116TH CONGRESS
1st Session

HOUSE OF REPRESENTATIVES

REPT. 116–151
Part 1

DAMON PAUL NELSON AND MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018, 2019, AND 2020

R E P O R T

OF THE

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

JULY 11, 2019.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

DAMON PAUL NELSON AND MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018, 2019, AND 2020

116TH CONGRESS
1st Session

HOUSE OF REPRESENTATIVES

REPT. 116–151
Part 1

DAMON PAUL NELSON AND MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018, 2019, AND 2020

R E P O R T

OF THE

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

JULY 11, 2019.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PUBLISHING OFFICE

37–060 WASHINGTON : 2019

116TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 116–151
Part 1

DAMON PAUL NELSON AND MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018, 2019, AND 2020

JULY 11, 2019.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

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

R E P O R T

[To accompany H.R. 3494]

[Including cost estimate of the Congressional Budget Office]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 3494) to authorize appropriations for fiscal year 2020 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill as amended do pass.

The amendments are as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020".

SEC. 2. DIVISIONS AND TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized into two divisions as follows:
(1) Division A—Intelligence Authorizations for Fiscal Year 2020.
(2) Division B—Intelligence Authorizations for Fiscal Years 2018 and 2019.

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

SEC. 3. DEFINITIONS.

In this Act:

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

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

DIVISION A—INTELLIGENCE AUTHORIZATIONS FOR FISCAL YEAR 2020

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2020 for the conduct of the intelligence and intelligence-related activities of the following elements of the United States Government:

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

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

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

(b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AUTHORIZATIONS.—

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

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

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

(A) as provided in section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 3306(a));
(B) to the extent necessary to implement the budget; or
(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2020 the sum of $565,637,000.

(b) CLASSIFIED AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2020 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a).

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability fund $514,000,000 for fiscal year 2020.

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. PAID PARENTAL LEAVE.

(a) PURPOSE.—The purpose of this section is to—

(1) help the intelligence community recruit and retain a dynamic, multi-talented, and diverse workforce capable of meeting the security goals of the United States; and

(2) establish best practices and processes for other elements of the Federal Government seeking to pursue similar policies.

(b) AUTHORIZATION OF PAID PARENTAL LEAVE FOR INTELLIGENCE COMMUNITY EMPLOYEES.—

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

"SEC. 305. PAID PARENTAL LEAVE.

"(a) PAID PARENTAL LEAVE.—Notwithstanding any other provision of law, a civilian employee of an element of the intelligence community shall have available a total of 12 administrative workweeks of paid parental leave in the event of the birth of a son or daughter of the employee, or placement of a son or daughter with the employee for adoption or foster care in order to care for such son or daughter. Such paid parental leave shall be used during the 12-month period beginning on the date of the birth or placement. Nothing in this section shall be construed to modify or otherwise affect the eligibility of an employee of an element of the intelligence community for benefits relating to leave under any other provision of law.

"(b) TREATMENT OF PARENTAL LEAVE REQUEST.—Notwithstanding any other provision of law—

"(1) an element of the intelligence community shall accommodate an employee's leave request under subsection (a), including a request to use such leave intermittently or to create a reduced work schedule, to the extent that the requested leave schedule does not unduly disrupt operations; and

"(2) to the extent that an employee's requested leave described in paragraph (1) arises out of medical necessity related to a serious health condition connected to the birth of a son or daughter, the employing element shall handle the scheduling consistent with the treatment of employees who are using leave under subparagraph (C) or (D) of section 6382(a)(1) of title 5, United States Code.

"(c) RULES RELATING TO PAID LEAVE.—Notwithstanding any other provision of law—

"(1) an employee may not be required to first use all or any portion of any unpaid leave available to the employee before being allowed to use the paid parental leave described in subsection (a); and

"(2) paid parental leave under subsection (a)—

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

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

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

"(D) may be granted only to the extent that the employee does not receive a total of more than 12 weeks of paid parental leave in any 12-month period beginning on the date of a birth or placement;

"(E) may not be granted—

"(i) in excess of a lifetime aggregate total of 30 administrative workweeks based on placements of a foster child for any individual employee; or

"(ii) in connection with temporary foster care placements expected to last less than 1 year;

"(F) may not be granted for a child being placed for foster care or adoption if such leave was previously granted to the same employee when the same child was placed with the employee for foster care in the past;

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

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

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

"(1) processes and procedures for implementing the paid parental leave policies under subsections (a) through (c);

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

"(3) all costs or operational expenses associated with the implementation of subsections (a) through (c).

"(e) DIRECTIVE.—Not later than 180 days after the Director of National Intelligence submits the implementation plan under subsection (d), the Director of National Intelligence shall issue a written directive to implement this section, which directive shall take effect on the date of issuance.

"(f) ANNUAL REPORT.—The Director of National Intelligence shall submit to the congressional intelligence committees an annual report that—

"(1) details the number of employees of each element of the intelligence community who applied for and took paid parental leave under subsection (a) during the year covered by the report;

"(2) details the number of—

"(A) employees of each element of the intelligence community stationed abroad who applied for and took paid parental leave under subsection (a) during the year covered by the report; and

"(B) employees of each element of the intelligence community stationed abroad who applied for paid parental leave but such application was not granted because of an undue impact on operations as specified in subsection (b)(1); and

"(3) includes updates on major implementation challenges or costs associated with paid parental leave.

"(g) DEFINITION OF SON OR DAUGHTER.—For purposes of this section, the term 'son or daughter' has the meaning given the term in section 6381 of title 5, United States Code.".

(2) CLERICAL AMENDMENT.—The table of contents in the matter preceding section 2 of the National Security Act of 1947 (50 U.S.C. 3002) is amended by inserting after the item relating to section 304 the following:

"Sec. 305. Paid parental leave.".

(c) APPLICABILITY.—Section 305 of the National Security Act of 1947, as added by subsection (b), shall apply with respect to leave taken in connection with the birth or placement of a son or daughter that occurs on or after the date on which the

Director of National Intelligence issues the written directive under subsection (e) of such section 305.

SEC. 304. UNFUNDED REQUIREMENTS OF THE INTELLIGENCE COMMUNITY.

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

"SEC. 512. UNFUNDED PRIORITIES OF THE INTELLIGENCE COMMUNITY.

"(a) BRIEFINGS.—Upon the request of an appropriate congressional committee, the Director of National Intelligence shall provide to the committee a briefing on the unfunded priorities of an element of the intelligence community.

"(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 Appropriations of the House of Representatives and the Senate.

"(2) UNFUNDED PRIORITY.—The term 'unfunded priority', in the case of a fiscal year, means a program, activity, or other initiative of an element of the intelligence community that—

"(A) was submitted by the head of the element to the Director of National Intelligence in the budget proposal for the element for that fiscal year, but was not included by the Director in the consolidated budget proposal submitted to the President for that fiscal year; or

"(B) was submitted by the Director in the consolidated budget proposal submitted to the President for that fiscal year, but was not included in the budget of the President submitted to Congress for that fiscal year pursuant to section 1105 of title 31, United States Code.".

(b) CLERICAL AMENDMENT.—The table of sections in the first section of such Act is amended by inserting after the item relating to section 511 the following new item:

"Sec. 512. Unfunded priorities of the intelligence community.".

SEC. 305. EXTENDING THE INTELLIGENCE IDENTITIES PROTECTION ACT OF 1982.

Section 605(4) of the National Security Act of 1947 (50 U.S.C. 3126(4)) is amended—

(1) in subparagraph (A)—

(A) by striking clause (ii);

(B) in clause (i), by striking ", and" and inserting ";"; and

(C) by striking "agency—" and all that follows through "whose identity" and inserting "agency whose identity"; and

(2) in subparagraph (B)(i), by striking "resides and acts outside the United States" and inserting "acts".

SEC. 306. INTELLIGENCE COMMUNITY PUBLIC-PRIVATE TALENT EXCHANGE.

(a) POLICIES, PROCESSES, AND PROCEDURES REQUIRED.—Not later than 270 days after the date of the enactment of this Act, the Director of National Intelligence shall develop policies, processes, and procedures to facilitate the rotation of personnel of the intelligence community to the private sector, and personnel from the private sector to the intelligence community.

(b) DETAIL AUTHORITY.—Under policies developed by the Director pursuant to subsection (a), pursuant to a written agreement with a private-sector organization, and with the consent of the employee, a head of an element of the intelligence community may arrange for the temporary detail of an employee of such element to such private-sector organization, or from such private-sector organization to such element under this section.

(c) AGREEMENTS.—

(1) IN GENERAL.—A head of an element of the intelligence community exercising the authority of the head under subsection (a) shall provide for a written agreement among the element of the intelligence community, the private-sector organization, and the employee concerned regarding the terms and conditions of the employee's detail under this section. The agreement—

(A) shall require that the employee of the element, upon completion of the detail, serve in the element, or elsewhere in the civil service if approved by the head of the element, for a period that is at least equal to the length of the detail;

(B) shall provide that if the employee of the element fails to carry out the agreement, such employee shall be liable to the United States for payment of all non-salary and benefit expenses of the detail, unless that failure

was for good and sufficient reason, as determined by the head of the element;

(C) shall contain language informing such employee of the prohibition on sharing, using, or otherwise improperly handling classified of unclassified non-public information for the benefit or advantage of the private-sector organization;

(D) shall contain language governing the handling of classified information by such employee during the detail; and

(E) shall contain language requiring the employee to acknowledge the obligations of the employee under section 1905 of title 18, United States Code.

(2) AMOUNT OF LIABILITY.—An amount for which an employee is liable under paragraph (1) shall be treated as a debt due the United States.

(3) WAIVER.—The head of an element of the intelligence community may waive, in whole or in part, collection of a debt described in paragraph (2) based on a determination that the collection would be against equity and good conscience and not in the best interests of the United States, after taking into account any indication of fraud, misrepresentation, fault, or lack of good faith on the part of the employee.

(d) TERMINATION.—A detail under this section may, at any time and for any reason, be terminated by the head of the element of the intelligence community concerned or the private-sector organization concerned.

(e) DURATION.—

(1) IN GENERAL.—A detail under this section shall be for a period of not less than 3 months and not more than 2 years, renewable up to a total of 3 years.

(2) LONGER PERIODS.—A detail under this section may be for a period in excess of 2 years, but not more than 3 years, if the head of the element making the detail determines that such detail is necessary to meet critical mission or program requirements.

