thereafter for 3 years, the Director, in consultation with the head of each element of the intel-
intelligence community, shall submit to the congressional intelligence committees a report on the policy developed under subsection (a).

(2) ELEMENTS.—Each report under paragraph (1) shall include, with respect to the period covered by the report, the following:

(A) An evaluation of the success of the policy, including with respect to the progress the elements have made in complying with parts 10 and 12 of the Federal Acquisition Regulation.

(B) A comparison of the number of contracts that were awarded for commercially available off-the-shelf items, nondevelopmental items, or commercial services versus the number awarded for covered items or services.

(C) A description of how any market analyses are conducted pursuant to subsection (a)(1)(A)(ii).

(D) Any recommendations to improve compliance with such parts 10 and 12.

(d) DEFINITIONS.—In this section:

(1) COMMERCIALY AVAILABLE OFF-THE-SHELF ITEM; COMMERCIAL SERVICE; NONDEVELOPMENTAL ITEM.—The terms “commercially available off-the-shelf item”, “commercial service”, and “non-
developmental items” have the meanings given, respect- 
ively, in subchapter I of division A of title 41, United States Code.

(2) COVERED ITEM OR SERVICE.—The term “covered item or service” means a product, system, or service that is not a commercially available off-the-shelf item, a commercial service, or a non-developmental item.

SEC. 516. POLICY ON REQUIRED USER ADOPTION METRICS IN CERTAIN CONTRACTS FOR ARTIFICIAL INTELLIGENCE SOFTWARE PRODUCTS.

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

(1) it is critical that the intelligence community acquire products that can be integrated, to the highest extent possible, within existing workflows and personnel capabilities;

(2) one step toward that goal is ensuring that products procured by the intelligence community have user-adoption metrics, which allow programmers and vendors to assess the effectiveness of a given product to an intelligence community user;

(3) requiring such metrics also incentivizes vendors to incorporate training and adoption programs into their products, as opposed to contracts which
simply sell an application to the intelligence community with no customer success feature built in; and

(4) in addition, this data is critical to informing decisions about the continued use of a product, including relating to whether a prototype will transition from development to an enterprise-wide contract or program of record.

(b) POLICY.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall establish a policy containing the following:

(1) With respect to a contract or other agreement entered into between the head of an element of the intelligence community and a commercial provider for the acquisition of a covered product for users within the intelligence community—

(A) a requirement that each such contract or other agreement include, as a term of the contract or agreement, a commitment by the commercial provider to furnish a means of collecting user adoption metrics for assessing the adoption of the covered product by such users; and

(B) a requirement that the head assess the user adoption of the covered product through such means.
(2) Such exceptions to the requirements under paragraph (1) as may be determined appropriate by the Director.

(c) REPORTS.—

(1) SUBMISSION.—Not later than 1 year after the date on which the Director of National Intelligence establishes the policy under subsection (b), and annually thereafter for 3 years, the Director, in coordination with the heads of the elements of the intelligence community, shall submit to the congressional intelligence committees a report on the user adoption metrics for each covered product acquired using, in whole or in part, funds made available under the National Intelligence Program.

(2) MATTERS.—Each report under paragraph (1) shall include, with respect to the year covered by the report, the following:

(A) A detailed description of the effectiveness of the policy under subsection (b), including a cost-benefit analysis of such policy.

(B) A summary of the user adoption metrics collected pursuant to such policy for each program referred to in paragraph (1).

(C) An identification of any instance in which the head of an element of the intelligence community...
community determined that requiring a commitment to furnish a means of collecting user adoption metrics as a term of a contract or agreement pursuant to such policy was not practicable pursuant to an exception specified in subsection (b)(2) and, as a result, did not require such commitment.

(D) A justification for the continuation of the use of any covered product acquired by the head of an element of the intelligence community that the head has determined, pursuant to an assessment required under subsection (b)(1)(B), was not sufficiently adopted by users or otherwise received negative user feedback.

(E) Any other matters, including any relevant recommendations, determined appropriate by the Director.

(3) Timing.—Each report under paragraph (1) shall be submitted prior to the date of the presentation of the consolidated National Intelligence Program budget for the year covered by the report to the President for approval pursuant to section 102A(e) of the National Security Act of 1947 (50 U.S.C. 3024).

(d) Definitions.—In this section:
(1) COVERED PRODUCT.—The term “covered product” means a commercial software product that involves artificial intelligence.

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

SEC. 517. ASSESSMENTS RELATING TO INFORMATION TECHNOLOGY AND SOFTWARE SYSTEMS.

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

(1) the intelligence community continues to rely heavily on legacy information technology systems and software;

(2) transitioning these systems as appropriate to modern software as a service, cloud-based, and open-source systems is a priority;

(3) in many instances, there are no incentives to make such a transition due to the cost, complexity, administrative hurdles, and user adoption challenges with any such transition; and

(4) therefore, it is imperative for the intelligence community to create incentives to ensure that its systems evolve with industry and remain
competitive with foreign adversaries of the United States.

(b) Assessments Required.—

(1) Intelligence community-wide baseline assessment.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community, shall complete an assessment of the information technology and software systems of each element of the intelligence community, to review whether such systems integrate new and emerging technology and, as appropriate, make recommendations to decommission or replace outdated systems. Such assessment shall include, with respect to each such system, an evaluation of the following:

(A) The usability of the system.

(B) Whether the system is the most up-to-date version of the system available.

(C) The compatibility of the system with new and emerging technology.

(D) The costs and benefits of using an alternative system in lieu of the system, including the financial cost of transitioning to such an al-
ternative system and any technical or adminis-
trative barriers to such transition.

(E) Such other matters as may be deter-
dined appropriate by the Director.

(2) ASSESSMENTS UPON ENTRY INTO, RE-
NEWAL, OR EXTENSION OF CERTAIN CONTRACTS.—
Not later than 60 days after the date on which the
head of an element of the intelligence community en-
ters into, renews, or extends a contract for the ac-
quision of an information technology or software
system, the Director of National Intelligence shall
conduct an assessment of such system in accordance
with paragraph (1), including by evaluating each of
the matters specified in subparagraphs (A) through
(E) of such paragraph, with respect to such system.

(e) GUIDANCE.—The Director shall issue to the
heads of the elements of the intelligence community guid-
ance to—

(1) incentivize each such head to adopt and in-
tegrate new and emerging technology within infor-
mation technology and software systems of the ele-
ment and to decommission and replace outdated sys-
tems, including through potential funding enhance-
ments; and
(2) incentivize, and hold accountable, personnel of the intelligence community with respect to the integration of new and emerging technology within such systems, including through the provision of appropriate training programs and evaluations.

(d) SUBMISSIONS TO CONGRESS.—

(1) REPORT ON ASSESSMENT RESULTS.—Not later than 60 days after the date on which the Director completes the assessment under subsection (b)(1), the Director shall submit to the appropriate congressional committees a report containing the results of such assessment.

(2) SUBMISSION OF GUIDANCE.—Not later than 60 days after the date on which the Director issues the guidance under subsection (c), the Director shall submit to the appropriate congressional committees a copy of such guidance.

(e) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term “appropriate congressional committees” means—

(1) the congressional intelligence committees; and

(2) the Committees on Appropriations of the House of Representatives and the Senate.
Subtitle C—Reports

SEC. 521. REPORTS ON INTEGRATION OF ARTIFICIAL INTELLIGENCE WITHIN INTELLIGENCE COMMUNITY.

(a) Sense of Congress.—It is the sense of Congress that—

(1) artificial intelligence and other emerging technologies must be incorporated into the intelligence community at a pace that matches industry and is competitive with United States adversaries;

(2) while collaboration can and does occur in instances, Congress is concerned that the United States is not integrated enough across disciplines to further this essential mission; and

(3) while each intelligence community element is pursuing artificial intelligence adoption by either establishing new offices or surging resources to existing offices, there is not a single office or official at each intelligence community element that has the authority to oversee artificial intelligence adoption at the agency, and can serve as the coordinator for interagency cooperation.

(b) Report by Director of National Intelligence.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intel—
ligence, in coordination with the heads of the elements of
the intelligence community, shall submit to the congres-
sional intelligence committees a report on the efforts of
the intelligence community to develop, acquire, adopt, and
maintain artificial intelligence across the intelligence com-
munity to improve intelligence collection across the collect-
tion spectrum and optimize internal work flows. Such re-
port shall contain a separate review of each such element
that includes, with respect to the element, the following:

(1) A description of the authorities of the ele-
ment relating to the use of artificial intelligence, and
whether the element lacks any resources or authori-
ties necessary to accelerate the adoption by the ele-
ment of artificial intelligence solutions, including
commercial products involving artificial intelligence.

(2) A description of the organizational roles, re-
sponsibilities, and authorities for any senior officials
of the element charged with accelerating the adopt-
ion by the element of artificial intelligence solutions,
and whether the head of the element lacks any re-
sources or authorities to hire the personnel neces-

(3) An identification of the senior official of the
element responsible for overseeing and coordinating
efforts relating to artificial intelligence across the in-

intelligence community, including through the integration of the acquisition, technology, human capital, and financial management aspects necessary for the adoption of artificial intelligence solutions.

(4) An assessment, conducted by the Inspector General of the Intelligence Community, of the efforts of the head of the element to acquire and adopt commercial products involving artificial intelligence and in particular, the efforts of such head to acquire and adopt such products in a timely manner.

(5) An assessment, conducted by the Inspector General of the Intelligence Community, of any administrative or technical barriers to the accelerated adoption of artificial intelligence by the element, including any such barriers to the efforts specified in paragraph (4). Such assessment shall be disaggregated by, and include input from, organizational units of the element that focus on the following:

(A) Acquisitions and contracting.

(B) Personnel and workforce matters.

(C) Financial management and budgeting.

(D) Operations and capabilities.

(6) An assessment, conducted by the Inspector General of the Intelligence Community, of the efforts
of the head of the element to coordinate across the intelligence community for the purpose of ensuring the adoption of best practices, sharing of information, and efficient use of resources relating to artificial intelligence, including an identification by such head of any administrative or technical barriers to such coordination, and recommendations for improving such coordination. With respect to the review of the Office of the Director of National Intelligence, such assessment shall also include a specific assessment of how the Director of National Intelligence, in consultation with the Director of Science and Technology and the Chief Data Officer, oversees, or plans to oversee, such coordination.

(c) Annual Reports by Director of Science and Technology.—

(1) Reports.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter for 3 years, the Director of Science and Technology, in coordination with the Chief Data Officer with respect to the matters specified in paragraph (3), and in consultation with the Director of National Intelligence and the heads of the elements of the intelligence community, shall submit to the congressional intelligence committees a report on the
progress of the adoption of artificial intelligence
within the intelligence community.

(2) MATTERS.—Each report under paragraph (1) shall include, with respect to the year covered by the report, the following:

(A) A detailed description of the progress of each element of the intelligence community in the adoption and maintenance of artificial intelligence during such year, including a description of any—

(i) artificial intelligence programs or systems adopted or decommissioned by the element;

(ii) contracts entered into by the head of the element with small- or medium-sized emerging technology companies for commercial products involving artificial intelligence;

(iii) efforts carried out by the head of the element for coordination across the intelligence community on artificial intelligence-related matters; and

(iv) relevant positions established or filled within the element.
(B) A description of any policies of the intelligence community issued during such year that relate to the adoption of artificial intelligence within the intelligence community, including an assessment of the compliance with such policies by the elements of the intelligence community.

(C) A list of recommendations by the Director of Science and Technology for the efficient, accelerated, and comprehensive adoption of artificial intelligence across the intelligence community during the year following the year covered by the report, including any technological advances in artificial intelligence that the intelligence community should leverage from industry actors.

(D) An overview of the advances of foreign adversaries in the field of artificial intelligence, and steps that may be taken to ensure the United States Government outpaces foreign adversaries in such field.