(3) LIMITATION.—No employee of an element of the intelligence community may be detailed under this section for more than a total of 5 years, inclusive of all such details.

(f) STATUS OF FEDERAL EMPLOYEES DETAILED TO PRIVATE-SECTOR ORGANIZATIONS.—

(1) IN GENERAL.—An employee of an element of the intelligence community who is detailed to a private-sector organization under this section shall be considered, during the period of detail, to be on a regular work assignment in the element. The written agreement established under subsection (c)(1) shall address the specific terms and conditions related to the employee's continued status as a Federal employee.

(2) REQUIREMENTS.—In establishing a temporary detail of an employee of an element of the intelligence community to a private-sector organization, the head of the element shall—

(A) certify that the temporary detail of such employee shall not have an adverse or negative impact on mission attainment or organizational capabilities associated with the detail; and

(B) in the case of an element of the intelligence community in the Department of Defense, ensure that the normal duties and functions of such employees are not, as a result of and during the course of such temporary detail, performed or augmented by contractor personnel in violation of the provisions of section 2461 of title 10, United States Code.

(g) TERMS AND CONDITIONS FOR PRIVATE-SECTOR EMPLOYEES.—An employee of a private-sector organization who is detailed to an element of the intelligence community under this section—

(1) shall continue to receive pay and benefits from the private-sector organization from which such employee is detailed and shall not receive pay or benefits from the element, except as provided in paragraph (2);

(2) is deemed to be an employee of the element for the purposes of—

(A) chapters 73 and 81 of title 5, United States Code;

(B) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18, United States Code;

(C) sections 1343, 1344, and 1349(b) of title 31, United States Code;

(D) chapter 171 of title 28, United States Code (commonly known as the "Federal Tort Claims Act") and any other Federal tort liability statute;

(E) the Ethics in Government Act of 1978 (5 U.S.C. App.); and

(F) chapter 21 of title 41, United States Code;

(3) may perform work that is considered inherently governmental in nature only when requested in writing by the head of the element;

(4) may not be used to circumvent any limitation or restriction on the size of the workforce of the element;

(5) shall be subject to the same requirements applicable to an employee performing the same functions and duties proposed for performance by the private sector employee; and

(6) in the case of an element of the intelligence community in the Department of Defense, may not be used to circumvent the provisions of section 2461 of title 10, United States Code.

(h) PROHIBITION AGAINST CHARGING CERTAIN COSTS TO THE FEDERAL GOVERNMENT.—A private-sector organization may not charge an element of the intelligence community or any other agency of the Federal Government, as direct costs under a Federal contract, the costs of pay or benefits paid by the organization to an employee detailed to an element of the intelligence community under this section for the period of the detail and any subsequent renewal periods.

(i) ADDITIONAL ADMINISTRATIVE MATTERS.—In carrying out this section, the Director, pursuant to procedures developed under subsection (a)—

(1) shall, to the degree practicable, ensure that small business concerns are represented with respect to details authorized by this section;

(2) may, notwithstanding any other provision of law, establish criteria for elements of the intelligence community to use appropriated funds to reimburse small business concerns for the salaries and benefits of its employees during the periods when the small business concern agrees to detail its employees to the intelligence community under this section;

(3) shall take into consideration the question of how details under this section might best be used to help meet the needs of the intelligence community, including with respect to the training of employees;

(4) shall take into consideration areas of private-sector expertise that are critical to the intelligence community; and

(5) shall establish oversight mechanisms to determine whether the public-private exchange authorized by this section improves the efficiency and effectiveness of the intelligence community.

(j) DEFINITIONS.—In this section:

(1) DETAIL.—The term "detail" means, as appropriate in the context in which such term is used—

(A) the assignment or loan of an employee of an element of the intelligence community to a private-sector organization without a change of position from the intelligence community element that employs the individual; or

(B) the assignment or loan of an employee of a private-sector organization to an element of the intelligence community without a change of position from the private-sector organization that employs the individual.

(2) PRIVATE-SECTOR ORGANIZATION.—The term "private-sector organization" means—

(A) a for-profit organization; or

(B) a not-for-profit organization.

(3) SMALL BUSINESS CONCERN.—The term "small business concern" has the meaning given such term in section 3703(e)(2) of title 5, United States Code.

SEC. 307. ASSESSMENT OF CONTRACTING PRACTICES TO IDENTIFY CERTAIN SECURITY AND COUNTERINTELLIGENCE CONCERNS.

(a) ASSESSMENT.—

(1) CONTRACTING PRACTICES.—The Director of National Intelligence shall conduct an assessment of the authorities, policies, processes, and standards used by the elements of the intelligence community to ensure that the elements appropriately weigh security and counterintelligence risks in awarding a contract to a contractor that—

(A) carries out any joint research and development activities with a covered foreign country; or

(B) performs any contract or other agreement entered into with a covered foreign country.

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

(A) An assessment of whether the authorities, policies, processes, and standards specified in paragraph (1) sufficiently identify security and counterintelligence concerns.

(B) Identification of any authority gaps in such authorities, policies, processes, and standards that prevent the intelligence community from considering the activities specified in subparagraphs (A) and (B) of paragraph (1) when evaluating offers for a contract.

(3) CONSULTATION.—In carrying out paragraph (1), the Director shall consult with each head of an element of the intelligence community.

(b) REPORT.—

(1) REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees a report on the assessment under subsection (a)(1).

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

(A) The assessment under subsection (a)(1).

(B) An identification of any known contractors that have—

(i) carried out activities specified in subparagraphs (A) and (B) of subsection (a)(1); and

(ii) submitted an offer for a contract with an element of the intelligence community.

(C) A description of the steps that the Director and the heads of the elements of the intelligence community took to identify contractors under subparagraph (B).

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

(c) COVERED FOREIGN COUNTRY DEFINED.—In this section, the term "covered foreign country" means the government, or any entity affiliated with the military or intelligence services of, the following foreign countries:

(1) The People's Republic of China.

(2) The Russian Federation.

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

(4) The Islamic Republic of Iran.

SEC. 308. REQUIRED COUNTERINTELLIGENCE BRIEFINGS AND NOTIFICATIONS.

(a) FOREIGN COUNTERINTELLIGENCE AND CYBERSECURITY THREATS TO FEDERAL ELECTION CAMPAIGNS.—

(1) REPORTS REQUIRED.—

(A) IN GENERAL.—As provided in subparagraph (B), for each Federal election, the Director of National Intelligence, in coordination with the Under Secretary of Homeland Security for Intelligence and Analysis and the Director of the Federal Bureau of Investigation, shall make publicly available on an Internet website an advisory report on foreign counterintelligence and cybersecurity threats to election campaigns for Federal offices. Each such report shall include, consistent with the protection of sources and methods, each of the following:

(i) A description of foreign counterintelligence and cybersecurity threats to election campaigns for Federal offices.

(ii) A summary of best practices that election campaigns for Federal offices can employ in seeking to counter such threats.

(iii) An identification of any publicly available resources, including United States Government resources, for countering such threats.

(B) SCHEDULE FOR SUBMITTAL.—A report under this subsection shall be made available as follows:

(i) In the case of a report regarding an election held for the office of Senator or Member of the House of Representatives during 2018, not later than the date that is 60 days after the date of the enactment of this Act.

(ii) In the case of a report regarding an election for a Federal office during any subsequent year, not later than the date that is 1 year before the date of the election.

(C) INFORMATION TO BE INCLUDED.—A report under this subsection shall reflect the most current information available to the Director of National Intelligence regarding foreign counterintelligence and cybersecurity threats.

(2) TREATMENT OF CAMPAIGNS SUBJECT TO HEIGHTENED THREATS.—If the Director of the Federal Bureau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis jointly determine that an election campaign for Federal office is subject to a heightened foreign counterintelligence or cybersecurity threat, the Director and the Under Secretary, consistent with the protection of sources and methods, may make available additional information to the appropriate representatives of such campaign.

(b) BRIEFINGS ON COUNTERINTELLIGENCE ACTIVITIES OF THE FEDERAL BUREAU OF INVESTIGATION.—

(1) IN GENERAL.—Title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.), as amended by section 304, is further amended by adding at the end the following new section:

"SEC. 513. BRIEFINGS AND NOTIFICATIONS ON COUNTERINTELLIGENCE ACTIVITIES OF THE FEDERAL BUREAU OF INVESTIGATION.

"(a) QUARTERLY BRIEFINGS.—In addition to, and without any derogation of, the requirement under section 501 to keep the congressional intelligence committees fully and currently informed of the intelligence and counterintelligence activities of the United States, not less frequently than once each quarter, the Director of the Federal Bureau of Investigation shall provide to the congressional intelligence committees a briefing on the counterintelligence activities of the Federal Bureau of Investigation. Such briefings shall include, at a minimum, an overview and update of—

"(1) the counterintelligence posture of the Bureau;

"(2) counterintelligence investigations; and

"(3) any other information relating to the counterintelligence activities of the Bureau that the Director determines necessary.

"(b) NOTIFICATIONS.—In addition to the quarterly briefings under subsection (a), the Director of the Federal Bureau of Investigation shall promptly notify the congressional intelligence committees of any counterintelligence investigation carried out by the Bureau with respect to any counterintelligence risk or threat that is related to an election or campaign for Federal office.

"(c) GUIDELINES.—

"(1) DEVELOPMENT AND CONSULTATION.—The Director shall develop guidelines governing the scope of the briefings provided under subsection (a), the notifications provided under subsection (b), and the information required by section 308(a)(2) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020. The Director shall consult the congressional intelligence committees during such development.

"(2) SUBMISSION.—The Director shall submit to the congressional intelligence committees—

"(A) the guidelines under paragraph (1) upon issuance; and

"(B) any updates to such guidelines by not later than 15 days after making such update.".

(2) CLERICAL AMENDMENT.—The table of contents at the beginning of such Act, as amended by section 304, is further amended by inserting after the item relating to section 512 the following new item:

"Sec. 513. Briefings and notifications on counterintelligence activities of the Federal Bureau of Investigation.".

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SEC. 401. ESTABLISHMENT OF CLIMATE SECURITY ADVISORY COUNCIL.

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

"SEC. 120. CLIMATE SECURITY ADVISORY COUNCIL.

"(a) ESTABLISHMENT.—The Director of National Intelligence shall establish a Climate Security Advisory Council for the purpose of—

"(1) assisting intelligence analysts of various elements of the intelligence community with respect to analysis of climate security and its impact on the areas of focus of such analysts;

"(2) facilitating coordination between the elements of the intelligence community and elements of the Federal Government that are not elements of the intelligence community in collecting data on, and conducting analysis of, climate change and climate security; and

"(3) ensuring that the intelligence community is adequately prioritizing climate change in carrying out its activities.