(E) Any gaps in resource or authorities, or other administrative or technical barriers, to the adoption of artificial intelligence by the intelligence community.
(F) Such other matters as the Director of Science and Technology may determine appropriate.

(3) ENTRY BY CHIEF DATA OFFICER.—Each report under paragraph (1) shall include an entry by the Chief Data Officer that addresses each of the matters specified in paragraph (2) with respect to the organization of data for the accelerated adoption of artificial intelligence solutions.

SEC. 522. REPORT ON POTENTIAL BENEFITS OF ESTABLISHMENT OF ICWERX.

(a) REPORT.—Not later than 180 days after the date of enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees an assessment of whether the intelligence community would benefit from the establishment of an organization to be known as “ICWERX”, the mission and activities of which would incorporate lessons learned from AFWERX of the Air Force (or such successor program), the Defense Innovation Unit of the Department of Defense, and other programs and elements of the Federal Government with a focus on technology or innovation.

(b) ELEMENTS.—The report under subsection (a) shall include the following:
(1) A review of the avenues for small- and medium-sized emerging technology companies to provide to the intelligence community artificial intelligence or other technology solutions, including an identification, for each of the 5 years preceding the year in which the report is submitted, of the annual number of such companies that have provided the intelligence community with such solutions.

(2) A review of the processes by which the heads of the elements of the intelligence community acquire and transition commercial research of small- and medium-sized emerging technology companies in a prototype or other early developmental stage.

(3) An assessment of—

(A) whether the intelligence community is postured to incorporate the technological innovations of emerging technology companies, including in software and hardware; and

(B) any areas in which the intelligence community lacks resources, authorities, personnel, expertise, or institutional mechanisms necessary for such incorporation.

(4) An assessment of the potential costs and benefits associated with the establishment of ICWERX in accordance with subsection (a).
SEC. 523. REQUIREMENTS AND REPORT ON WORKFORCE NEEDS OF INTELLIGENCE COMMUNITY RELATING TO SCIENCE, TECHNOLOGY, ENGINEERING, AND MATH, AND RELATED AREAS.

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

(1) increasing the talent diversity, density, and expertise for critical fields in the intelligence community is essential to accelerating the incorporation, integration, and maintenance of emerging technologies into the workflows and business practices of the intelligence community;

(2) Congress is concerned that the intelligence community has not yet conducted a baseline assessment of what talent currently exists within the intelligence community, and where gaps prevent the intelligence community from meeting the technology demands in the next decade;

(3) Congress is aware that the Director of National Intelligence is starting the process to lead a needs assessment across the intelligence community and encourages all elements of the intelligence community to work expeditiously with the Director to develop that detailed assessment; and

(4) this type of needs assessment should be institutionalized and built into the future human cap-
ital strategy for the next generation of intelligence
officers and officials.

(b) REQUIREMENTS.—The Director of National In-
telligence, in coordination with the Chief Technology Offi-
cer and the Chief Human Capital Officer of the Office
of the Director of National Intelligence, shall—

(1) develop an organizational management plan
for the adoption and maintenance of artificial intel-
ligence across the intelligence community; and

(2) require that each head of an element of the
intelligence community, with respect to such ele-
ment—

(A) develop a plan for the recruitment of
personnel to positions the primary duties of
which involve the integration, maintenance, or
use of artificial intelligence (and the retention
and training of personnel serving in such posi-
tions);

(B) develop a plan for—

(i) the review and evaluation, on a
continuous basis, of the expertise necessary
to accelerate the adoption of artificial intel-
ligence and other emerging technology so-
lutions; and
(ii) the update of efforts to recruit and retain personnel with such expertise; and

(C) coordinate and share information and best practices relating to such recruitment and retention within the element and across the intelligence community.

(c) Report.—

(1) Submission.—Not later than January 1, 2024, the Director of National Intelligence, in coordination with the Chief Technology Officer and the Chief Human Capital Officer of the Office of the Director of National Intelligence, shall submit to the congressional intelligence committees a report on the workforce needs of the intelligence community relating to artificial intelligence, cybersecurity, and other science, technology, engineering, and math areas.

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

(A) A detailed description of the organizational management plan under subsection (b)(1).

(B) With respect to each element of the intelligence community, the following:
(i) A detailed breakdown of the personnel of the element serving in positions the primary duties of which involve the integration, maintenance, or use of artificial intelligence, including (for each such position) the title of the position, the office under which the position is organized, and the approximate percent of time personnel serving in the position spend carrying out such duties under the position, as compared to carrying out other duties under the position.

(ii) A detailed description of the plan of the head of the element under subsection (b)(2)(A), including an identification of any official responsible for coordinating recruitment, retention, and training for the element under such plan.

(iii) A detailed description of the plan of the head of the element under subsection (b)(2)(B).

(iv) A detailed description of the methods by which the head coordinates and shares information and best practices under subsection (b)(2)(C), including an
identification of any official responsible for such coordination and sharing for the element.

(v) Such other matters as the Director of National Intelligence may determine appropriate.

(C) An assessment of any gaps in the organizational management plan specified in subsection (b)(1), including, for each element of the intelligence community, an identification of any additional roles, positions, expertise, or authorities necessary for the adoption and maintenance of artificial intelligence by that element.

(D) An assessment of the quality and sustainability of the talent pipeline of the intelligence community with respect to talent in cybersecurity and other science, technology, engineering, and math areas. Such assessment shall include the following:

(i) An assessment of the priorities of the intelligence community with respect to cybersecurity and other science, technology, engineering, and math areas, and the personnel necessary to address such priorities.
(ii) A summary of the education, recruitment, and retention programs (including skills-based training and career and technical educational programs) available to personnel of the intelligence community, regardless of whether such programs are administered by the head of an element of the intelligence community or the head of another Federal department or agency, and an analysis of how such programs support the quality and sustainability of such talent pipeline.

(iii) A description of the relevant authorities available to the heads of the elements of the intelligence community to support the quality and sustainability of such talent pipeline.

(iv) An assessment of any gaps in authorities, resources, recruitment or retention incentives, skills-based training, or educational programs, that may negatively affect the quality or sustainability of such talent pipeline.

(d) INFORMATION ACCESS.—The heads of the elements of the intelligence community shall furnish to the
Chief Technology Officer and the Chief Human Capital Officer of the Office of the Director of National Intelligence such information as may be necessary for the development of the report under subsection (c).

Subtitle D—Other Matters

Sec. 531. Improvements to Use of Commercial Software Products.

(a) Sense of Congress.—It is the sense of Congress that—

(1) systems integration is a critical part of incorporating emerging technologies into the intelligence community;

(2) unfortunately, Congress understands that there remains an uneven approach across the intelligence community for contracting and executing system integration;

(3) such disparate policies lead to added administrative costs for both the intelligence community and commercial vendors, and inhibit integration and operationalization in a coordinated, efficient way;

(4) further, as a result of a lack of a cohesive policy, some contracts do not always adhere to the best practices of commercial software as a service product, or are executed by legacy contractors who
create added expenses and sustainment costs, among other issues; and

(5) including standardized terms across intelligence community contracts can help reduce administrative and technical barriers to systems integration, make such integration more efficient and effective, and ensure that each contract comports with best practices and standard commercial software as a service feature.

(b) PROCUREMENT OF COMMERCIAL SOFTWARE PRODUCTS.—

(1) POLICY.—Not later than January 1, 2024, the Director of Science and Technology of the Office of the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community, shall recommend to the Director of National Intelligence an intelligence community-wide policy to ensure that the procurement of commercial software products by the intelligence community is carried out in accordance with best practices.

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

(A) Guidelines for the heads of the elements of the intelligence community to deter-
mine which contracts for commercial software
products are covered by the policy, including
with respect to agreements, authorizations to
operate, and other acquisition activities.

(B) Guidelines for using standardized
terms in such contracts, modeled after commer-
cial best practices, including common proce-
dures and language regarding—

(i) terms for who is responsible for
system integration under the contract;

(ii) a timeline required for system in-
tegration;

(iii) a mechanism included in each
contract to ensure the ability of the vendor
to provide continuous updates and version
control for the software;

(iv) a mechanism included in each
contract that allows the United States
Government to receive and use the latest
updates for the software and receive such
updates in near real-time;

(v) automatic technological mecha-
nisms for security and data validation, in-
cluding security protocols that are predi-
cated on commercial best practices; and
(vi) procedures to provide incentives, and a technical framework, for system integration for new commercial software solutions to fit within existing workflows and information technology infrastructure.

(C) Guidelines to ensure coordination of the policy throughout the intelligence community, including identifying the officials in each element of the intelligence who are responsible for enforcing the policy.

(3) REPORT.—Not later than January 1, 2025, and annually thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the policy recommended under paragraph (1), including the following with respect to the period covered by the report:

(A) An evaluation of compliance with such policy by the elements of the intelligence community.

(B) An identification of the elements of such policy that achieve the goal referred to in paragraph (1), and the elements of such policy that fail to achieve such goal, including any concerns with system integration.
(C) Recommendations to better coordinate system integration throughout the intelligence community using best practices.

(D) For each element of the intelligence community—

(i) a description by the head of the element of specific successes and concerns in contracting for, and incorporating, system integration; and

(ii) recommendations to improve the recommended policy.

(c) CODE-FREE ARTIFICIAL INTELLIGENCE ENABLEMENT TOOLS.—

(1) POLICY.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Director of Science and Technology and the heads of the elements of the intelligence community that the Director of National Intelligence determines appropriate, shall implement a policy to promote the intelligence community-wide use of code-free artificial intelligence enablement tools.

(2) ELEMENTS.—The policy under paragraph (1) shall include the following:
(A) A detailed set of incentives for using code-free artificial intelligence enablement tools.

(B) A plan to ensure coordination throughout the intelligence community, including by designating an official of each element of the intelligence community to oversee implementation of the policy and such coordination.

(3) Submission.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees the proposed policy under paragraph (1), including a detailed plan and timeline for carrying out the incentives described in paragraph (2)(A).

(4) Annual Reports or Briefings.—Not later than 1 year after commencing the implementation of the policy under paragraph (1), and annually thereafter for 3 years, the Director of National Intelligence, in consultation with the Director of Science and Technology and the heads of the elements of the intelligence community that the Director of National Intelligence determines appropriate, shall submit to the congressional intelligence committees a report, or provide to such committees a briefing, that—
1. (A) details the success of the policy;
2. (B) includes statistics on the progress of
3. the intelligence community in implementing
4. code-free artificial intelligence enablement tools;
5. and
6. (C) contains any recommendations for im-
7. provements or enhancements to the policy.
8. (d) CODE-FREE ARTIFICIAL INTELLIGENCE
9. ENABLEMENT TOOLS DEFINED.—In this section, the
10. term “code-free artificial intelligence enablement tools”
11. means software that provides an environment where visual
12. drag-and-drop applications or similar tools allow 1 or more
13. individuals to program applications without linear coding.
14. SEC. 532. IMPROVEMENTS TO EMPLOYEES AND MANAGERS
15. RELATING TO EMERGING TECHNOLOGIES,
16. SOFTWARE DEVELOPMENT, ACQUISITION,
17. AND SUSTAINMENT.
18. (a) CADRE OF EXPERTS.—
19. (1) ESTABLISH OF CADRE.—Not later than January 1, 2024, the Director of National Intel-
20. ligence, acting through the Director of Science and Technology, shall establish a cadre of personnel who are experts in emerging technologies, software devel-
21. opment, systems integration, and acquisition, to im-
prove the adoption by the intelligence community of commercial solutions for emerging technologies.

(2) STRUCTURE.—The Director of Science and Technology—

(A) shall ensure the cadre has the appropriate number of members;

(B) shall establish an appropriate leadership structure and office within which the cadre shall be managed; and

(C) shall determine the appropriate officials to whom members of the cadre shall report.