"(b) COMPOSITION OF COUNCIL.—

"(1) MEMBERS.—The Council shall be composed of the following individuals appointed by the Director of National Intelligence:

"(A) An appropriate official from the National Intelligence Council, who shall chair the Council.

"(B) The lead official with respect to climate and environmental security analysis from—

"(i) the Central Intelligence Agency;

"(ii) the Bureau of Intelligence and Research of the Department of State;

"(iii) the National Geospacial-Intelligence Agency;

"(iv) the Office of Intelligence and Counterintelligence of the Department of Energy;

"(v) the Office of the Under Secretary of Defense for Intelligence; and

"(vi) the Defense Intelligence Agency.

"(C) Three appropriate officials from elements of the Federal Government that are not elements of the intelligence community that are responsible for—

"(i) providing decision-makers with a predictive understanding of the climate;

"(ii) making observations of our Earth system that can be used by the public, policymakers, and to support strategic decisions; or

"(iii) coordinating Federal research and investments in understanding the forces shaping the global environment, both human and natural, and their impacts on society.

"(D) Any other officials as the Director of National Intelligence or the chair of the Council may determine appropriate.

"(2) RESPONSIBILITIES OF CHAIR.—The chair of the Council shall have responsibility for—

"(A) identifying agencies to supply individuals from elements of the Federal Government that are not elements of the intelligence community;

"(B) securing the permission of the relevant agency heads for the participation of such individuals on the Council; and

"(C) any other duties that the Director of National Intelligence may direct.

"(c) DUTIES AND RESPONSIBILITIES OF COUNCIL.—The Council shall carry out the following duties and responsibilities:

"(1) To meet at least quarterly to—

"(A) exchange appropriate data between elements of the intelligence community and elements of the Federal Government that are not elements of the intelligence community;

"(B) discuss processes for the routine exchange of such data and implementation of such processes; and

"(C) prepare summaries of the business conducted at each meeting.

"(2) To assess and determine best practices with respect to the analysis of climate security, including identifying publicly available information and intelligence acquired through clandestine means that enables such analysis.

"(3) To assess and identify best practices with respect to prior efforts of the intelligence community to analyze climate security.

"(4) To assess and describe best practices for identifying and disseminating climate security indicators and warnings;

"(5) To recommend methods of incorporating analysis of climate security and the best practices identified under paragraphs (2) through (4) into existing analytic training programs.

"(6) To consult, as appropriate, with other elements of the intelligence community that conduct analysis of climate change or climate security and elements of the Federal Government that are not elements of the intelligence community that conduct analysis of climate change or climate security, for the purpose of sharing information about ongoing efforts and avoiding duplication of existing efforts.

"(7) To work with elements of the intelligence community that conduct analysis of climate change or climate security and elements of the Federal Government that are not elements of the intelligence community that conduct analysis of climate change or climate security—

"(A) to exchange appropriate data between such elements, establish processes, procedures and practices for the routine exchange of such data, discuss the implementation of such processes; and

"(B) to enable and facilitate the sharing of findings and analysis between such elements.

"(8) To assess whether the elements of the intelligence community that conduct analysis of climate change or climate security may inform the research direction of academic work and the sponsored work of the United States Government.

"(9) At the discretion of the chair of the Council, to convene conferences of analysts and non-intelligence community personnel working on climate change or climate security on subjects that the chair shall direct.

"(d) SUNSET.—The Council shall terminate on the date that is 4 years after the date of the enactment of this section.

"(e) DEFINITIONS.—In this section:

"(1) CLIMATE SECURITY.—The term 'climate security' means the effects of climate change on the following:

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

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

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

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

"(2) CLIMATE INTELLIGENCE INDICATIONS AND WARNINGS.—The term 'climate intelligence indications and warnings' means developments relating to climate security with the potential to—

"(A) imminently and substantially alter the political stability or degree of human security in a country or region; or

"(B) imminently and substantially threaten—

"(i) the national security of the United States;

"(ii) the military, political, or economic interests of allies and partners of the United States; or

"(iii) citizens of the United States abroad.".

(b) CLERICAL AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by inserting after the item relating to section 119B the following new item:

"Sec. 120. Climate Security Advisory Council.".

(c) INITIAL APPOINTMENTS.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall appoint the members of the Council under section 120 of the National Security Act of 1947, as added by subsection (a).

SEC. 402. TRANSFER OF NATIONAL INTELLIGENCE UNIVERSITY TO THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.

(a) TRANSFER.—Not later than 90 days after the date of the enactment of this Act, the Director of the Defense Intelligence Agency shall transfer to the Director of National Intelligence the National Intelligence University, including the functions, personnel, assets, and liabilities of the University.

(b) DEGREE-GRANTING AUTHORITY.—

(1) REGULATIONS.—Under regulations prescribed by the Director of National Intelligence, the President of the National Intelligence University may, upon the recommendation of the faculty of the University, confer appropriate degrees upon graduates who meet the degree requirements.

(2) LIMITATION.—A degree may not be conferred under this section unless—

(A) the appropriate head of a Department of the Federal Government has recommended approval of the degree in accordance with any Federal policy applicable to the granting of academic degrees by departments and agencies of the Federal Government; and

(B) the University is accredited by the appropriate civilian academic accrediting agency or organization to award the degree, as determined by such appropriate head of a Department.

(c) CONGRESSIONAL NOTIFICATION REQUIREMENTS.—

(1) NOTIFICATION.—When seeking to establish degree-granting authority under this section, the Director shall submit to the congressional intelligence committees—

(A) a copy of the self-assessment questionnaire required by the Federal policy specified in subsection (b)(2)(A); and

(B) any subsequent recommendations and rationale of the appropriate head of a Department specified in such subsection regarding establishing such degree-granting authority.

(2) MODIFICATION.—Upon any modification or redesignation of existing degree-granting authority, the Director shall submit to the congressional intelligence committees a report containing the rationale for the proposed modification or redesignation and any subsequent recommendation described in paragraph (1)(B) with respect to the proposed modification or redesignation.

(3) ACTIONS ON NONACCREDITATION.—The Director shall submit to the congressional intelligence committees a report containing an explanation of any action by the appropriate academic accrediting agency or organization not to accredit the University to award any new or existing degree.

(d) CONFORMING REPEAL.—Effective 90 days after the date of the enactment of this Act, section 2161 of title 10, United States Code, is repealed, and the table of sections at the beginning of chapter 108 of such title is amended by striking the item relating to such section 2161.

TITLE V—MATTERS RELATING TO FOREIGN COUNTRIES

SEC. 501. ANNUAL REPORTS ON INFLUENCE OPERATIONS AND CAMPAIGNS IN THE UNITED STATES BY THE COMMUNIST PARTY OF CHINA.

(a) REPORTS.—Title XI of the National Security Act of 1947 (50 U.S.C. 3231 et seq.), as amended by section 2718, is further amended by adding at the end the following new section:

"SEC. 1106. ANNUAL REPORTS ON INFLUENCE OPERATIONS AND CAMPAIGNS IN THE UNITED STATES BY THE COMMUNIST PARTY OF CHINA.

"(a) REQUIREMENT.—On an annual basis, the Director of the National Counterintelligence and Security Center shall submit to the congressional intelligence committees a report on the influence operations and campaigns in the United States conducted by the Communist Party of China.

"(b) CONTENTS.—Each report under subsection (a) shall include the following:

"(1) A description of the organization of the United Front Work Department of the People's Republic of China, or the successors of the United Front Work Department, and the links between the United Front Work Department and the Central Committee of the Communist Party of China.

"(2) An assessment of the degree to which organizations that are associated with or receive funding from the United Front Work Department, particularly such entities operating in the United States, are formally tasked by the Chinese Communist Party or the Government of China.

"(3) A description of the efforts by the United Front Work Department and subsidiary organizations of the United Front Work Department to target, coerce, and influence foreign populations, particularly those of ethnic Chinese descent.

"(4) An assessment of attempts by the Chinese Embassy, consulates, and organizations affiliated with the Chinese Communist Party (including, at a minimum, the United Front Work Department) to influence the United States-based Chinese Student Scholar Associations.

"(5) A description of the evolution of the role of the United Front Work Department under the leadership of the President of China.

"(6) An assessment of the activities of the United Front Work Department designed to influence the opinions of elected leaders of the United States, or candidates for elections in the United States, with respect to issues of importance to the Chinese Communist Party.

"(7) A listing of all known organizations affiliated with the United Front Work Department that are operating in the United States as of the date of the report.

"(8) With respect to reports submitted after the first report, an assessment of the change in goals, tactics, techniques, and procedures of the influence operations and campaigns conducted by the Chinese Communist Party.

"(c) COORDINATION.—In carrying out subsection (a), the Director shall coordinate with the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, the Director of the National Security Agency, and any other relevant head of an element of the intelligence community.

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

(b) CLERICAL AMENDMENT.—The table of contents in the first section of the National Security Act of 1947, as amended by section 2718, is further amended by inserting after the item relating to section 1105 the following new item:

"Sec. 1106. Annual reports on influence operations and campaigns in the United States by the Communist Party of China.".

(c) INITIAL REPORT.—The Director of the National Counterintelligence and Security Center shall submit to the congressional intelligence committees the first report under section 1106 of the National Security Act of 1947, as added by subsection (a), by not later than 180 days after the date of the enactment of this Act.

SEC. 502. REPORT ON REPRESSION OF ETHNIC MUSLIM MINORITIES IN THE XINJIANG REGION OF THE PEOPLE'S REPUBLIC OF CHINA.

(a) REPORT.—Not later than 150 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 activity by the People's Republic of China to repress ethnic Muslim minorities in the Xinjiang region of China.

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

(1) An assessment of the number of individuals detained in "political reeducation camps", and the conditions in such camps for detainees, in the Xinjiang re-

gion of China, including whether detainees endure torture, forced renunciation of faith, or other mistreatment.

(2) A description, as possible, of the geographic location of such camps.

(3) A description, as possible, of the methods used by China to "reeducate" detainees and the elements of China responsible for such "reeducation".

(4) A description of any forced labor in such camps, and any labor performed in regional factories for low wages under the threat of being sent back to "political reeducation camps".