(3) RESPONSIBILITIES.—The cadre of personnel authorized under paragraph (1) shall be responsible for—

(A) assisting the Director of Science and Technology with continuing to develop and evolve intelligence community-wide policies, rules, and procedures to accelerate the adoption of emerging technologies, including with respect to artificial intelligence, machine learning, and software development and systems integration into the intelligence community;
(B) assisting elements of the intelligence community with software development and acquisition;

(C) establishing training requirements for acquisition professionals within the intelligence community to increase the number of acquisition experts, with a particular emphasis on—

(i) the principles contained in the TechFAR Handbook for Procuring Digital Services Using Agile Processes of the U.S. Digital Service; and

(ii) the requirements under parts 10 and 12 of the Federal Acquisition Regulation, in accordance with the protocol of the Director of National Intelligence relating to such parts pursuant to section 515; and

(D) other functions as the Director of Science and Technology determines appropriate based on the evolving needs of identifying, incorporating, and maintaining evolving technology in the intelligence community.

(4) ASSIGNMENT.—The Director of Science and Technology shall establish processes to assign members of the cadre to provide—
(A) expertise on matters relating to software development, integration, acquisition, and sustainment; and

(B) support for appropriate programs or activities of the intelligence community.

(5) ADMINISTRATION.—

(A) IN GENERAL.—The Director of Science and Technology, in coordination with the President of the Defense Acquisition University and in consultation with academia and industry, shall develop a career path, including training, development opportunities, exchanges, and talent management programs, for the cadre. The Director of Science and Technology may use existing personnel and acquisition authorities to establish the cadre, as appropriate, including—

(i) section 9903 of title 5, United States Code;

(ii) authorities relating to services contracting;

(iii) the Intergovernmental Personnel Act of 1970 (42 U.S.C. 4701 et seq.); and

(iv) authorities relating to exchange programs with industry.
(B) ASSIGNMENTS.—Civilian and military personnel from within the intelligence community may be assigned to serve as members of the cadre.

(6) FUNDING.—The Director of Science and Technology may use amounts made available under the National Intelligence Program for the purpose of recruitment, training, and retention of members of the cadre, including by using such amounts to pay salaries of newly hired members of the cadre for up to 3 years.

(7) COORDINATION.—The Director of Science and Technology shall coordinate with the Under Secretary of Defense for Acquisition and Sustainment and the Under Secretary of Defense for Research and Engineering to ensure that the programs, policies, rules, and regulations relating to the cadre of the intelligence community and the cadre of the Department of Defense are consistent and streamlined.

(8) REPORTS.—On an annual basis, the Director of Science and Technology shall submit to the congressional intelligence committees a report on the cadre, including, with respect to the period covered by the report, the following:
(A) The number of experts onboarded as part of the cadre and the backgrounds and expertise of the experts.

(B) The number of experts required for the cadre.

(C) The training requirements for the cadre.

(D) A comprehensive assessment of the value of the cadre to carry out this section, including details on specific work the cadre is carrying out to facilitate faster adoption of emerging technologies into the intelligence community.

(b) TRAINING.—

(1) Training Curriculum.—The Secretary of Defense and the Director of National Intelligence, in consultation with the President of the Defense Acquisition University and the heads of the elements of the intelligence community that the Secretary and Director determine appropriate, shall jointly establish a training curriculum for acquisition officials within the Department of Defense and the intelligence community focused on improving the understanding and awareness of contracting authorities and procedures for the acquisition of emerging tech-
nologies. The Secretary and the Director shall ensure that the curriculum substantially relies on the principles contained in the TechFAR Handbook for Procuring Digital Services Using Agile Processes of the U.S. Digital Service.

(2) Provision of Training.—The Director shall ensure that the training curriculum under paragraph (1) is provided to each element of the intelligence community.

(3) Report.—Not later than January 1, 2023, the Secretary and the Director shall jointly submit to the congressional intelligence committees a report containing an update on the status of the curriculum under paragraph (1).

(c) Executive Education Activities.—

(1) Establishment.—Not later than January 1, 2024, the Director of National Intelligence, in coordination with the heads of the elements of the intelligence community, shall establish executive education activities on emerging technologies for appropriate managers within the intelligence community who are members of the Senior Intelligence Service or are paid at the GS–13, GS–14, or GS–15 levels. The activities shall be specifically designed to prepare new and existing managers on relevant tech-
nologies and how these technologies may be applied to the intelligence community.

(2) PARTICIPATION.—The Director, in coordination with the heads of the elements of the intelligence community, shall develop a plan for managers described in paragraph (1) to participate in the education activities established under such paragraph. The Director shall ensure that—

(A) the plan is tailored to each individual element of the intelligence community; and

(B) not later than 2 years after the establishment of the education activities, all such managers are required to certify that the managers have successfully completed the education activities.

(3) REPORT.—Not later than January 1, 2023, the Director shall submit to the congressional intelligence committees a report containing an update on the executive education activities under paragraph (1). The report shall include the following:

(A) An overview of—

(i) who participated in the activities;

(ii) what technologies were included in the activities and how those technologies were identified; and
(iii) what other efforts are underway to ensure that the leadership of the intelligence community is able to identify, incorporate, and maintain the most advanced technology in executing the missions of the intelligence community.

(B) An identification of other incentives, activities, resources, and programs that the Director determines may be necessary to ensure that the managers described in paragraph (1) are generally trained in the most advanced technologies.

TITLE VI—MATTERS RELATING TO FOREIGN COUNTRIES

Subtitle A—Miscellaneous Authorities, Requirements, and Limitations

SEC. 601. NOTICE OF DEPLOYMENT OR TRANSFER OF CONTAINERIZED MISSILE SYSTEMS BY RUSSIA, CHINA, OR IRAN.

Section 501 of the Intelligence Authorization Act for Fiscal Year 2016 (division M of Public Law 114–113; 129 Stat. 2923) is amended—

(1) by striking “the Russian Federation” each place it appears and inserting “a covered country”;

f:\VHLD\071922\D071922.067.xml
July 19, 2022 (3:18 p.m.)
(2) by striking “Club-K container missile system” each place it appears and inserting “missile launcher disguised as or concealed in a shipping container”;

(3) in subsection (a)(1)—

(A) by striking “deploy, the” and inserting “deploy, a”; and

(B) by striking “the Russian military” and inserting “the military of the covered country”;

(4) by striking subsection (c) and inserting the following new subsection:

“(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.

“(C) The Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate.

“(2) COVERED COUNTRY.—The term ‘covered country’ means the following:
“(A) Russia.

“(B) China.

“(C) Iran.

“(D) North Korea.”; and

(5) in the heading, by striking “CLUB–K CONTAINER MISSILE SYSTEM BY THE RUSSIAN FEDERATION” and inserting “CONTAINERIZED MISSILE SYSTEM BY RUSSIA OR CERTAIN OTHER COUNTRIES”.

SEC. 602. INTELLIGENCE COMMUNITY COORDINATOR FOR RUSSIAN ATROCITIES ACCOUNTABILITY.

(a) INTELLIGENCE COMMUNITY COORDINATOR FOR RUSSIAN ATROCITIES ACCOUNTABILITY.—

(1) DESIGNATION.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall designate a senior official of the Office of the Director of National Intelligence to serve as the intelligence community coordinator for Russian atrocities accountability (in this section referred to as the “Coordinator”).

(2) DUTIES.—The Coordinator shall oversee the efforts of the intelligence community relating to the following:

(A) Identifying, and (as appropriate) disseminating within the United States Govern-
ment, intelligence relating to the identification, location, or activities of foreign persons suspected of playing a role in committing Russian atrocities in Ukraine.

(B) Identifying analytic and other intelligence needs and priorities of the intelligence community with respect to the commitment of such Russian atrocities.

(C) Addressing any gaps in intelligence collection relating to the commitment of such Russian atrocities and developing recommendations to address any gaps so identified, including by recommending the modification of the priorities of the intelligence community with respect to intelligence collection.

(D) Collaborating with appropriate counterparts across the intelligence community to ensure appropriate coordination on, and integration of the analysis of, the commitment of such Russian atrocities.

(E) Identifying intelligence and other information that may be relevant to preserve evidence of potential war crimes by Russia, consistent with the public commitments of the
United States to support investigations into the conduct of Russia.

(F) Ensuring the Atrocities Early Warning Task Force and other relevant departments and agencies of the United States Government receive appropriate support from the intelligence community with respect to the collection, analysis, preservation, and, as appropriate, dissemination, of intelligence related to Russian atrocities in Ukraine.

(3) PLAN REQUIRED.—Not later than 30 days after the date of enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees—

(A) the name of the official designated as the Coordinator pursuant to paragraph (1); and

(B) the strategy of the intelligence community for the collection of intelligence related to Russian atrocities in Ukraine, including a detailed description of how the Coordinator shall support, and assist in facilitating the implementation of, such strategy.

(4) ANNUAL REPORT TO CONGRESS.—

(A) REPORTS REQUIRED.—Not later than May 1, 2023, and annually thereafter until May
1, 2026, the Director of National Intelligence shall submit to the congressional intelligence committees a report detailing, for the year covered by the report—

(i) the analytical findings and activities of the intelligence community with respect to Russian atrocities in Ukraine; and

(ii) the recipients of information shared pursuant to this section for the purpose of ensuring accountability for such Russian atrocities, and the date of any such sharing.

(B) FORM.—Each report submitted under subparagraph (A) may be submitted in classified form, consistent with the protection of intelligence sources and methods.

(C) SUPPLEMENT.—The Director of National Intelligence may supplement an existing reporting requirement with the information required under subparagraph (A) on an annual basis to satisfy that requirement with prior notification of intent to do so to the congressional intelligence committees.

(b) DEFINITIONS.—In this section:
(1) ATROCITY.—The term “atrocity” means a war crime, crime against humanity, genocide, or crime of aggression.

(2) COMMIT.—The term “commit”, with respect to an atrocity, includes the planning, committing, aiding, and abetting of such atrocity.

(3) FOREIGN PERSON.—The term “foreign person” means a person that is not a United States person.

(4) RUSSIAN ATROCITY.—The term “Russian atrocity” means an atrocity that is committed by an individual who is—

(A) a member of the armed forces, or the security or other defense services, of the Russian Federation;

(B) an employee of any other element of the Russian Government; or

(C) an agent or contractor of an individual specified in subparagraph (A) or (B).

(5) UNITED STATES PERSON.—The term “United States person” has the meaning given that term in section 105A(c) of the National Security Act of 1947 (50 U.S.C. 3039).
(c) SUNSET.—This section shall cease to have effect on the date that is 4 years after the date of the enactment of this Act.

SEC. 603. LEAD INTELLIGENCE COMMUNITY COORDINATOR FOR COUNTERING AND NEUTRALIZING PROLIFERATION OF IRAN-ORIGIN UNMANNED AIRCRAFT SYSTEMS.

(a) COORDINATOR.—

(1) DESIGNATION.—Not later than 30 days after the date of enactment of this Act, the Director of National Intelligence shall designate an official from an element of the intelligence community to serve as the lead intelligence community coordinator for countering and neutralizing the proliferation of Iran-origin unmanned aircraft systems (in this section referred to as the “Coordinator”).

(2) PLAN.—Not later than 120 days after the date on which the Coordinator is designated under paragraph (1), the Coordinator shall—

(A) develop a comprehensive plan of action, driven by intelligence information, for countering and neutralizing the threats posed by the proliferation of Iran-origin unmanned aircraft systems; and
(B) provide to the congressional intelligence committees a briefing on such plan of action.

(3) Final Report.—

(A) Submission.—Not later than January 1, 2024, the Director of National Intelligence shall submit to the congressional intelligence committees a final report on the activities and findings of the Coordinator.

(B) Matters.—The report under subparagraph (A) shall include the following:

(i) An assessment of the threats posed by Iran-origin unmanned aircraft systems, including the threat to facilities and personnel of the United States Government in the greater Middle East, particularly in the areas of such region that are located within the area of responsibility of the Commander of the United States Central Command.

(ii) A detailed description of intelligence sharing efforts, as well as other joint efforts driven by intelligence information, with allies and partners of the United
States, to assist in countering and neutralizing of such threats.