(5) An assessment of the level of access China grants to foreign persons observing the situation in Xinjiang and a description of measures used to impede efforts to monitor the conditions in Xinjiang.

(6) An assessment of the surveillance, detection, and control methods used by China to target ethnic minorities, including new "high-tech" policing models and a description of any civil liberties or privacy protections provided under such models.

(c) COORDINATION.—The Director of National Intelligence shall carry out subsection (a) in coordination with the Director of the Central Intelligence Agency, the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, and the head of any other agency of the Federal Government that the Director of National Intelligence determines appropriate.

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

SEC. 503. REPORT ON EFFORTS BY PEOPLE'S REPUBLIC OF CHINA TO INFLUENCE ELECTION IN TAIWAN.

(a) REPORT.—Consistent with section 3(c) of the Taiwan Relations Act (Public Law 96–8; 22 U.S.C. 3302(c)), not later than 45 days after the date of the election for the President and Vice President of Taiwan in 2020, the Director of National Intelligence shall submit to the congressional intelligence committees a report on any—

(1) influence operations conducted by China to interfere in or undermine such election; and

(2) efforts by the United States to disrupt such operations.

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

(1) A description of any significant efforts by the intelligence community to coordinate technical and material support for Taiwan to identify, disrupt, and combat influence operations specified in subsection (a)(1).

(2) A description of any efforts by the United States Government to build the capacity of Taiwan to disrupt external efforts that degrade a free and fair election process.

(3) An assessment of whether and to what extent China conducted influence operations specified in subsection (a)(1), and, if such operations occurred—

(A) a comprehensive list of specific governmental and nongovernmental entities of China that were involved in supporting such operations and a description of the role of each such entity; and

(B) an identification of any tactics, techniques, and procedures used in such operations.

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

SEC. 504. ASSESSMENT OF LEGITIMATE AND ILLEGITIMATE FINANCIAL AND OTHER ASSETS OF VLADIMIR PUTIN.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the United States should do more to expose the corruption of Vladimir Putin, whose ill-gotten wealth is perhaps the most powerful global symbol of his dishonesty and his persistent efforts to undermine the rule of law and democracy in the Russian Federation.

(b) ASSESSMENT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate congressional committees an assessment, based on all sources of intelligence, on the net worth and financial and other assets, legitimate as well as illegitimate, of Russian President Vladimir Putin and his family members, including—

(1) the estimated net worth of Vladimir Putin and his family members;

(2) a description of their legitimately and illegitimately obtained assets, including all real, personal, and intellectual property, bank or investment or similar accounts, and any other financial or business interests or holdings, including those outside of Russia;

(3) the details of the legitimately and illegitimately obtained assets, including real, personal, and intellectual property, bank or investment or similar accounts, and any other financial or business interests or holdings, including those outside of Russia, that are owned or controlled by, accessible to, or otherwise maintained for the benefit of Vladimir Putin, including their nature, loca-

tion, manner of acquisition, value, and publicly named owner (if other than Vladimir Putin);

(4) the methods used by Vladimir Putin or others acting at his direction, with his knowledge, or for his benefit, to conceal Putin's interest in his accounts, holdings, or other assets, including the establishment of "front" or shell companies and the use of intermediaries; and

(5) an identification of the most significant senior Russian political figures, oligarchs, and any other persons who have engaged in activity intended to conceal the true financial condition of Vladimir Putin.

(c) FORM.—The assessment required under subsection (b) shall be submitted either—

(1) in unclassified form to the extent consistent with the protection of intelligence sources and methods, and may include a classified annex; or

(2) simultaneously as both an unclassified version and a classified version.

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

(1) the Select Committee on Intelligence, the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, and the Committee on Finance of the Senate; and

(2) the Permanent Select Committee on Intelligence, Committee on Foreign Affairs, the Committee on Financial Services, and the Committee on Ways and Means of the House of Representatives.

SEC. 505. ASSESSMENTS OF INTENTIONS OF POLITICAL LEADERSHIP OF THE RUSSIAN FEDERATION.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, and the head of any element of the intelligence community that the Director determines appropriate, shall submit to the appropriate congressional committees each of the assessments described in subsection (b).

(b) ASSESSMENTS DESCRIBED.—The assessments described in this subsection are assessments based on intelligence obtained from all sources that assess the current intentions of the political leadership of the Russian Federation with respect to the following:

(1) Potential military action against members of the North Atlantic Treaty Organization (NATO).

(2) Potential responses to an enlarged United States or NATO military presence in eastern Europe or to increased United States military support for allies and partners in the region, such as the provision of additional lethal military equipment to Ukraine or Georgia.

(3) Potential actions taken for the purpose of exploiting perceived divisions among the governments of Russia's Western adversaries.

(c) FORM.—Each assessment required under subsection (a) may be submitted in classified form but shall also include an unclassified executive summary, consistent with the protection of intelligence sources and methods.

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

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

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

SEC. 506. REPORT ON DEATH OF JAMAL KHASHOGGI.

(a) IN GENERAL.—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 death of Jamal Khashoggi. Such report shall include identification of those who carried out, participated in, ordered, or were otherwise complicit in or responsible for the death of Jamal Khashoggi, to the extent consistent with the protection of sources and methods.

(b) FORM.—The report submitted under subsection (a) shall be submitted in unclassified form.

TITLE VI—FEDERAL EFFORTS AGAINST DOMESTIC TERRORISM

SEC. 601. DEFINITIONS.

In this title:

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

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

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

(2) DOMESTIC TERRORISM.—The term "domestic terrorism" has the meaning given that term in section 2331 of title 18, United States Code.

(3) HATE CRIME.—The term "hate crime" means a criminal offense under—

(A) sections 241, 245, 247, and 249 of title 18, United States Code; and

(B) section 3631 of title 42, United States Code.

(4) INTERNATIONAL TERRORISM.—The term "international terrorism" has the meaning given that term in section 2331 of title 18, United States Code.

(5) TERMS IN ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS.—The terms "assessments", "full investigations", "enterprise investigations","predicated investigations", and "preliminary investigations" have the meanings given those terms in the most recent, approved version of the Attorney General's Guidelines for Domestic FBI Operations (or successor).

(6) TERMS IN FBI BUDGET MATERIALS.—The terms "Consolidated Strategy Guide", "Field Office Strategic Plan", "Integrated Program Management Process", and "Threat Review and Prioritization" have the meanings given those terms in the materials submitted to Congress by the Attorney General in support of the Federal Bureau of Investigation budget for fiscal year 2020.

(7) TERRORISM.—The term "terrorism" includes domestic terrorism and international terrorism.

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

(9) TIME UTILIZATION AND RECORDKEEPING DATA.—The term "time utilization and recordkeeping data" means data collected on resource utilization and workload activity of personnel of the Federal Bureau of Investigation in accordance with Federal law.

SEC. 602. ANNUAL STRATEGIC INTELLIGENCE ASSESSMENT OF AND COMPREHENSIVE REPORT ON DOMESTIC TERRORISM.

(a) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter through 2025, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Under Secretary of Homeland Security for Intelligence and Analysis shall jointly submit to the appropriate congressional committees a report on domestic terrorism containing the following:

(A) Strategic intelligence assessment under subsection (b).

(B) Discussion of activities under subsection (c).

(C) Data on domestic terrorism under subsection (d).

(2) RESPONSIBILITIES.—

(A) COORDINATION OF REPORTS AND INTEGRATION OF INFORMATION.—The Director of National Intelligence, acting through the Director of the National Counterterrorism Center, shall be the lead official for coordinating the production of and integrating terrorism information into—

(i) each report under paragraph (1); and

(ii) each strategic intelligence assessment under subsection (b).

(B) INFORMATION SHARING.—The Director of the Federal Bureau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis shall provide to the Director of the National Counterterrorism Center all appropriate information requested by the Director of the National Counterterrorism Center to carry out this section.

(b) STRATEGIC INTELLIGENCE ASSESSMENT.—The Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Under Secretary of Homeland Security for Intelligence and Analysis shall include—

(1) in the first report under subsection (a)(1), a strategic intelligence assessment of domestic terrorism in the United States during fiscal years 2017, 2018, and 2019; and

(2) in each subsequent report under such subsection, a strategic intelligence assessment of domestic terrorism in the United States during the prior fiscal year.

(c) DISCUSSION OF ACTIVITIES.—Each report under subsection (a)(1) shall discuss and compare the following:

(1) The criteria for opening, managing, and closing domestic and international terrorism investigations by the Federal Government.

(2) Standards and procedures for the Federal Bureau of Investigation, the Office of Intelligence and Analysis of the Department of Homeland Security, and the National Counterterrorism Center, with respect to the review, prioritization, and mitigation of domestic and international terrorism threats in the United States.

(3) The planning, development, production, analysis, and evaluation by the United States Government of intelligence products relating to terrorism, including both raw and finished intelligence.

(4) The sharing of information relating to domestic and international terrorism by and between—

(A) the Federal Government;

(B) State, local, Tribal, territorial, and foreign governments;

(C) the appropriate congressional committees;

(D) non-governmental organizations; and

(E) the private sector.

(5) The criteria and methodology used by the Federal Bureau of Investigation, the Office of Intelligence and Analysis of the Department of Homeland Security, and the National Counterterrorism Center, to identify or assign terrorism classifications to incidents of terrorism or investigations of terrorism, including—

(A) a comparison of the criteria and methodology used with respect to domestic terrorism and international terrorism;

(B) the identification of any changes made to investigative classifications; and

(C) a discussion of the rationale for any changes identified under subparagraph (B).

(d) DATA ON DOMESTIC TERRORISM.—

(1) DATA REQUIRED.—The Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Under Secretary of Homeland Security for Intelligence and Analysis shall include in each report under subsection (a)(1) the following data:

(A) For each completed or attempted incident of domestic terrorism that has occurred in the United States during the applicable period—

(i) a description of such incident;

(ii) the number and type of completed and attempted Federal nonviolent crimes committed during such incident;

(iii) the number and type of completed and attempted Federal and State property crimes committed during such incident, including an estimate of economic damages resulting from such crimes; and

(iv) the number and type of completed and attempted Federal violent crimes committed during such incident, including the number of people injured or killed as a result of such crimes.

(B) For the applicable period—

(i) an identification of each assessment, preliminary investigation, full investigation, and enterprise investigation with a nexus to domestic terrorism opened, pending, or closed by the Federal Bureau of Investigation;

(ii) the number of assessments or investigations identified under clause (i) associated with each domestic terrorism investigative classification (including subcategories);

(iii) the number and domestic terrorism investigative classification (including subcategories) with respect to such investigations initiated as a result of a referral or investigation by a State, local, Tribal, territorial, or foreign government of a hate crime;

(iv) the number of Federal criminal charges with a nexus to domestic terrorism, including the number of indictments and complaints associated with each domestic terrorism investigative classification (including subcategories), a summary of the allegations contained in each such indictment, the disposition of the prosecution, and, if applicable, the sentence imposed as a result of a conviction on such charges;

(v) referrals of incidents of domestic terrorism by State, local, Tribal, or territorial governments to departments or agencies of the Federal Government for investigation or prosecution, including the number of such referrals associated with each domestic terrorism investigation classification (including any subcategories), and a summary of each such referral that includes the rationale for such referral and the disposition of the applicable Federal investigation or prosecution;

(vi) intelligence products produced by the intelligence community relating to domestic terrorism, including—

(I) the number of such products associated with each domestic terrorism investigative classification (including any subcategories); and

(II) with respect to the Federal Bureau of Investigation, at a minimum, all relevant data available through the Integrated Program Management Process;

(vii) with respect to the National Counterterrorism Center, the number of staff (expressed in terms of full-time equivalents and positions) working on matters relating to domestic terrorism described in clauses (i) through (vi); and

(viii) with respect to the Federal Bureau of Investigation—

(I) the number of staff (expressed in terms of full-time equivalents and positions) working on matters relating to domestic terrorism described in clauses (i) through (vi); and

(II) a summary of time utilization and recordkeeping data for personnel working on such matters, including the number or percentage of such personnel associated with each domestic terrorism investigative classification (including any subcategories) in the FBI Headquarters Operational Divisions and Field Divisions.

(2) APPLICABLE PERIOD.—For purposes of this subsection, the applicable period is the following:

(A) For the first report required under subsection (a)(1)—

(i) with respect to the data described in paragraph (1)(A) of this subsection, the period on or after April 19, 1995; and

(ii) with respect to the data described in paragraph (1)(B) of this subsection, each of fiscal years 2017, 2018, and 2019.

(B) For each subsequent report required under subsection (a)(1), the prior fiscal year.

(e) PROVISION OF OTHER DOCUMENTS AND MATERIALS.—

(1) IN GENERAL.—Together with each report under subsection (a)(1), the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Under Secretary of Homeland Security for Intelligence and Analysis shall also submit to the appropriate congressional committees the following documents and materials:

(A) With respect to the Federal Bureau of Investigation, at a minimum, the most recent, approved versions of—

(i) the Attorney General's Guidelines for Domestic FBI Operations (or any successor);

(ii) the FBI Domestic Investigations and Operations Guide (or any successor);

(iii) the FBI Counterterrorism Policy Guide (or any successor);

(iv) materials relating to terrorism within the Threat Review and Prioritization process for the headquarters and field divisions of the Federal Bureau of Investigation;

(v) the Consolidated Strategy Guide (or any successor); and

(vi) the Field Office Strategic Plans (or any successor).

(B) With respect to the intelligence community, each finished intelligence product described in subsection (d)(1)(B)(vi).

(2) NONDUPLICATION.—If any documents or materials required under paragraph (1) have been previously submitted to the appropriate congressional committees under such paragraph and have not been modified since such submission, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Under Secretary of Homeland Security for Intelligence and Analysis may provide a list of such documents or materials in lieu of making the submission under paragraph (1) for those documents or materials.

(f) FORMAT.—The information required under subsection (d) may be provided in a format that uses the marking associated with the Central Records System (or any successor system) of the Federal Bureau of Investigation.

(g) CLASSIFICATION AND PUBLIC RELEASE.—Each report under subsection (a) shall be—

(1) unclassified, but may contain a classified annex;

(2) with respect to the unclassified portion of the report, made available on the public internet website of the National Counterterrorism Center in an electronic format that is fully indexed and searchable; and

(3) with respect to a classified annex, submitted to the appropriate congressional committees in an electronic format that is fully indexed and searchable.

TITLE VII—REPORTS AND OTHER MATTERS

SEC. 701. MODIFICATION OF REQUIREMENTS FOR SUBMISSION TO CONGRESS OF CERTAIN REPORTS.

(a) MODIFICATION OF REPORTS RELATING TO GUANTANAMO BAY.—

(1) MODIFICATION.—Section 506I(b) of the National Security Act of 1947 (50 U.S.C. 3105(b)) is amended by striking "once every 6 months" and inserting "annually".

(2) MODIFICATION.—Section 319(a) of the Supplemental Appropriations Act, 2009 (10 U.S.C. 801 note) is amended by striking "every 90 days" and inserting "annually".

(3) REPEAL.—Section 601 of the Intelligence Authorization Act for Fiscal Year 2017 (division N of Public Law 115–31; 131 Stat. 827) is repealed.

(b) MODIFICATION TO REPORTS ON VIOLATIONS OF LAW OR EXECUTIVE ORDER.—Section 511(a) of the National Security Act of 1947 (50 U.S.C. 3110(a)) is amended—

(1) by striking "The Director of National Intelligence" and inserting "The head of each element of the intelligence community"; and

(2) by striking "an element" and inserting "the element".

(c) MODIFICATION TO REPORTS ON ANALYTIC INTEGRITY.—Subsection (c) of section 1019 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3364) is amended—

(1) in the heading, by striking "REPORTS" and inserting "BRIEFINGS"; and

(2) by striking "submit to the congressional intelligence committees, the heads of the relevant elements of the intelligence community, and the heads of analytic training departments a report containing" and inserting "provide to the congressional intelligence committees, the heads of the relevant elements of the intelligence community, and the heads of analytic training departments a briefing with".

(d) REPEAL OF REPORTS RELATING TO INTELLIGENCE FUNCTIONS.—Section 506J of the National Security Act of 1947 (50 U.S.C. 3105a) is repealed and the table of contents in the first section of such Act is amended by striking the item relating to section 506J.

(e) REPEAL OF REPORTS RELATING TO CUBA.—Section 108 of the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 (22 U.S.C. 6038) is repealed.

(f) REPEAL OF REPORTS RELATING TO ENTERTAINMENT INDUSTRY.—Section 308 of the Intelligence Authorization Act for Fiscal Year 2017 (50 U.S.C. 3332) is amended by striking subsection (c).

SEC. 702. INCREASED TRANSPARENCY REGARDING COUNTERTERRORISM BUDGET OF THE UNITED STATES.

(a) FINDINGS.—Congress finds the following:

(1) Consistent with section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 3306(a)), the recent practice of the intelligence community has been to release to the public—

(A) around the date on which the President submits to Congress a budget for a fiscal year pursuant to section 1105 of title 31, United States Code, the "top-line" amount of total funding requested for the National Intelligence Program for such fiscal year; and

(B) the amount of requested and appropriated funds for the National Intelligence Program and Military Intelligence Program for certain prior fiscal years, consistent with the protection of intelligence sources and methods.

(2) The Directorate of Strategic Operational Planning of the National Counterterrorism Center is responsible for producing an annual National Counterterrorism Budget report, which examines the alignment of intelligence and other resources in the applicable fiscal year budget with the counterterrorism goals and areas of focus in the National Strategy for Counterterrorism.

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

(1) despite the difficulty of compiling and releasing to the public comprehensive information on the resource commitments of the United States to counterterrorism activities and programs, including with respect to such activities and programs of the intelligence community, the United States Government could take additional steps to enhance the understanding of the public with respect to such resource commitments, in a manner consistent with the protection of intelligence sources and methods and other national security interests; and

(2) the United States Government should release to the public as much information as possible regarding the funding of counterterrorism activities and programs, including activities and programs of the intelligence community, in a

manner consistent with the protection of intelligence sources and methods and other national security interests.

(c) BRIEFING ON PUBLIC RELEASE OF INFORMATION.—

(1) REQUIREMENT.—Not later than 90 days after the date of the enactment of this Act, and not later than 90 days after the beginning of each fiscal year thereafter, the President shall ensure that the congressional intelligence committees receive a briefing from appropriate personnel of the United States Government on the feasibility of releasing to the public additional information relating to counterterrorism efforts of the intelligence community.

(2) ELEMENTS.—Each briefing required by paragraph (1) shall include a discussion of the feasibility of—

(A) subject to paragraph (3), releasing to the public the National Counterterrorism Budget report described in subsection (a)(2) for the prior fiscal year; and

(B) declassifying other reports, documents, or activities of the intelligence community relating to counterterrorism and releasing such information to the public in a manner consistent with the protection of intelligence sources and methods and other national security interests.

(3) RELEASE OF NATIONAL COUNTERTERRORISM BUDGET REPORT.—The President may satisfy the requirement under paragraph (2)(A) during a fiscal year by, not later than 90 days after the beginning of the fiscal year, releasing to the public the National Counterterrorism Budget report (with any redactions the Director determines necessary to protect intelligence sources and methods and other national security interests) for the prior fiscal year.

SEC. 703. TASK FORCE ON ILLICIT FINANCING OF ESPIONAGE AND FOREIGN INFLUENCE OPERATIONS.

(a) ESTABLISHMENT.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall establish a task force to study and assess the illicit financing of espionage and foreign influence operations directed at the United States.

(b) MEMBERSHIP.—The task force shall be composed of the following individuals (or designees of the individual):

(1) The Director of the Central Intelligence Agency.

(2) The Director of the Federal Bureau of Investigation.

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

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

(5) Such other heads of the elements of the intelligence community that the Director of National Intelligence determines appropriate.

(c) CHAIRPERSON; MEETINGS.—

(1) CHAIRPERSON.—The Director of National Intelligence shall appoint a senior official within the Office of the Director of National Intelligence to serve as the chairperson of the task force.

(2) MEETINGS.—The task force shall meet regularly but not less frequently than on a quarterly basis.

(d) REPORTS.—

(1) INITIAL REPORT.—Not later than 180 days after the date of the enactment of this Act, the task force shall submit to the appropriate congressional committees a report on the illicit financing of espionage and foreign influence operations directed at the United States. The report shall address the following:

(A) The extent of the collection by the intelligence community, from all sources (including the governments of foreign countries), of intelligence and information relating to illicit financing of espionage and foreign influence operations directed at the United States, and any gaps in such collection.

(B) Any specific legal, regulatory, policy, or other prohibitions, or financial, human, technical, or other resource limitations or constraints, that have affected the ability of the Director of National Intelligence or other heads of relevant elements of the intelligence community in collecting or analyzing intelligence or information relating to illicit financing of espionage and foreign influence operations directed at the United States.