(iii) Recommendations for any changes in United States policy or legislative authorities to improve the capacity of the intelligence community to assist in countering and neutralizing such threats.

(C) FORM.—The report under subparagraph (A) may be submitted in classified form.

(b) COLLABORATION WITH FIVE EYES PARTNERSHIP AND ISRAEL.—Taking into account the findings of the final report under subsection (a)(3), the Director of National Intelligence shall seek to—

(1) develop and implement a common approach among the Five Eyes Partnership toward countering the threats posed by Iran-origin unmanned aircraft systems, including by leveraging the unique intelligence capabilities and information of the members of the Five Eyes Partnership; and

(2) intensify cooperation with Israel for the purpose of countering Iran-origin unmanned aircraft systems, including by strengthening and expanding existing cooperative efforts conducted pursuant to section 1278 of the National Defense Authorization

(c) DEFINITIONS.—In this section:

(1) Five eyes partnership.—The term “Five Eyes Partnership” means the intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

(2) Unmanned aircraft system.—The term “unmanned aircraft system” includes an unmanned powered aircraft (including communication links and the components that control the unmanned aircraft), that—

(A) does not carry a human operator;

(B) may fly autonomously or be piloted remotely;

(C) may be expendable or recoverable; and

(D) may carry a lethal payload or explode upon reaching a designated location.

(d) SunSet.—This section shall cease to have effect on the date on which the final report is submitted under subsection (a)(3).
SEC. 604. COLLABORATION BETWEEN INTELLIGENCE COMMUNITY AND DEPARTMENT OF COMMERCE TO COUNTER FOREIGN COMMERCIAL THREATS.

(a) Working Group.—

(1) Establishment.—Unless the Director of National Intelligence and the Secretary of Commerce make the joint determination specified in subsection (b), the Director and the Secretary, in consultation with the head of any other department or agency of the United States Government determined appropriate by the Director or the Secretary, shall jointly establish a working group to counter foreign commercial threats (in this section referred to as the “Working Group”).

(2) Membership.—The composition of the Working Group may include any officer or employee of a department or agency of the United States Government determined appropriate by the Director or the Secretary.

(3) Duties.—The duties of the Working Group shall be the following:

(A) To identify current foreign commercial threats.

(B) To identify probable future foreign commercial threats.
(C) To discuss opportunities to address the harm to the national security of the United States arising out of foreign commercial threats.

(D) To identify goods, services, or intellectual property that, if produced by, offered by, sold by, licensed by, or otherwise distributed under the control of, the United States, would mitigate the foreign commercial threat.

(4) MEETINGS.—Not later than 30 days after the date of the enactment of this Act, and on a regular basis that is not less frequently than quarterly thereafter until the date of termination under paragraph (5), the Working Group shall meet.

(5) TERMINATION.—Beginning on the date that is 2 years after the date of the establishment under paragraph (1), the Working Group may be terminated upon the Director of National Intelligence and the Secretary of Commerce jointly—

(A) determining that termination of the Working Group is appropriate; and

(B) submitting to the appropriate congressional committees a notification of such determination (including a description of the justification for such determination).
(6) REPORTS.—

(A) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, and biannually thereafter until the date of termination under paragraph (5), the Working Group shall submit to the appropriate congressional committees a report on the activities of the Working Group.

(B) MATTERS.—Each report under subparagraph (A) shall include a description of the following:

(i) Any current foreign commercial threats identified by the Working Group.

(ii) Any future foreign commercial threats identified by the Working Group.

(iii) The strategy of the United States Government, if any, to mitigate any current foreign commercial threats or future foreign commercial threats so identified.

(iv) The plan of the intelligence community to provide to the Department of Commerce and other nontraditional customers of the intelligence community support in addressing foreign commercial threats.
(v) Any other significant activity of the Working Group.

(b) **OPTION TO DISCHARGE OBLIGATION THROUGH OTHER MEANS.**—If the Director of National Intelligence and the Secretary of Commerce make a joint determination that the requirements of the Working Group under subsection (a) (including the duties under paragraph (3) and the reporting requirement under paragraph (6) of such subsection) may be appropriately filled by an existing entity or structure, and submit to the congressional intelligence committees a notification of such determination (including a description of the justification for such determination), the Director and Secretary may task such entity or structure with such requirements in lieu of establishing the Working Group.

(e) **DEFINITIONS.**—In this section:

(1) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term “appropriate congressional committees” means—

(A) the congressional intelligence committees;

(B) the Committee on Energy and Commerce of the House of Representatives; and

(C) the Committee on Commerce, Science, and Transportation of the Senate.
(2) FOREIGN ADVERSARY.—The term “foreign adversary” means the following:

(A) China.

(B) Iran.

(C) North Korea.

(D) Russia.

(E) Any other foreign country that the Director of National Intelligence or the Secretary of Commerce designates for purposes of this section.

(3) FOREIGN COMMERCIAL THREAT.—The term “foreign commercial threat” means a scenario in which a rare commercial item or service is produced by, offered by, sold by, licensed by, or otherwise distributed under the control of a foreign adversary in a manner that may provide the foreign adversary leverage over an intended recipient by—

(A) withholding, or threatening to withhold, the rare commercial item or service; or

(B) creating reliance on the rare commercial item or service as essential to the safety, health, or economic well-being of the intended recipient.

(4) RARE COMMERCIAL ITEM OR SERVICE.—

The term “rare commercial item or service” means
a good, service, or intellectual property that is not widely available for distribution.

SEC. 605. INTELLIGENCE ASSESSMENT ON FOREIGN WEAPONIZATION OF ADVERTISEMENT TECHNOLOGY DATA.

(a) Assessment.—The Director of National Intelligence shall conduct an intelligence assessment of the counterintelligence risks of, and the exposure of intelligence community personnel to, tracking by foreign adversaries through advertisement technology data.

(b) Report.—Not later than 60 days after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees a report on the intelligence assessment under subsection (a).

(c) Advertisement Technology Data Defined.—In this section, the term “advertisement technology data” means commercially available data derived from advertisement technology that is used, or can be used, to geolocate individuals or gain other targeting information on individuals.

SEC. 606. INTELLIGENCE COMMUNITY ASSESSMENT REGARDING RUSSIAN GRAY ZONE ASSETS.

(a) Intelligence Community Assessment Regarding Russian Gray Zone Assets.—
(1) INTELLIGENCE COMMUNITY ASSESSMENT.—

The Director of National Intelligence, acting through the National Intelligence Council, shall produce an intelligence community assessment that contains—

(A) a description of the gray zone assets of Russia;

(B) an identification of any opportunities to hold such gray zone assets at risk, as a method of influencing the behavior of Russia; and

(C) an assessment of the risks and potential benefits, with respect to the interests of the United States, that may result from the seizure of such gray zone assets to hold the assets at risk.

(2) CONSIDERATIONS.—In identifying opportunities to hold a gray zone asset of Russia at risk under paragraph (1)(B), the National Intelligence Council shall consider the following:

(A) The effect on civilians of holding the gray zone asset at risk.

(B) The extent to which the gray zone asset is substantially state-owned or substantially controlled by Russia.
(C) The likelihood that holding the gray zone asset at risk will influence the behavior of Russia.

(D) The likelihood that holding the gray asset at risk, or degrading the asset, will affect any attempt of Russia to use force to change existing borders or undermine the political independence or territorial integrity of any state, including Ukraine.

(E) Such other factors as the National Intelligence Council may determine appropriate.

(3) APPENDIX.—The intelligence community assessment under paragraph (1) shall include an appendix that contains a list of the categories of gray zone assets of Russia, with specific examples of—

(A) gray zone assets in each category; and

(B) for each such gray zone asset listed, the ways in which Russia uses the asset to advance its gray zone activities.

(4) SUBMISSION.—The Director, consistent with the protection of sources and methods, shall submit to the congressional intelligence committees the intelligence community assessment under paragraph (1).
(5) FORM.—The intelligence community assessment under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex.

(b) DEFINITIONS.—In this section:

(1) GRAY ZONE ACTIVITY.—The term “gray zone activity” has the meaning given that term in section 825 of the Intelligence Authorization Act for Fiscal Year 2022 (Public Law 117–103).

(2) GRAY ZONE ASSET.—The term “gray zone asset”—

(A) means an entity or proxy that is controlled, in whole or in part, by a foreign adversary of the United States and is used by such foreign adversary in connection with a gray zone activity; and

(B) includes a state-owned enterprise of a foreign adversary that is so used.

SEC. 607. INTELLIGENCE ASSESSMENT ON EFFECTS OF SANCTIONS ON RUSSIA.

(a) REQUIREMENT.—Not later than 120 days after the date of the enactment of this Act, the Assistant Secretary of the Treasury for Intelligence and Analysis, in consultation with other departments and agencies of the United States Government that the Assistant Secretary determines appropriate, shall submit to the appropriate
congressional committees an intelligence assessment on
the effects of the financial and economic sanctions the
United States and the allies and partners of the United
States have imposed on Russia following its further un-
justified incursion onto Ukrainian territory on February
24, 2022.

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

(1) An analysis of the effects of sanctions on
the economy of Russia and on individual sectors, ent-
tities, and persons.

(2) Methodologies for assessing the effects of
different categories of financial and economic sanc-
tions and export controls on the targets of the sanc-
tions, including with respect to specific industries,
entities, individuals, or transactions.

(3) A discussion of sanctions that had signifi-
cant effects based on the methodologies under para-
graph (2).

(4) A discussion of sanctions that had no meas-
urable effects based on the methodologies under
paragraph (2).

(5) A description of measures that the Russian
Government has introduced to mitigate the effects of
sanctions and an analysis of the efficacy of such measures.

(6) A projection of the effects of sanctions in the short- and long-term following the date of the assessment.

(7) A description of evasion techniques used by the Russian Government, entities, and persons covered by the sanctions, and by other governments, entities, and persons who have assisted in the use of such techniques, in response to the sanctions.

(8) An enumeration of—

(A) the known governments, entities, and persons who have assisted in the use of evasion techniques described in paragraph (7); and

(B) the types of transactions for which assistance has been provided.

(c) FORM.—The intelligence assessment under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary, consistent with the protection of sources and methods.

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

(1) the congressional intelligence committees;
(2) the Committee on Foreign Affairs and the Committee on Finance of the House of Representatives; and

(3) the Committee on Foreign Relations and the Committee on Finance of the Senate.

Subtitle B—Reports and Other Matters

SEC. 611. REPORT ON ASSESSING WILL TO FIGHT.

(a) FINDINGS.—Congress finds the following:

(1) According to a study by the RAND corporation, “will to fight” is poorly analyzed and the least understood aspect of war.

(2) In testimony before the Select Committee on Intelligence of the Senate in May 2022, top intelligence officials of the United States indicated that although the intelligence community accurately anticipated Russia’s invasion of Ukraine, the intelligence community did not accurately assess the will of Ukrainian forces to fight in opposition to a Russian invasion or that the Ukrainian forces would succeed in averting a rapid Russian military occupation of Kyiv.

(3) According to the RAND corporation, the intelligence community estimated that the Afghan government’s forces could hold out against the Taliban
for as long as 2 years if all ground forces of the United States were withdrawn. This estimate was revised in June 2021 to reflect an intelligence community view that Afghanistan’s military collapse could come in 6 to 12 months. In August 2021, the Afghan government fell within days after the ground forces of the United States were withdrawn.

(4) Similarly, the rapid advance of the Islamic State in Iraq and Syria and near-total collapse of the Iraqi Security Forces in 2014 appeared to take the policymakers of the United States by surprise.

(5) The apparent gaps in these analyses had important implications for policy decisions of the United States toward Russia and Afghanistan, and suggest a need for further examination of how the intelligence community assesses a foreign military’s will to fight.

(b) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, acting through the National Intelligence Council, and in coordination with the heads of the elements of the intelligence community that the Director determines appropriate, shall submit to the appropriate congressional committees a report examining the extent to which analyses of the military will to fight and the national will to
fight informed the all-source analyses of the intelligence community regarding how the armed forces and governments of Ukraine, Afghanistan, and Iraq would perform at key junctures.

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

(1) The methodology of the intelligence community for measuring the military will to fight and the national will to fight of a foreign country.

(2) The extent to which analysts of the intelligence community applied such methodology when assessing the military will to fight and the national will to fight of—

   (A) Afghanistan following the April 2021 announcement of the full withdrawal of the United States Armed Forces;

   (B) Iraq in the face of the rapid emergence and advancement in 2014 of Islamic State in Iraq and Syria; and

   (C) Ukraine and Russia during the initial phase of the invasion and march toward Kyiv by Russia in February 2022.

(3) The extent to which—

   (A) the assessments described in paragraph (2) depended on the observations of per-
sonnel of the United States Armed Forces who
had trained Afghan, Iraqi, and Ukrainian
armed forces; and

(B) such observations reflected any stand-
ardized, objective methodology.

(4) Whether shortcomings in assessing the mili-
tary will to fight and the national will to fight may
have affected the capacity of the intelligence commu-
nity to provide “early warning” about the collapse of
government forces in Iraq and Afghanistan.

(5) The extent to which “red teaming” was used to test the assessments described in paragraph (2).

(6) The extent to which dissenting opinions of intelligence analysts were highlighted in final written products presented to senior policymakers of the United States.

(7) The extent to which analysts and supervi-
sors adhered to the policies, procedures, directives,
and best practices of the intelligence community.

(8) Recommendations for analyses by the intel-
ligence community going forward to incorporate les-
sions learned and enhance the quality of future ana-
lytical products to more accurately reflect the mili-
tary will to fight and the national will to fight and
improve the capacity of the intelligence community
to accurately predict the success or failure of the
armed forces of a foreign country.

(d) ANNEX.—In submitting the report under sub-
section (b) to the congressional intelligence committees,
the Director shall also include an accompanying annex,
which shall be classified, providing an inventory of the fol-
lowing:

(1) Collection gaps and challenges that may
have affected the analysis of the collapse of govern-
ment forces in Iraq and Afghanistan.

(2) Actions that the Director of National Intel-
ligence has taken to mitigate such gaps and chal-
lenges.

(e) FORM.—The report under subsection (b) may be
submitted in classified form, but if so submitted, shall in-
clude an unclassified summary of key findings, consistent
with the protection of intelligence sources and methods.

(f) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMIT-
TEES.—The term “appropriate congressional com-
mittees” means the following:

(A) The congressional intelligence commit-
tees.
(B) The Committee on Foreign Affairs and the Committee on Armed Services of the House of Representatives.

(C) The Committee on Foreign Relations and the Committee on Armed Services of the Senate.

(2) MILITARY WILL TO FIGHT.—The term “military will to fight” means, with respect to the military of a country, the disposition and decision to fight, act, or persevere as needed.

(3) NATIONAL WILL TO FIGHT.—The term “national will to fight” means, with respect to the government of a country, the resolve to conduct sustained military and other operations for an objective even when the expectation of success decreases or the need for significant political, economic, and military sacrifices increases.

SEC. 612. REPORT ON IMPACT OF RUSSIA INVASION OF UKRAINE ON GLOBAL FOOD SECURITY.

(a) REQUIREMENT.—Not later than 180 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the Assistant Secretary of State for Intelligence and Research and other heads of elements of the intelligence community as the Director determines appropriate, shall submit to the congressional in-
intelligence committees a report on the implications of Russia’s invasion of Ukraine on global food insecurity and the impact on national security.

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

(1) An assessment of global food insecurity resulting from Russia’s invasion of Ukraine, including—

(A) the potential for political instability as a result of such food insecurity;

(B) the implications for national security;

and

(C) a description of which regions are at greatest risk of such food insecurity.

(2) An assessment of whether Russia has taken intentional steps to cause a global food shortage.

(3) An assessment of whether Russia, China, or any other foreign actor has the capability to weaponize food supply or cause disruptions in global food supply to serve geopolitical purposes.

(c) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.
SEC. 613. REPORT ON THREAT FROM HYPERSONIC WEAPONS.

(a) 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 containing an assessment of the threat to the United States from hypersonic weapons in light of the use of such weapons by Russia in Ukraine.

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

(1) The information learned by the United States regarding the hypersonic weapons capabilities of Russia.

(2) Insights into the doctrine of Russia regarding the use of hypersonic weapons.

(3) An assessment of how foreign countries view the threat of hypersonic weapons.

(4) An assessment of the degree to which the development of missiles with similar capabilities as hypersonic weapons used by Russia would enhance or reduce the ability of the United States to deter Russia from threatening the national security of the United States.

(c) FORM.—The report under subsection (a) may be submitted in classified form.
SEC. 614. REPORT ON ORDNANCE OF RUSSIA AND CHINA.

(a) REQUIREMENT.—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 and the congressional defense committees a report on ordnance of Russia and China, including the technical specificity required for the safe handling and disposal of such ordnance.

(b) COORDINATION.—The Director shall carry out subsection (a) in coordination with the head of any element of the Defense Intelligence Enterprise that the Director determines appropriate.

(c) DEFINITIONS.—In this section:

(1) CONGRESSIONAL DEFENSE COMMITTEES.—The term “congressional defense committees” has the meaning given that term in section 101(a) of title 10, United States Code.

(2) DEFENSE INTELLIGENCE ENTERPRISE.—The term “Defense Intelligence Enterprise” has the meaning given that term in section 426(b) of title 10, United States Code.

SEC. 615. REPORT ON ACTIVITIES OF CHINA AND RUSSIA TARGETING LATIN AMERICA AND THE CARIBBEAN.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National In-
intelligence, acting through the National Intelligence Coun-
cil, shall submit to the congressional intelligence commit-
tees a report on activities undertaken by China and Russia
in Latin America and the Caribbean that are intended to
increase the influence of China and Russia, respectively,
therein. Such report shall include a description of the fol-
lowing:

(1) Foreign malign influence campaigns by
China and Russia targeting Latin America and the
Caribbean.

(2) Financial investments intended to increase
Chinese or Russian influence in Latin America and
the Caribbean.

(3) Efforts by China and Russia to expand dip-
lomatic, military, or other ties to Latin America and
the Caribbean.

(4) Any other activities determined appropriate
by the Director.

(b) MATTERS.—With respect to the description of
foreign malign influence campaigns under subsection (a),
the report shall include an assessment of the following:

(1) The objectives of any such campaign.

(2) The themes and messaging used in any
such campaign.
(3) The scale and nature of the threat posed by any such campaign.

(4) The effect of such threat on the national security, diplomatic, military, or economic interests of the United States.

(5) Any gaps in the intelligence collection or analysis of the intelligence community with respect to such threat, and recommendations for the mitigation of any such gaps.

(6) Opportunities for the heads of the intelligence community, or other relevant United States Government entities, to identify, disrupt, or counter the campaigns specified in subsection (a).

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

(d) DEFINITIONS.—In this section:

(1) FOREIGN MALIGN INFLUENCE.—The term “foreign malign influence” means any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a foreign country with the objective of influencing, through overt or covert means—

(A) the political, military, economic, or other policies or activities of the government of
the country that is the target of the hostile ef-
fort, including any election within such target
country; or

(B) the public opinion within such target
country.

(2) LATIN AMERICA AND THE CARIBBEAN.—
The term “Latin America and the Caribbean”
means the countries and non-United States terri-
tories of South America, Central America, the Carib-
bean, and Mexico.

SEC. 616. REPORT ON SUPPORT PROVIDED BY CHINA TO
RUSSIA.

(a) REQUIREMENT.—Not later than 90 days after the
date of the enactment of this Act, and every 180 days
thereafter, consistent with the protection of intelligence
sources and methods, the Director of National Intel-
ligence, in consultation with the heads of elements of the
intelligence community that the Director determines ap-
propriate, shall submit to the appropriate congressional
committees a report on whether and how China, including
with respect to the Government of the People’s Republic
of China, the Chinese Communist Party, any Chinese
state-owned enterprise, and any other Chinese entity, has
provided support to Russia with respect to the unprovoked
invasion of and full-scale war by Russia against Ukraine.
(b) MATTERS INCLUDED.—The report under subsection (a) shall include a discussion of support provided by China to Russia with respect to—

   (1) helping the Government of Russia or Russian entities evade or circumvent sanctions by the United States or multilateral sanctions and export controls;

   (2) deliberately inhibiting onsite United States Government export control end-use checks, including interviews and investigations, in China;

   (3) providing Russia with any technology, including semiconductors classified as EAR99, that supports Russian intelligence or military capabilities;

   (4) establishing economic or financial arrangements that will have the effect of alleviating the effect of sanctions by the United States or multilateral sanctions; and

   (5) providing any material, technical, or logistical support, including to Russian military or intelligence agencies and state-owned or state-linked enterprises.

(c) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may contain a classified annex.
(d) **SUNSET.**—The requirement to submit the report under subsection (a) shall terminate on the earlier of—

1. the date on which the Director of National Intelligence determines the conflict in Ukraine has ended; or
2. the date that is 2 years after the date of the enactment of this Act.

(e) **APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.**—In this section, the term “appropriate congressional committees” means—

1. the congressional intelligence committees;
2. the Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives; and
3. the Committee on Foreign Relations and the Committee on Banking, Housing, and Urban Affairs of the Senate.

**SEC. 617. REPORT ON GLOBAL CCP INVESTMENT IN PORT INFRASTRUCTURE.**

(a) **IN GENERAL.**—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Secretary of State and the Secretary of Defense, shall submit to the appropriate congressional committees a report documenting all Chinese investment in port infrastructure globally, during
the period beginning on January 1, 2012, and ending on
the date of the submission of the report, and the commer-
cial and economic implications of such investments. The
report shall also include the following:

(1) A review of existing and potential or
planned future Chinese investments, including in-
vestments by government entities, and state-owned
to enterprises, in port infrastructure at such ports.

(2) Any known Chinese interest in establishing
a military presence at or near such ports.

(3) An assessment of China’s current and po-
tential future ability to leverage commercial ports
for military purposes and the implications of such
ability for the national and economic security of the
United States.

(b) FORM.—The report required by subsection (a)
shall be submitted in unclassified form but may include
a classified annex produced consistent with the protection
of sources and methods.

c) APPROPRIATE CONGRESSIONAL COMMITTEES DE-
FINED.—In this section, the term “appropriate congress-
sional committees” means—

(1) the congressional intelligence committees;
(2) the Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives; and

(3) the Committee on Armed Services and the Committee on Foreign Relations of the Senate.

SEC. 618. SENSE OF CONGRESS ON PROVISION OF SUPPORT BY INTELLIGENCE COMMUNITY FOR ATROCITY PREVENTION AND ACCOUNTABILITY.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the efforts of the United States Government regarding atrocity prevention and response through inter-agency coordination, such as the Atrocity Warning Task Force, are critically important and that the Director of National Intelligence and the Secretary of Defense should, as appropriate, do the following:

(1) Require each element of the intelligence community to support the Atrocity Warning Task Force in its mission to prevent genocide and atrocity prevention and response through policy formulation and program development by—

(A) collecting and analyzing intelligence identified as an atrocity, as defined in the Elie Wiesel Genocide and Atrocities Prevention Act of 2018 (Public Law 115–441; 132 Stat. 5586);
(B) preparing unclassified intelligence data and geospatial imagery products for coordination with appropriate domestic, foreign, and international courts and tribunals prosecuting persons responsible for crimes for which such imagery and intelligence may provide evidence (including genocide, crimes against humanity, and war crimes, including with respect to missing persons and suspected atrocity crime scenes); and

(C) reassessing archived geospatial imagery containing indicators of war crimes, other atrocities, forced disappearances, and atrocity crime scenes.