(C) The methods, as of the date of the report, by which hostile governments of foreign countries or foreign organizations, and any groups or persons acting on behalf of or with the support of such governments or organizations, seek to disguise or obscure relationships between such governments, organizations, groups, or persons and United States persons, for the purpose of conducting espionage or foreign influence operations directed at the United States, including by exploiting financial laws, systems, or instruments, of the United States.

(D) The existing practices of the intelligence community for ensuring that intelligence and information relating to the illicit financing of espionage

and foreign influence operations is analyzed and shared with other elements of the intelligence community, and any recommendations for improving such analysis and sharing.

(2) ANNUAL UPDATE.—Not later than November 1, 2020, and each year thereafter through the date specified in subsection (e), the task force shall submit to the appropriate congressional committees an update on the report under paragraph (1).

(3) FORM.—Each report submitted under this subsection may be submitted in classified form, but if submitted in such form, shall include an unclassified summary.

(e) TERMINATION.—The task force shall terminate on January 1, 2025.

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

(1) The congressional intelligence committees.

(2) The Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives.

(3) The Committee on Foreign Relations and the Committee on Banking, Housing, and Urban Affairs of the Senate.

SEC. 704. STUDY ON ROLE OF RETIRED AND FORMER PERSONNEL OF INTELLIGENCE COMMUNITY WITH RESPECT TO CERTAIN FOREIGN INTELLIGENCE OPERATIONS.

(a) STUDY.—The Director of National Intelligence shall conduct a study on former intelligence personnel providing covered intelligence assistance.

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

(1) An identification of, and discussion of the effectiveness of, existing laws, policies, procedures, and other measures relevant to the ability of elements of the intelligence community to prevent former intelligence personnel from providing covered intelligence assistance—

(A) without proper authorization; or

(B) in a manner that would violate legal or policy controls if the personnel performed such assistance while working for the United States Government; and

(2) Make recommendations for such legislative, regulatory, policy, or other changes as may be necessary to ensure that the United States consistently meets the objectives described in paragraph (1).

(c) REPORT AND PLAN.—Not later than 90 days after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees—

(1) a report on the findings of the Director with respect to each element of the study under subsection (a); and

(2) a plan to implement any recommendations made by the Director that the Director may implement without changes to Federal law.

(d) FORM.—The report and plan under subsection (c) may be submitted in classified form.

(e) DEFINITIONS.—In this section:

(1) COVERED INTELLIGENCE ASSISTANCE.—The term "covered intelligence assistance" means assistance—

(A) provided by former intelligence personnel directly to, or for the benefit of, the government of a foreign country or indirectly to, or for the benefit of, such a government through a company or other entity; and

(B) that relates to intelligence or law enforcement activities of a foreign country, including with respect to operations that involve abuses of human rights, violations of the laws of the United States, or infringements on the privacy rights of United States persons.

(2) FORMER INTELLIGENCE PERSONNEL.—The term "former intelligence personnel" means retired or former personnel of the intelligence community, including civilian employees of elements of the intelligence community, members of the Armed Forces, and contractors of elements of the intelligence community.

SEC. 705. REPORT BY DIRECTOR OF NATIONAL INTELLIGENCE ON FIFTH-GENERATION WIRELESS NETWORK TECHNOLOGY.

(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 on—

(1) the threat to the national security of the United States posed by the global and regional adoption of fifth-generation wireless network (in this section referred to as "5G wireless network") technology built by foreign companies; and

(2) possible efforts to mitigate the threat.

(b) CONTENTS.—The report under subsection (a) shall include—

(1) the timeline and scale of global and regional adoption of foreign 5G wireless network technology;

(2) the implications of such global and regional adoption on the cyber and espionage threat to the United States, the interests of the United States, and the cyber and collection capabilities of the United States; and

(3) the effect of possible mitigation efforts, including with respect to—

(A) a policy of the United States Government promoting the use of strong, end-to-end encryption for data transmitted over 5G wireless networks;

(B) a policy of the United States Government promoting or funding free, open-source implementation of 5G wireless network technology;

(C) subsidies or incentives provided by the United States Government that could be used to promote the adoption of secure 5G wireless network technology developed by companies of the United States or companies of allies of the United States; and

(D) a strategy by the United States Government to reduce foreign influence and political pressure in international standard-setting bodies.

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

SEC. 706. ESTABLISHMENT OF 5G PRIZE COMPETITION.

(a) PRIZE COMPETITION.—Pursuant to section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719), the Director of National Intelligence, acting through the Director of the Intelligence Advanced Research Projects Agency, shall carry out a program to award prizes competitively to stimulate research and development relevant to 5G technology.

(b) PRIZE AMOUNT.—In carrying out the program under subsection (a), the Director may award not more than a total of $5,000,000 to one or more winners of the prize competition.

(c) CONSULTATION.—In carrying out the program under subsection (a), the Director may consult with the heads of relevant departments and agencies of the Federal Government.

(d) 5G TECHNOLOGY DEFINED.—In this section, the term "5G technology" means hardware, software, or other technologies relating to fifth-generation wireless networks.

SEC. 707. ESTABLISHMENT OF DEEPFAKES PRIZE COMPETITION.

(a) PRIZE COMPETITION.—Pursuant to section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719), the Director of National Intelligence, acting through the Director of the Intelligence Advanced Research Projects Agency, shall carry out a program to award prizes competitively to stimulate the research, development, or commercialization of technologies to automatically detect machine-manipulated media.

(b) PRIZE AMOUNT.—In carrying out the program under subsection (a), the Director may award not more than a total of $5,000,000 to one or more winners of the prize competition.

(c) CONSULTATION.—In carrying out the program under subsection (a), the Director may consult with the heads of relevant departments and agencies of the Federal Government.

(d) MACHINE-MANIPULATED MEDIA DEFINED.—In this section, the term "machine-manipulated media" means video, image, or audio recordings generated or substantially modified using machine-learning techniques in order to falsely depict events or to falsely depict the speech or conduct of an individual.

DIVISION B—INTELLIGENCE AUTHORIZATIONS FOR FISCAL YEARS 2018 AND 2019

TITLE XXI—INTELLIGENCE ACTIVITIES

SEC. 2101. AUTHORIZATION OF APPROPRIATIONS.

(a) FISCAL YEAR 2019.—Funds are hereby authorized to be appropriated for fiscal year 2019 for the conduct of the intelligence and intelligence-related activities of the following elements of the United States Government:

(1) The Office of the Director of National Intelligence.

(2) The Central Intelligence Agency.

(3) The Department of Defense.

(4) The Defense Intelligence Agency.

(5) The National Security Agency.

(6) The Department of the Army, the Department of the Navy, and the Department of the Air Force.

(7) The Coast Guard.
(8) The Department of State.
(9) The Department of the Treasury.
(10) The Department of Energy.
(11) The Department of Justice.
(12) The Federal Bureau of Investigation.
(13) The Drug Enforcement Administration.
(14) The National Reconnaissance Office.
(15) The National Geospatial-Intelligence Agency.
(16) The Department of Homeland Security.

(b) FISCAL YEAR 2018.—Funds that were appropriated for fiscal year 2018 for the conduct of the intelligence and intelligence-related activities of the elements of the United States set forth in subsection (a) are hereby authorized.

SEC. 2102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) SPECIFICATIONS OF AMOUNTS.—The amounts authorized to be appropriated under section 2101 for the conduct of the intelligence activities of the elements listed in paragraphs (1) through (16) of section 2101, 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. 2103. 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 2019 the sum of $522,424,000.

(b) CLASSIFIED AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2019 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 2102(a).

TITLE XXII—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 2201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund $514,000,000 for fiscal year 2019.

SEC. 2202. COMPUTATION OF ANNUITIES FOR EMPLOYEES OF THE CENTRAL INTELLIGENCE AGENCY.

(a) COMPUTATION OF ANNUITIES.—

(1) IN GENERAL.—Section 221 of the Central Intelligence Agency Retirement Act (50 U.S.C. 2031) is amended—

(A) in subsection (a)(3)(B), by striking the period at the end and inserting ", as determined by using the annual rate of basic pay that would be payable for full-time service in that position.";
(B) in subsection (b)(1)(C)(i), by striking "12-month" and inserting "2-year";
(C) in subsection (f)(2), by striking "one year" and inserting "two years";
(D) in subsection (g)(2), by striking "one year" each place such term appears and inserting "two years";
(E) by redesignating subsections (h), (i), (j), (k), and (l) as subsections (i), (j), (k), (l), and (m), respectively; and
(F) by inserting after subsection (g) the following:

"(h) CONDITIONAL ELECTION OF INSURABLE INTEREST SURVIVOR ANNUITY BY PARTICIPANTS MARRIED AT THE TIME OF RETIREMENT.—

"(1) AUTHORITY TO MAKE DESIGNATION.—Subject to the rights of former spouses under subsection (b) and section 222, at the time of retirement a married participant found by the Director to be in good health may elect to receive an annuity reduced in accordance with subsection (f)(1)(B) and designate in writing an individual having an insurable interest in the participant to receive an annuity under the system after the participant's death, except that any such election to provide an insurable interest survivor annuity to the participant's spouse shall only be effective if the participant's spouse waives the spousal right to a survivor annuity under this Act. The amount of the annuity shall be equal to 55 percent of the participant's reduced annuity.

"(2) REDUCTION IN PARTICIPANT'S ANNUITY.—The annuity payable to the participant making such election shall be reduced by 10 percent of an annuity computed under subsection (a) and by an additional 5 percent for each full 5 years the designated individual is younger than the participant. The total reduction under this subparagraph may not exceed 40 percent.

"(3) COMMENCEMENT OF SURVIVOR ANNUITY.—The annuity payable to the designated individual shall begin on the day after the retired participant dies and terminate on the last day of the month before the designated individual dies.

"(4) RECOMPUTATION OF PARTICIPANT'S ANNUITY ON DEATH OF DESIGNATED INDIVIDUAL.—An annuity that is reduced under this subsection shall, effective the first day of the month following the death of the designated individual, be recomputed and paid as if the annuity had not been so reduced.".

(2) CONFORMING AMENDMENTS.—

(A) CENTRAL INTELLIGENCE AGENCY RETIREMENT ACT.—The Central Intelligence Agency Retirement Act (50 U.S.C. 2001 et seq.) is amended—

(i) in section 232(b)(1) (50 U.S.C. 2052(b)(1)), by striking "221(h)," and inserting "221(i),"; and

(ii) in section 252(h)(4) (50 U.S.C. 2082(h)(4)), by striking "221(k)" and inserting "221(l)".

(B) CENTRAL INTELLIGENCE AGENCY ACT OF 1949.—Subsection (a) of section 14 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3514(a)) is amended by striking "221(h)(2), 221(i), 221(l)," and inserting "221(i)(2), 221(j), 221(m),".

(b) ANNUITIES FOR FORMER SPOUSES.—Subparagraph (B) of section 222(b)(5) of the Central Intelligence Agency Retirement Act (50 U.S.C. 2032(b)(5)(B)) is amended by striking "one year" and inserting "two years".

(c) PRIOR SERVICE CREDIT.—Subparagraph (A) of section 252(b)(3) of the Central Intelligence Agency Retirement Act (50 U.S.C. 2082(b)(3)(A)) is amended by striking "October 1, 1990" both places that term appears and inserting "March 31, 1991".

(d) REEMPLOYMENT COMPENSATION.—Section 273 of the Central Intelligence Agency Retirement Act (50 U.S.C. 2113) is amended—

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

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

"(b) PART-TIME REEMPLOYED ANNUITANTS.—The Director shall have the authority to reemploy an annuitant on a part-time basis in accordance with section 8344(l) of title 5, United States Code.".

(e) EFFECTIVE DATE AND APPLICATION.—The amendments made by subsection (a)(1)(A) and subsection (c) shall take effect as if enacted on October 28, 2009, and shall apply to computations or participants, respectively, as of such date.

TITLE XXIII—GENERAL INTELLIGENCE COMMUNITY MATTERS

SEC. 2301. RESTRICTION ON CONDUCT OF INTELLIGENCE ACTIVITIES.

The authorization of appropriations by this division 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. 2302. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY LAW.

Appropriations authorized by this division 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. 2303. MODIFICATION OF SPECIAL PAY AUTHORITY FOR SCIENCE, TECHNOLOGY, ENGINEERING, OR MATHEMATICS POSITIONS AND ADDITION OF SPECIAL PAY AUTHORITY FOR CYBER POSITIONS.

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

(1) by amending subsection (a) to read as follows:

"(a) SPECIAL RATES OF PAY FOR POSITIONS REQUIRING EXPERTISE IN SCIENCE, TECHNOLOGY, ENGINEERING, OR MATHEMATICS.—

"(1) IN GENERAL.—Notwithstanding part III of title 5, United States Code, the head of each element of the intelligence community may, for 1 or more categories of positions in such element that require expertise in science, technology, engineering, or mathematics—

"(A) establish higher minimum rates of pay; and

"(B) make corresponding increases in all rates of pay of the pay range for each grade or level, subject to subsection (b) or (c), as applicable.

"(2) TREATMENT.—The special rate supplements resulting from the establishment of higher rates under paragraph (1) shall be basic pay for the same or similar purposes as those specified in section 5305(j) of title 5, United States Code.";

(2) by redesignating subsections (b) through (f) as subsections (c) through (g), respectively;

(3) by inserting after subsection (a) the following:

"(b) SPECIAL RATES OF PAY FOR CYBER POSITIONS.—

"(1) IN GENERAL.—Notwithstanding subsection (c), the Director of the National Security Agency may establish a special rate of pay—

"(A) not to exceed the rate of basic pay payable for level II of the Executive Schedule under section 5313 of title 5, United States Code, if the Director certifies to the Under Secretary of Defense for Intelligence, in consultation with the Under Secretary of Defense for Personnel and Readiness, that the rate of pay is for positions that perform functions that execute the cyber mission of the Agency; or

"(B) not to exceed the rate of basic pay payable for the Vice President of the United States under section 104 of title 3, United States Code, if the Director certifies to the Secretary of Defense, by name, individuals that have advanced skills and competencies and that perform critical functions that execute the cyber mission of the Agency.

"(2) PAY LIMITATION.—Employees receiving a special rate under paragraph (1) shall be subject to an aggregate pay limitation that parallels the limitation established in section 5307 of title 5, United States Code, except that—

"(A) any allowance, differential, bonus, award, or other similar cash payment in addition to basic pay that is authorized under title 10, United States Code, (or any other applicable law in addition to title 5 of such Code, excluding the Fair Labor Standards Act of 1938 (29 U.S.C. 201 et seq.)) shall also be counted as part of aggregate compensation; and

"(B) aggregate compensation may not exceed the rate established for the Vice President of the United States under section 104 of title 3, United States Code.

"(3) LIMITATION ON NUMBER OF RECIPIENTS.—The number of individuals who receive basic pay established under paragraph (1)(B) may not exceed 100 at any time.

"(4) LIMITATION ON USE AS COMPARATIVE REFERENCE.—Notwithstanding any other provision of law, special rates of pay and the limitation established under paragraph (1)(B) may not be used as comparative references for the purpose of fixing the rates of basic pay or maximum pay limitations of qualified positions under section 1599f of title 10, United States Code, or section 226 of the Homeland Security Act of 2002 (6 U.S.C. 147).";

(4) in subsection (c), as redesignated by paragraph (2), by striking "A minimum" and inserting "Except as provided in subsection (b), a minimum";

(5) in subsection (d), as redesignated by paragraph (2), by inserting "or (b)" after "by subsection (a)"; and

(6) in subsection (g), as redesignated by paragraph (2)—

(A) in paragraph (1), by striking "Not later than 90 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2017" and inserting "Not later than 90 days after the date of the enactment of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019"; and

(B) in paragraph (2)(A), by inserting "or (b)" after "subsection (a)".

SEC. 2304. MODIFICATION OF APPOINTMENT OF CHIEF INFORMATION OFFICER OF THE INTELLIGENCE COMMUNITY.

Section 103G(a) of the National Security Act of 1947 (50 U.S.C. 3032(a)) is amended by striking "President" and inserting "Director".

SEC. 2305. DIRECTOR OF NATIONAL INTELLIGENCE REVIEW OF PLACEMENT OF POSITIONS WITHIN THE INTELLIGENCE COMMUNITY ON THE EXECUTIVE SCHEDULE.

(a) REVIEW.—The Director of National Intelligence, in coordination with the Director of the Office of Personnel Management, shall conduct a review of positions within the intelligence community regarding the placement of such positions on the Executive Schedule under subchapter II of chapter 53 of title 5, United States Code. In carrying out such review, the Director of National Intelligence, in coordination with the Director of the Office of Personnel Management, shall determine—

(1) the standards under which such review will be conducted;

(2) which positions should or should not be on the Executive Schedule; and

(3) for those positions that should be on the Executive Schedule, the level of the Executive Schedule at which such positions should be placed.

(b) REPORT.—Not later than 60 days after the date on which the review under subsection (a) is completed, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Oversight and Reform of the House of Representatives an unredacted report describing the standards by which the review was conducted and the outcome of the review.

SEC. 2306. SUPPLY CHAIN AND COUNTERINTELLIGENCE RISK MANAGEMENT TASK FORCE.

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

(1) The congressional intelligence committees.

(2) The Committee on Armed Services and the Committee on Homeland Security and Governmental Affairs of the Senate.

(3) The Committee on Armed Services, the Committee on Homeland Security, and the Committee on Oversight and Reform of the House of Representatives.

(b) REQUIREMENT TO ESTABLISH.—The Director of National Intelligence shall establish a Supply Chain and Counterintelligence Risk Management Task Force to standardize information sharing between the intelligence community and the acquisition community of the United States Government with respect to the supply chain and counterintelligence risks.

(c) MEMBERS.—The Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall be composed of—

(1) a representative of the Defense Security Service of the Department of Defense;

(2) a representative of the General Services Administration;

(3) a representative of the Office of Federal Procurement Policy of the Office of Management and Budget;

(4) a representative of the Department of Homeland Security;

(5) a representative of the Federal Bureau of Investigation;

(6) the Director of the National Counterintelligence and Security Center; and

(7) any other members the Director of National Intelligence determines appropriate.

(d) SECURITY CLEARANCES.—Each member of the Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall have a security clearance at the top secret level and be able to access sensitive compartmented information.

(e) ANNUAL REPORT.—The Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall submit to the appropriate congressional committees an annual report that describes the activities of the Task Force during the previous year, including identification of the supply chain and counterintelligence risks shared with the acquisition community of the United States Government by the intelligence community.

SEC. 2307. CONSIDERATION OF ADVERSARIAL TELECOMMUNICATIONS AND CYBERSECURITY INFRASTRUCTURE WHEN SHARING INTELLIGENCE WITH FOREIGN GOVERNMENTS AND ENTITIES.

Whenever the head of an element of the intelligence community enters into an intelligence sharing agreement with a foreign government or any other foreign entity, the head of the element shall consider the pervasiveness of telecommunications and cybersecurity infrastructure, equipment, and services provided by adversaries of the United States, particularly China and Russia, or entities of such adversaries in the country or region of the foreign government or other foreign entity entering into the agreement.

SEC. 2308. CYBER PROTECTION SUPPORT FOR THE PERSONNEL OF THE INTELLIGENCE COMMUNITY IN POSITIONS HIGHLY VULNERABLE TO CYBER ATTACK.

(a) DEFINITIONS.—In this section:

(1) PERSONAL ACCOUNTS.—The term "personal accounts" means accounts for online and telecommunications services, including telephone, residential Internet access, email, text and multimedia messaging, cloud computing, social media, health care, and financial services, used by personnel of the intelligence community outside of the scope of their employment with elements of the intelligence community.

(2) PERSONAL TECHNOLOGY DEVICES.—The term "personal technology devices" means technology devices used by personnel of the intelligence community outside of the scope of their employment with elements of the intelligence community, including networks to which such devices connect.

(b) AUTHORITY TO PROVIDE CYBER PROTECTION SUPPORT.—

(1) IN GENERAL.—Subject to a determination by the Director of National Intelligence, the Director may provide cyber protection support for the personal technology devices and personal accounts of the personnel described in paragraph (2).

(2) AT-RISK PERSONNEL.—The personnel described in this paragraph are personnel of the intelligence community—

(A) who the Director determines to be highly vulnerable to cyber attacks and hostile information collection activities because of the positions occupied by such personnel in the intelligence community; and

(B) whose personal technology devices or personal accounts are highly vulnerable to cyber attacks and hostile information collection activities.