(2) Continue to make available inputs to the Atrocity Warning Task Force for the development of the Department of State Atrocity Early Warning Assessment and share open-source data to support pre-atrocity and genocide indicators and warnings to the Atrocity Warning Task Force.

(3) Provide the President and Congress with recommendations to improve policies, programs, resources, and tools relating to atrocity intelligence collection and interagency coordination.
(4) Regularly consult and participate with designated interagency representatives of relevant agencies and departments of the United States Government.

(5) Ensure resources are made available for the policies, programs, and tools relating to atrocity intelligence collection and coordination with the Atrocity Warning Task Force.

(b) DEFINITIONS.—In this section:

(1) ATROCITIES.—The term “atrocities” has the meaning given that term in section 6 of the Elie Wiesel Genocide and Atrocities Prevention Act of 2018 (Public Law 115–441; 132 Stat. 5586).

(2) ATROCITY CRIME SCENE.—The term “atrocity crime scene” means 1 or more locations that are relevant to the investigation of an atrocity, including buildings or locations (including bodies of water) where physical evidence may be collected relating to the perpetrators, victims, and events of the atrocity, such as mass graves and other sites containing deceased individuals.
TITLE VII—REPORTS AND OTHER MATTERS

SEC. 701. REPEAL OF CERTAIN REPORT REQUIREMENTS.


(b) Reports on Security Services of the People’s Republic of China in the Hong Kong Special Administrative Region.—Section 1107A of the National Security Act of 1947 (50 U.S.C. 3237a) is repealed.

(c) Annual Update to Report on Foreign Weaponization of Deepfakes and Deepfake Technology.—Section 5709 of the National Defense Authorization Act for Fiscal Year 2020 (50 U.S.C. 3369a) is amended—

(1) by striking subsection (d); and

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

SEC. 702. INCREASED INTELLIGENCE-RELATED ENGINEERING, RESEARCH, AND DEVELOPMENT CAPABILITIES OF MINORITY INSTITUTIONS.

(a) Plan.—

(1) Requirement.—The Director of National Intelligence shall develop a plan to promote intelligence-related engineering, research, and develop-
ment activities at covered institutions for the purpose of contributing toward the research necessary to achieve the intelligence advantage of the United States.

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

(A) An assessment of opportunities to support engineering, research, and development at covered institutions in computer sciences, including artificial intelligence, quantum computing, and machine learning, and synthetic biology and an assessment of opportunities to support the associated workforce and physical research infrastructure of such institutions.

(B) An assessment of opportunities to enhance the ability of covered institutions—

(i) to participate in intelligence-related engineering, research, and development activities; and

(ii) to effectively compete for intelligence-related engineering, research and development contracts in support of the most urgent research requirements of the intelligence community.
(C) An assessment of the activities and investments the Director determines necessary—

(i) to expand opportunities for covered institutions to partner with other research organizations and educational institutions that the intelligence community frequently partners with to conduct research; and

(ii) to increase participation of covered institutions in intelligence-related engineering, research, and development activities.

(D) Recommendations identifying actions that may be taken by the Director, Congress, covered institutions, and other organizations to increase participation of such institutions in intelligence-related engineering, research, and development activities and contracts.

(E) Specific goals, incentives, and metrics to increase and measure the capacity of covered institutions to address the engineering, research, and development needs of the intelligence community.

(3) CONSULTATION.—In developing the plan under paragraph (1), the Director shall consult with covered institutions and other departments or agen-
cies of the United States Government or private sec-
tor organizations that the Director determines ap-
propriate.

(4) REPORT.—Not later than 1 year after the
date of the enactment of this Act, the Director shall
submit to the congressional intelligence committees,
and make publicly available on the internet website
of the Director, a report containing the plan under
paragraph (1).

(b) ACTIVITIES TO SUPPORT RESEARCH AND ENGI-
NEERING CAPACITY.—Subject to the availability of appro-
priations for such purpose, the Director may establish a
program to award contracts, grants, or other agreements,
on a competitive basis, and to perform other appropriate
activities, for any of the following purposes:

(1) Developing the capability, including the
workforce and the research infrastructure, for cov-
ered institutions to more effectively compete for in-
telligence-related engineering, research, and develop-
ment activities and contracts.

(2) Any other purposes the Director determines
appropriate to enhance the capabilities of covered in-
stitutions to carry out intelligence-related engineer-
ing, research, and development activities and con-
tracts.
(c) Increased Partnerships Between IARPA and Covered Institutions.—The Director shall establish goals and incentives to encourage the Intelligence Advanced Research Projects Activity to—

(1) partner with covered institutions to advance the research and development needs of the intelligence community through partnerships and collaborations with the Intelligence Advanced Research Projects Activity; and

(2) if the Director determines appropriate, foster the establishment of similar relationships between such institutions and other organizations that have partnerships with the Intelligence Advanced Research Projects Activity.

(d) Covered Institution Defined.—In this section, the term “covered institution” means the following:

(1) A part B institution (as defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061)).

(2) An institution of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) not covered by paragraph (1) at which not less than 50 percent of the total student enrollment consists of students from ethnic groups that are underrepresented in the fields of
science and engineering, as determined by the Director of National Intelligence.

SEC. 703. ANNUAL REPORT ON RESPONSE TO GOVERNMENT ACCOUNTABILITY OFFICE RECOMMENDATIONS TO INTELLIGENCE COMMUNITY.

(a) ANNUAL REPORT.—Not later than October 31, 2023, and annually thereafter until October 31, 2028, the Director of National Intelligence shall submit to the congressional intelligence committees a report, consolidated from each element of the intelligence community, regarding the status of responses to the recommendations made by the Comptroller General to the Director or to the other heads of the elements of the intelligence community.

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

(1) A list of any open recommendations as of September 30 of the year in which the report is submitted (using a unique identifier for each open recommendation).

(2) A description of the actions the Director or the other heads of the elements of the intelligence community have taken, alone or in coordination with other departments or agencies of the United States
Government, to implement or otherwise respond to each such open recommendation.

(3) Of such open recommendations, a list of any recommendations (using a unique identifier for each recommendation) with which the Director or the other heads of the elements of the intelligence community do not concur and intend to take no action to implement, including a detailed justification for each such determination.

(c) Open Recommendation Defined.—In this section, the term “open recommendation” means a recommendation that the Comptroller General has not designated as closed.

SEC. 704. ANNUAL REPORT ON EFFORTS OF THE FEDERAL BUREAU OF INVESTIGATION TO IDENTIFY AND PROMOTE DIVERSE CANDIDATES.

(a) Statistical Report.—

(1) Requirement.—Not later than 90 days after the date of the enactment of this Act, and annually thereafter through 2027, the Director of the Federal Bureau of Investigation shall submit to the appropriate congressional committees, and make publicly available on the internet website of the Director, a statistical report on the status of the ef-
forts of the Federal Bureau of Investigation to identify and promote diverse candidates.

(2) ELEMENTS.—Each report under paragraph (1) shall include, with respect to the year covered by the report, tables of figures that break down, by race and gender, the following:

(A) With respect to each covered position—

(i) the total number of Special Agents, and the percentage of Special Agents, who apply to such positions;

(ii) the total number of Special Agents, and the percentage of Special Agents, who are interviewed for such positions;

(iii) the total number of Special Agents, and the percentage of Special Agents, who are selected for such positions; and

(iv) the average number of times a Special Agent applied for such position before selection.

(B) With respect to GS–14 and GS–15 positions—
(i) the total number of individuals in such positions, and the percentage of such individuals, who retired; and

(ii) the total number of individuals in such positions, and the percentage of such individuals, who retired early.

(b) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees; and

(B) the Committees on the Judiciary and the Committees on Appropriations of the House of Representatives and the Senate.

(2) COVERED POSITION.—The term “covered position” means, with respect to positions in the Federal Bureau of Investigation, the following:

(A) Federal Bureau of Investigation Headquarters Supervisory Special Agent program manager.

(B) Field Supervisory Special Agent.

(C) Assistant Special Agent in Charge.

(D) Special Agent in Charge.

(E) Senior executive.
(3) SENIOR EXECUTIVE.—The term “senior executive” means, with respect to positions in the Federal Bureau of Investigation, the following:

(A) Deputy Assistant Director.

(B) Assistant Director.

(C) Executive Assistant Director.

(D) Associate Deputy Director.

(E) Deputy Director.

SEC. 705. REPORTS ON PERSONNEL VETTING PROCESSES AND PROGRESS UNDER TRUSTED WORKFORCE 2.0 INITIATIVE.

(a) REPORTS.—Not later than September 30, 2023, and annually thereafter until September 30, 2027, the Security Executive Agent, in coordination with the Chair and other Principals of the Council, shall submit to the congressional intelligence committees a report on the personnel vetting processes of the United States Government.

(b) ELEMENTS.—Each report under subsection (a) shall include, with respect to the preceding fiscal year, the following:

(1) An analysis of the timeliness, costs, and other related information for the initiations, investigations (including initial investigations and periodic reinvestigations), and adjudications of personnel
security clearances. Such analysis shall include the following:

(A) The average periods of time taken (from the date of the submission of a completed security clearance application to the date of the ultimate disposition and notification to the subject and the employer of the subject) by each authorized investigative agency and authorized adjudicative agency to initiate investigations, conduct investigations, and adjudicate security clearances, as compared with established timeliness objectives.

(B) The number of initial investigations and periodic reinvestigations initiated and adjudicated by each authorized investigative agency and authorized adjudicative agency.

(C) The number of initial investigations and periodic reinvestigations carried over to the fiscal year covered by the report from a prior fiscal year by each authorized investigative agency and authorized adjudicative agency.

(D) The number of initial investigations and periodic reinvestigations that resulted in a denial or revocation of a security clearance by each authorized adjudicative agency.
(E) The costs to the executive branch relating to personnel security clearance initi-
ations, investigations, adjudications, revoca-
tions, and continuous vetting with respect to such clearances.

(F) A discussion of any impediments, in-
cluding with respect to resources, personnel, or authorities, to the timely processing of per-
sonnel security clearances.

(G) The number of individuals who hold a personnel security clearance and are enrolled in a program of continuous vetting with respect to such clearance, and the numbers and types of adverse actions taken by each authorized adju-
dicative agency as a result of such continuous vetting.

(H) The number of personnel security clearances awaiting or under investigation (in-
cluding initial investigation and periodic re-investigation) by the Director of the Defense Counterintelligence and Security Agency and each authorized investigative agency.

(I) Such other information as the Security Executive Agent may determine appropriate, in-
cluding any recommendations to improve the
timeliness and efficiency of personnel security clearance initiations, investigations, and adjudications.

(2) An analysis of the status of the implementation of the Trusted Workforce 2.0 initiative sponsored by the Council, including the following:

(A) A list of the policies issued by the Council for the Trusted Workforce 2.0 initiative, and a list of expected issuance dates for planned policies of the Council for such initiative.

(B) A list of the departments and agencies of the executive branch that have identified a senior implementation official to be accountable for the implementation of the Trusted Workforce 2.0 initiative, in accordance with the memorandum on transforming Federal personnel vetting issued by the Assistant to the President for National Security Affairs on December 14, 2021, including an identification of the position of such senior implementation official within the respective department or agency.

(C) A list of the departments and agencies of the executive branch that have submitted implementation plans, and subsequent progress re-
ports, with respect to the Trusted Workforce
2.0 initiative, as required by the memorandum
specified in subparagraph (B).

(D) A summary of the progress that the
departments and agencies of the executive
branch have made implementing the Trusted
Workforce 2.0 initiative.

(3) An analysis of the transfers between, and
reciprocal recognition among, the heads of the de-
partments and agencies of the executive branch of
security clearance background investigations and de-
terminations and other investigations and deter-
minations relating to personnel vetting (including
with respect to trust, suitability, fitness,
credentialing, and access). Such analysis shall in-
clude, with respect to such investigations and deter-
minations, the following:

(A) The number of employees for whom a
prior such investigation or determination was
recognized and accepted by the head of a de-
partment or agency without the head requiring
additional investigative or adjudicative steps,
disaggregated by department or agency.

(B) The number of employees for whom a
prior such investigation or determination was
not recognized or accepted by the head of a department or agency without the head requiring additional investigative or adjudicative steps, disaggregated by department or agency.

(C) The reasons most frequently cited by such heads for the failure to recognize or accept a prior such investigation or determination, disaggregated by department or agency.

(D) The average number of days for the head of a department or agency to recognize and accept a prior such investigation or determination (from the date the head initiates the process to consider the prior investigation or determination for recognition and acceptance, to the date the head makes a final determination on such recognition and acceptance), disaggregated by agency.

(4) A discussion of any impediments, constraints, and opportunities relating to—

(A) the timeliness of the personnel security clearance process across the United States Government;

(B) the implementation of the Trusted Workforce 2.0 initiative; or
(C) the transfer and reciprocal recognition
of determinations relating to personnel vetting
between and among departments and agencies.

(c) Definitions.—In this section:

(1) Authorized adjudicative agency; au-
thorized investigative agency; personnel sec-
curity investigation; periodic reinvestiga-
tion.—The terms “authorized adjudicative agency”,
“authorized investigative agency”, “personnel secu-
ritiy investigation”, and “periodic reinvestigation”
have the meanings given those terms in section
3001(a) of the Intelligence Reform and Terrorism
Prevention Act of 2004 (50 U.S.C. 3341(a)).

(2) Continuous vetting; council; security
executive agent.—The terms “continuous vet-
ting”, “Council”, and “Security Executive Agent”
have the meanings given those terms in section 6601
of the Damon Paul Nelson and Matthew Young Pol-
lard Intelligence Authorization Act for Fiscal Years

SEC. 706. REPORTS RELATING TO PROGRAMS OF RECORD
OF NATIONAL GEOSPATIAL-INTELLIGENCE
AGENCY.

(a) Findings.—Congress finds the following:
(1) The National Geospatial-Intelligence Agency has struggled to identify the programs and activities of the Agency, to include significant, enduring programs determined by the Agency to be “programs of record”, comprehensively and in a fashion that enables budget auditable and oversight by the Office of the Director of National Intelligence, the Office of Management and Budget, and the congressional intelligence committees.

(2) The National Geospatial-Intelligence Agency has rebuffed repeated requests by the House Permanent Select Committee on Intelligence to furnish to such Committee the definition for the term “program of record” used by the Agency.

(b) REPORTS REQUIRED.—

(1) REPORT TO CONGRESSIONAL INTELLIGENCE COMMITTEES.—Not later than 30 days after the date of the enactment of this Act, the Director of the National Geospatial-Intelligence Agency, consistent with the protection of intelligence sources and methods, shall submit to the congressional intelligence committees a report on the programs and activities of the Agency. Such report shall include, at a minimum, the following:
(A) An identification of any definition for the term “program of record” used by the Agency during the period beginning October 1, 2017, and ending on the date of the submission of the report.

(B) A detailed description of each current program and activity of the Agency, including each current program of record of the Agency.

(C) A detailed explanation of how funding and other information relating to each such program of record or other program or activity may be located within the budget justification materials submitted to Congress.

(2) REPORT TO CONGRESSIONAL INTELLIGENCE AND DEFENSE COMMITTEES.—Not later than 30 days after the date of the enactment of this Act, the Director of the National Geospatial-Intelligence Agency, consistent with the protection of intelligence sources and methods, shall submit to the appropriate congressional committees a report on the programs and activities of the Agency that are funded in full or in part under the Military Intelligence Program. Such report shall include, at a minimum, the following:
(A) An identification of any definition for
the term “program of record” used by the
Agency during the period beginning October 1,
2017 and ending on the date of the submission
of the report.

(B) A detailed description of each current
program and activity of the Agency funded in
full or in part under the Military Intelligence
Program, including each current program of
record of the Agency funded in full or in part
under the Military Intelligence Program.

(C) A detailed explanation of how funding
and other information relating to each such
program of record or other program or activity
funded in full or in part under the Military In-
telligence Program may be located within the
budget justification materials submitted to Con-
gress.

(3) Form.—Each report under this subsection
may be submitted in classified form, but if so sub-
mitted shall include an unclassified executive sum-
mary.

(e) Appropriate Congressional Committees De-

fined.—In this section, the term “appropriate congres-
sional 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).

SEC. 707. PLAN REGARDING SOCIAL MEDIA DATA AND THREAT ANALYSIS CENTER.

(a) Plan.—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 plan to operationalize the Social Media Data and Threat Analysis Center in accordance with section 5323 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (division E of Public Law 116–92; 50 U.S.C. 3369).

(b) Elements.—The plan under subsection (a) shall include a description of how the Social Media Data and Threat Analysis Center shall—

(1) coordinate with social media companies and other public-facing internet-based platforms to determine—

(A) what categories of data and metadata are useful indicators of internet-based foreign malign influence activities; and
(B) how such data and metadata may be
shared effectively with the Center while pro-
tecting the privacy and civil liberties of United
States users of social media platforms and
other public-facing internet-based platforms;
and
(2) develop criteria under which social media
companies and other public-facing internet-based
platforms shall share indicators of internet-based
foreign malign influence activities with the Center,
including a description of—
(A) the timeliness and consistency of such
sharing of indicators;
(B) the categories of indicators to be
shared; and
(C) the protection of privacy, civil liberties,
and constitutionally protected activities of users
of social media platforms and other public-fac-
ing internet-based platforms.

SEC. 708. REPORT ON USE OF PUBLICLY AVAILABLE SO-
CIAL MEDIA INFORMATION IN PERSONNEL
VETTING DETERMINATIONS.

(a) Report.—Not later than 180 days after the date
of the enactment of this Act, the Director of National In-
telligence, in coordination with other heads of the elements
of the intelligence community that the Director determines
appropriate, and in consultation with the other principal
members of the Council, shall submit to the congressional
intelligence committees a report regarding the current and
planned use of publicly available social media information
in the personnel vetting and security clearance processes.

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

(1) A description of how departments and agen-
cies of the United States Government have imple-
mented Security Executive Agent Directive 5 titled
“Collection, Use, and Retention of Publicly Available
Social Media Information in Personnel Security
Background Investigations and Adjudications”, and
relevant agency implementing guidance, including
Department of Defense Instruction 1325.06 titled
“Handling Protest, Extremist, and Criminal Gang
Activities among Members of the Armed Forces”.

(2) A description of how the use of publicly
available social media in personnel vetting deter-
minations and security clearance investigations and
adjudications is, or will be, captured in the National
Background Investigation Services system and other
information technology systems used in the per-
sonnel vetting process.
(3) A description of how publicly available social media information is used, and will be used, in continuous vetting and security clearances processes and insider threat programs.

(4) A description of any privacy or civil liberties concerns with the use of publicly available social media information in personnel vetting or security clearance determinations, including a discussion of the risks, benefits, and drawbacks of allowing for the voluntary provision of, or voluntary access to, non-publicly available social media information in the regular course of personnel vetting and security clearance processes.

(5) A discussion of the extent to which officials and entities of the United States Government responsible for privacy and civil liberties matters, including the Chief of the Office of Civil Liberties, Privacy, and Transparency of the Office of the Director of National Intelligence and the civil liberties officers of departments and agencies of the United States Government, are involved in the development and operation of programs to use social media information in personnel vetting and security clearance processes.
(6) A discussion of any impediments, constraints, risks, or drawbacks relating to the use of publicly available social media information in personnel vetting and security clearance processes, including—

(A) challenges associated with implementation of Security Executive Agent Directive 5, Department of Defense Instruction 1325.06, and other relevant guidance;

(B) the resources required, including with respect to personnel, funding, and information systems, to gather, assess, and make use of such information; and

(C) an analysis of the costs and benefits of the use of publicly available social media information.

(7) An implementation plan for the future use of publicly available social media information, based on relevant findings under paragraphs (1) through (6).

(c) DEFINITIONS.—The terms “continuous vetting”, “Council”, and “Security Executive Agent” have the meanings given those terms in section 6601 of the Damon

Paul Nelson and Matthew Young Pollard Intelligence Au-

SEC. 709. REPORT ON STRENGTHENING WORKFORCE DIVERSITY PLANNING AND OVERSIGHT.

(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 heads of the elements of the intelligence community, shall submit to the congressional intelligence committees a report discussing steps to enhance the strategic planning for, measure the progress of, and assess barriers to workforce diversity in the intelligence community.

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

(1) A discussion of existing, updated, or new guidance requiring all elements of the intelligence community to maintain current and complete diversity strategic plans that contain specific objectives, timeframes, and responsibilities.

(2) A discussion of progress made by individual elements toward maintaining such plans.

(3) A discussion of existing, updated, or new guidance to ensure individual elements develop performance measures to assess the contribution of ac-
tivities toward achieving diversity goals and overall progress.

(4) A discussion of progress made by individual elements toward developing measures to assess progress toward achieving diversity management efforts.

(5) A discussion of existing, updated, or new guidance ensuring that each element routinely identifies and takes steps toward eliminating barriers to workforce diversity.

(6) A discussion of steps taken by the Director to ensure that individual elements are routinely completing required assessments to identify and eliminate barriers to diversity.

(7) A discussion of steps taken by the Director to establish specific implementation objectives and timeframes for the elements that support intelligence community-wide diversity goals to ensure the elements are held accountable for making progress.

SEC. 710. REPORT ON IMPROVING OPPORTUNITIES FOR WOMEN AND MINORITIES FOR PROMOTIONS IN THE INTELLIGENCE COMMUNITY.

(a) Report.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence, acting through the Chief Human Capital Offi-
cer of the Intelligence Community, and in consultation
with other heads of the elements of the intelligence com-
munity, shall submit to the congressional intelligence com-
mittees a consolidated report on specific steps taken by
each element of the intelligence community to—

(1) enhance opportunities for women and mi-
norities for promotions across all mission categories
of the intelligence community; and

(2) reduce the gap among gender and racial
and ethnic categories at senior levels of the intel-
ligence community.

(b) STRATEGIC PLAN.—The report under subsection
(a) shall contain a strategic plan from each element of
the intelligence community on the following:

(1) Overcoming any barriers or obstacles identi-
ified in the report.

(2) Proposing new or enhanced mentoring pro-
grams or similar workplace forums to support
women and minority officers of the intelligence com-
munity who are interested in or may qualify for po-
tential promotion opportunities or similar career ad-
vancements.

(3) Recommending additional steps and initia-
tives to achieve diversity among senior roles in the
intelligence community.
(4) Addressing gaps in relevant tools, resources, or authorities.

(c) Supplement Not Supplant.—The report under subsection (a) shall supplement the annual report required under 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)).

SEC. 711. REPORT ON TRANSITION OF NATIONAL RECONNAISSANCE OFFICE TO DIGITAL ENGINEERING ENVIRONMENT.

(a) Findings.—Congress finds the following:

(1) Potential foreign adversaries are outpacing the United States in the fielding of new generations of space systems that dull the edge the United States has enjoyed in space.

(2) A digital engineering environment, also known as digital systems engineering, reduces the time to field new space systems.

(3) Digital engineering environment tools enable the rapid iterations of requirements and architectures into digital system depictions capable of use by private industry to further the design and development of space systems.
(b) SENSE OF CONGRESS.—It is the sense of Congress that, to maintain a competitive advantage in space, the National Reconnaissance Office should transition to a digital engineering environment by not later than 3 years after the date of the enactment of this Act.

(e) REPORT.—

(1) SUBMISSION.—Not later than 180 days after the date of the enactment of this Act, the Director of the National Reconnaissance Office shall submit to the appropriate congressional committees a report that contains the following:

(A) A plan for the transition of the National Reconnaissance Office to a digital engineering environment.

(B) An identification of the date by which such transition shall be completed.

(C) A description of the metrics the Director plans to use to measure progress made with respect to such transition and resulting efficiencies gained.

(D) A description of the initial pilot programs of the National Reconnaissance Office relating to digital engineering and the plans to expand such pilot programs in scale and scope.
with respect to acquisition carried out under such pilot programs.

(E) A description of any training requirements or certifications necessary to advance a digital engineering environment within the National Reconnaissance Office.

(F) A description of how the Director plans to incorporate input and best practices from private industry to facilitate and accelerate the transition of the National Reconnaissance Office to a digital engineering environment.

(2) FORM.—The report under paragraph (1) 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 congressional defense committees (as defined in section 101(a)(16) of title 10, United States Code).
SEC. 712. REPORT ON DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE ENTERPRISE.

(a) Report on Intelligence Activities.—Consistent with section 501 of the National Security Act of 1947 (50 U.S.C. 3091), not later than 150 days after the date of the enactment of this Act, the Chief Intelligence Officer of the Department of Homeland Security shall submit to the appropriate congressional committees a report that includes the following:

(1) A comprehensive account of any intelligence activity conducted during the period beginning on January 1, 2018, and ending on the date of the report, by any component of the Department of Homeland Security intelligence enterprise.

(2) With respect to each such intelligence activity, a description of the activity, including, at a minimum, a description of—

(A) the nature of the activity;

(B) the component undertaking the activity;

(C) the legal authority for such activity;

and

(D) the source of funding for such activity.

(3) A description of any finished intelligence product, or intelligence information report, produced or contributed to by a component of the Department...
of Homeland Security intelligence enterprise during
the period specified in paragraph (1).

(4) An identification of any external or internal
guidelines, policies, processes, practices, or programs
governing the collection, retention, analysis, or dis-
semination by such a component of information re-
garding United States citizens, lawful permanent
residents of the United States, or individuals located
within the United States.

(b) FORM.—The report under subsection (a) may be
submitted in classified form.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMIT-
TEES.—The term “appropriate congressional com-
mittees” means the following:

(A) The congressional intelligence commit-
tees.

(B) The Committee on Homeland Security
of the House of Representatives.

(C) The Committee on Homeland Security
and Governmental Affairs of the Senate.

(2) DEPARTMENT OF HOMELAND SECURITY IN-
TELLIGENCE ENTERPRISE.—The term “Department
of Homeland Security intelligence enterprise” means
the primary mechanism for the integration and man-
agement of the intelligence programs, projects, and activities of the Department of Homeland Security and includes the following components:

(A) The Cybersecurity and Infrastructure Security Agency.

(B) The Federal Emergency Management Agency.

(C) The Transportation Security Administration.

(D) The United States Citizenship and Immigration Services.

(E) The United States Customs and Border Protection.

(F) The United States Immigration and Customs Enforcement.

SEC. 713. REPORT ON DECLASSIFICATION EFFORTS OF CENTRAL INTELLIGENCE AGENCY.

Not later than 270 days after the date of the enactment of this Act, the Inspector General of the Central Intelligence Agency shall submit to the congressional intelligence committees a report on the declassification efforts of the Central Intelligence Agency. Such report shall include—

(1) an identification of the resources that are dedicated to such efforts; and
(2) an assessment as to whether such resources are sufficient.

SEC. 714. REPORT ON NATIONAL SPACE INTELLIGENCE CENTER.

(a) REPORT.—Not later than March 1, 2023, the Director of National Intelligence, in coordination with the Chief of Space Operations, shall submit to the appropriate congressional committees a report on the National Space Intelligence Center.

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

(1) A description of the status of the National Space Intelligence Center since the activation of the Center and the implications of the Center being aligned under a Field Command rather than a field operating agency aligned to the Director of Intelligence, Surveillance, and Reconnaissance of the Space Force.

(2) A review of the ability of the Center to address the full set of national space intelligence analytical demands (including with respect to acquisition and operational mission requirements of the Space Force, the Department of Defense, the intelligence community, and other national customers)
while being assigned as a subordinate to Space Operations Command, a Field Command, including—

(A) an assessment of the ability of the Center to respond to the broadest space intelligence requirements as compared to a service specific need; and

(B) a review specifically addressing any perceived mission misalignment, potential mitigating measures, or other structural organization concerns.

(3) An assessment of—

(A) the current resourcing posture, including any additional personnel required as a result of subordination to a Field Command; and

(B) the resourcing posture if the Center were aligned to the Director of Intelligence, Surveillance, and Reconnaissance of the Space Force as described in paragraph (1).

(4) Lessons learned since unit activation, including with respect to—

(A) organizational efficiencies and inefficiencies;

(B) financial implications;

(C) organizational redundancy;
(D) parity mismatch and synergies with other service intelligence centers; and

(E) lessons learned through comparisons to other service intelligence centers organized as a field operating agency and aligned under the senior intelligence officer of the respective Armed Force.

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

(d) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term “appropriate congressional committees” means the following:

(1) The congressional intelligence committees.

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

SEC. 715. REPORT ON IMPLEMENTATION OF EXECUTIVE ORDER 13556, REGARDING CONTROLLED UNCLASSIFIED INFORMATION.

(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 coordination with the heads of other elements of the intelligence community, shall submit
to the congressional intelligence committees a report on
the implementation by the intelligence community of Exec-
utive Order 13556, regarding controlled unclassified infor-
mation.

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

(1) during the period when the National Secu-

rity Council conducts a review of the dissemination
controls with respect to national security informa-
tion, the elements of the intelligence should pause
the implementation of Executive Order 13556; and

(2) Executive Order 13556 should be repealed.

SEC. 716. COMPTROLLER GENERAL OF THE UNITED
STATES COMPILATION OF UNIDENTIFIED
AEROSPACE-UNDERSEA PHENOMENA
RECORDS.

(a) Compilation Required.—Not later than 1 year
after the date of the enactment of this Act, the Com-
troller General of the United States shall—

(1) commence a review of the records and docu-
ments of the intelligence community, oral history
interviews, open source analytic analysis, interviews
of current and former government officials, classified
and unclassified national archives (including those
records any third party obtained pursuant to section
552 of title 5, United States Code (commonly known as the “Freedom of Information Act” or “FOIA”), and such other relevant historical sources as the Comptroller General considers appropriate; and

(2) for the period beginning on January 1, 1947, and ending on the date on which the Comptroller General completes activities under this subsection, compile and itemize a complete historical record of the intelligence community’s involvement with unidentified aerospace-undersea phenomena, including successful or unsuccessful efforts to identify and track unidentified aerospace-undersea phenomena, efforts to recover or transfer related technologies to United States-based industry or National Laboratories, and any intelligence community efforts to obfuscate, manipulate public opinion, hide, or otherwise provide unclassified or classified misinformation about unidentified aerospace-undersea phenomena or related activities, based on the review conducted under paragraph (1).

(b) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date on which the Comptroller General completes the compilation and itemization required by subsection (a)(2), the Comptroller General shall
submit to Congress a report summarizing the historical record described in such subsection.

(2) RESOURCES.—The report submitted under paragraph (1) shall include citations to the resources relied upon and instructions as to how the resources can be accessed.

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

(c) COOPERATION OF INTELLIGENCE COMMUNITY.—

The heads of elements of the intelligence community whose participation the Comptroller General determines necessary to carry out subsections (a) and (b), including the Director of National Intelligence, the Under Secretary of Defense for Intelligence and Security, and the Director of the Unidentified Aerospace Undersea Phenomena Joint Program Office, shall fully cooperate with the Comptroller General and provide to the Comptroller General such information as the Comptroller General determines necessary to carry out such subsections.

(d) ACCESS TO RECORDS OF THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION.—The Archivist of the United States shall make available to the Comptroller General such information maintained by the National Archives and Records Administration, including
classified information, as the Comptroller General considers necessary to carry out subsections (a) and (b).

SEC. 717. NATIONAL MUSEUM OF INTELLIGENCE AND SPECIAL OPERATIONS.

(a) RECOGNITION.—The privately-funded museum to honor the intelligence community and special operations forces that is planned to be constructed in Ashburn, Virginia, may be recognized, upon completion, as the “National Museum of Intelligence and Special Operations”.

(b) PURPOSES.—The purpose of recognizing the National Museum of Intelligence and Special Operations under subsection (a) are to—

(1) commemorate the members of the intelligence community and special operations forces who have been critical to securing the Nation against enemies of the United States for nearly a century;

(2) preserve and support the historic role that the intelligence community and special operations forces have played, and continue to play, both in secrecy as well as openly, to keep the United States and its values and way of life secure; and

(3) foster a greater understanding of the intelligence community and special operations forces to ensure a common understanding, dispel myths, recognize those who are not otherwise able to be pub-
licely recognized, and increase science, technology, en-
gineering, and math education through museum pro-
grams designed to promote more interest and great-
er diversity in recruiting with respect to the intel-
ligence and special operations career field.

SEC. 718. TECHNICAL CORRECTIONS.

(a) NATIONAL SECURITY ACT OF 1947.—The Na-
tional Security Act of 1947 (50 U.S.C. 3001 et seq.), as
amended by section 511, is further amended as follows:

(1) In section 105(a)(1) (50 U.S.C.
3038(a)(1)), by striking “chairman” and inserting
“Chairman”.

(2) In section 113B(b) (50 U.S.C. 3049a(b))—

(A) in paragraph (1)(A), by striking
“Under Secretary of Defense for Intelligence”
and inserting “Under Secretary of Defense for
Intelligence and Security”; and

(B) in paragraph (4), by striking “section
226 of the Homeland Security Act of 2002 (6
U.S.C. 147)” and inserting “section 2208 of
658)”.

(3) In section 118(a) (50 U.S.C. 3055(a)), by
striking “a annual” and inserting “an annual”.

285
(4) In section 301(j) (50 U.S.C. 3071(j)), by striking “and includes” and inserting “and including”.

(5) In section 506G(e) (50 U.S.C. 3103(c)), by striking “pursuant section” and inserting “pursuant to section”.

(6) In section 507(a)(1) (50 U.S.C. 3106(a)(1)), by striking “Generals” and inserting “General”.

(7) In section 1024(g)(7)(A) (50 U.S.C. 3224(g)(7)(A)), by striking “places” and inserting “place”.

(8) In section 1104(b)(1)(B) (50 U.S.C. 3234(b)(1)(B)), by striking the period at the end and inserting a semicolon.

(b) DAMON PAUL NELSON AND MATTHEW YOUNG


(1) in section 5704(b)(1) (50 U.S.C. 3334b(b)(1)), by striking “, and subject to paragraph (3)”;

23456789
(2) in section 6316 (50 U.S.C. 3334b note), by striking “congressional committees” and inserting “congressional intelligence committees”; and

(3) in section 6604 (50 U.S.C. 3352e), by striking “subsections (b) and (c)” both places it appears and inserting “subsections (a) and (b)”.

(e) INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2012.—Section 309(a)(5) of the Intelligence Authorization Act for Fiscal Year 2012 (50 U.S.C. 3334e) is amended by striking “section 3542(b)” and inserting “section 3552”.

(d) PUBLIC INTEREST DECLASSIFICATION ACT OF 2000.—The Public Interest Declassification Act of 2000 (50 U.S.C. 3355 et seq.) is amended—

(1) in section 703(a)(2) (50 U.S.C. 3355a(a)(2)), by striking “Executive Order 12958” and inserting “Executive Order 13526”;

(2) in section 704(e)(3) (50 U.S.C. 3355b(e)(3)), by striking the comma before “shall”;

(3) in section 705(e) (50 U.S.C. 3355e(e)), by striking “section 103(c)(6) of the National Security Act of 1947 (50 U.S.C. 403–3(c)(6))” and inserting “section 102A(i) of the National Security Act of 1947 (50 U.S.C. 3024(i))”; and
(4) in section 706 (50 U.S.C. 3355d), by striking “Executive Order No. 12958” both places it appears and inserting “Executive Order 13526”.