(c) NATURE OF CYBER PROTECTION SUPPORT.—Subject to the availability of resources, the cyber protection support provided to personnel under subsection (b) may include training, advice, assistance, and other services relating to cyber attacks and hostile information collection activities.

(d) LIMITATION ON SUPPORT.—Nothing in this section shall be construed—

(1) to encourage personnel of the intelligence community to use personal technology devices for official business; or

(2) to authorize cyber protection support for senior intelligence community personnel using personal devices, networks, and personal accounts in an official capacity.

(e) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees a report on the provision of cyber protection support under subsection (b). The report shall include—

(1) a description of the methodology used to make the determination under subsection (b)(2); and

(2) guidance for the use of cyber protection support and tracking of support requests for personnel receiving cyber protection support under subsection (b).

SEC. 2309. ELIMINATION OF SUNSET OF AUTHORITY RELATING TO MANAGEMENT OF SUPPLY-CHAIN RISK.

Section 309 of the Intelligence Authorization Act for Fiscal Year 2012 (Public Law 112–87; 50 U.S.C. 3329 note) is amended by striking subsection (g).

SEC. 2310. LIMITATIONS ON DETERMINATIONS REGARDING CERTAIN SECURITY CLASSIFICATIONS.

(a) PROHIBITION.—An officer of an element of the intelligence community who has been nominated by the President for a position that requires the advice and consent of the Senate may not make a classification decision with respect to information related to such officer's nomination.

(b) CLASSIFICATION DETERMINATIONS.—

(1) IN GENERAL.—Except as provided in paragraph (2), in a case in which an officer described in subsection (a) has been nominated as described in such subsection and classification authority rests with the officer or another officer who reports directly to such officer, a classification decision with respect to information relating to the officer shall be made by the Director of National Intelligence.

(2) NOMINATIONS OF DIRECTOR OF NATIONAL INTELLIGENCE.—In a case described in paragraph (1) in which the officer nominated is the Director of National Intelligence, the classification decision shall be made by the Principal Deputy Director of National Intelligence.

(c) REPORTS.—Whenever the Director or the Principal Deputy Director makes a decision under subsection (b), the Director or the Principal Deputy Director, as the case may be, shall submit to the congressional intelligence committees a report detailing the reasons for the decision.

SEC. 2311. JOINT INTELLIGENCE COMMUNITY COUNCIL.

(a) MEETINGS.—Section 101A(d) of the National Security Act of 1947 (50 U.S.C. 3022(d)) is amended—

(1) by striking "regular"; and

(2) by inserting "as the Director considers appropriate" after "Council".

(b) REPORT ON FUNCTION AND UTILITY OF THE JOINT INTELLIGENCE COMMUNITY COUNCIL.—

(1) IN GENERAL.—No later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Executive Office of the President and members of the Joint Intelligence Community Council, shall submit to the congressional intelligence committees a report on the function and utility of the Joint Intelligence Community Council.

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

(A) The number of physical or virtual meetings held by the Council per year since the Council's inception.

(B) A description of the effect and accomplishments of the Council.

(C) An explanation of the unique role of the Council relative to other entities, including with respect to the National Security Council and the Executive Committee of the intelligence community.

(D) Recommendations for the future role and operation of the Council.

(E) Such other matters relating to the function and utility of the Council as the Director considers appropriate.

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

SEC. 2312. INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY ENVIRONMENT.

(a) DEFINITIONS.—In this section:

(1) CORE SERVICE.—The term "core service" means a capability that is available to multiple elements of the intelligence community and required for consistent operation of the intelligence community information technology environment.

(2) INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY ENVIRONMENT.—The term "intelligence community information technology environment" means all of the information technology services across the intelligence community, including the data sharing and protection environment across multiple classification domains.

(b) ROLES AND RESPONSIBILITIES.—

(1) DIRECTOR OF NATIONAL INTELLIGENCE.—The Director of National Intelligence shall be responsible for coordinating the performance by elements of the intelligence community of the intelligence community information technology environment, including each of the following:

(A) Ensuring compliance with all applicable environment rules and regulations of such environment.

(B) Ensuring measurable performance goals exist for such environment.

(C) Documenting standards and practices of such environment.

(D) Acting as an arbiter among elements of the intelligence community related to any disagreements arising out of the implementation of such environment.

(E) Delegating responsibilities to the elements of the intelligence community and carrying out such other responsibilities as are necessary for the effective implementation of such environment.

(2) CORE SERVICE PROVIDERS.—Providers of core services shall be responsible for—

(A) providing core services, in coordination with the Director of National Intelligence; and

(B) providing the Director with information requested and required to fulfill the responsibilities of the Director under paragraph (1).

(3) USE OF CORE SERVICES.—

(A) IN GENERAL.—Except as provided in subparagraph (B), each element of the intelligence community shall use core services when such services are available.

(B) EXCEPTION.—The Director of National Intelligence may provide for a written exception to the requirement under subparagraph (A) if the Director determines there is a compelling financial or mission need for such exception.

(c) MANAGEMENT ACCOUNTABILITY.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall designate and

maintain one or more accountable executives of the intelligence community information technology environment to be responsible for—

(1) management, financial control, and integration of such environment;

(2) overseeing the performance of each core service, including establishing measurable service requirements and schedules;

(3) to the degree feasible, ensuring testing of each core service of such environment, including testing by the intended users, to evaluate performance against measurable service requirements and to ensure the capability meets user requirements; and

(4) coordinate transition or restructuring efforts of such environment, including phaseout of legacy systems.

(d) SECURITY PLAN.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall develop and maintain a security plan for the intelligence community information technology environment.

(e) LONG-TERM ROADMAP.—Not later than 180 days after the date of the enactment of this Act, and during each of the second and fourth fiscal quarters thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a long-term roadmap that shall include each of the following:

(1) A description of the minimum required and desired core service requirements, including—

(A) key performance parameters; and

(B) an assessment of current, measured performance.

(2) implementation milestones for the intelligence community information technology environment, including each of the following:

(A) A schedule for expected deliveries of core service capabilities during each of the following phases:

(i) Concept refinement and technology maturity demonstration.

(ii) Development, integration, and demonstration.

(iii) Production, deployment, and sustainment.

(iv) System retirement.

(B) Dependencies of such core service capabilities.

(C) Plans for the transition or restructuring necessary to incorporate core service capabilities.

(D) A description of any legacy systems and discontinued capabilities to be phased out.

(3) Such other matters as the Director determines appropriate.

(f) BUSINESS PLAN.—Not later than 180 days after the date of the enactment of this Act, and during each of the second and fourth fiscal quarters thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a business plan that includes each of the following:

(1) A systematic approach to identify core service funding requests for the intelligence community information technology environment within the proposed budget, including multiyear plans to implement the long-term roadmap required by subsection (e).

(2) A uniform approach by which each element of the intelligence community shall identify the cost of legacy information technology or alternative capabilities where services of the intelligence community information technology environment will also be available.

(3) A uniform effort by which each element of the intelligence community shall identify transition and restructuring costs for new, existing, and retiring services of the intelligence community information technology environment, as well as services of such environment that have changed designations as a core service.

(g) QUARTERLY PRESENTATIONS.—Beginning not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall provide to the congressional intelligence committees quarterly updates regarding ongoing implementation of the intelligence community information technology environment as compared to the requirements in the most recently submitted security plan required by subsection (d), long-term roadmap required by subsection (e), and business plan required by subsection (f).

(h) ADDITIONAL NOTIFICATIONS.—The Director of National Intelligence shall provide timely notification to the congressional intelligence committees regarding any policy changes related to or affecting the intelligence community information technology environment, new initiatives or strategies related to or impacting such environment, and changes or deficiencies in the execution of the security plan required by subsection (d), long-term roadmap required by subsection (e), and business plan required by subsection (f).

(i) SUNSET.—The section shall have no effect on or after September 30, 2024.

SEC. 2313. REPORT ON DEVELOPMENT OF SECURE MOBILE VOICE SOLUTION FOR INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency and the Director of the National Security Agency, shall submit to the congressional intelligence committees a classified report on the feasibility, desirability, cost, and required schedule associated with the implementation of a secure mobile voice solution for the intelligence community.

(b) CONTENTS.—The report required by subsection (a) shall include, at a minimum, the following:

(1) The benefits and disadvantages of a secure mobile voice solution.

(2) Whether the intelligence community could leverage commercially available technology for classified voice communications that operates on commercial mobile networks in a secure manner and identifying the accompanying security risks to such networks.

(3) A description of any policies or community guidance that would be necessary to govern the potential solution, such as a process for determining the appropriate use of a secure mobile telephone and any limitations associated with such use.

SEC. 2314. POLICY ON MINIMUM INSIDER THREAT STANDARDS.

(a) POLICY REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence shall establish a policy for minimum insider threat standards that is consistent with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

(b) IMPLEMENTATION.—Not later than 180 days after the date of the enactment of this Act, the head of each element of the intelligence community shall implement the policy established under subsection (a).

SEC. 2315. SUBMISSION OF INTELLIGENCE COMMUNITY POLICIES.

(a) DEFINITIONS.—In this section:

(1) ELECTRONIC REPOSITORY.—The term "electronic repository" means the electronic distribution mechanism, in use as of the date of the enactment of this Act, or any successor electronic distribution mechanism, by which the Director of National Intelligence submits to the congressional intelligence committees information.

(2) POLICY.—The term "policy", with respect to the intelligence community, includes unclassified or classified—

(A) directives, policy guidance, and policy memoranda of the intelligence community;

(B) executive correspondence of the Director of National Intelligence; and

(C) any equivalent successor policy instruments.

(b) SUBMISSION OF POLICIES.—

(1) CURRENT POLICY.—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 using the electronic repository all nonpublicly available policies issued by the Director of National Intelligence for the intelligence community that are in effect as of the date of the submission.

(2) CONTINUOUS UPDATES.—Not later than 15 days after the date on which the Director of National Intelligence issues, modifies, or rescinds a policy of the intelligence community, the Director shall—

(A) notify the congressional intelligence committees of such addition, modification, or removal; and

(B) update the electronic repository with respect to such addition, modification, or removal.

SEC. 2316. EXPANSION OF INTELLIGENCE COMMUNITY RECRUITMENT EFFORTS.

In order to further increase the diversity of the intelligence community workforce, not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with heads of elements of the Intelligence Community, shall create, implement, and submit to the congressional intelligence committees a written plan to ensure that rural and underrepresented regions are more fully and consistently represented in such elements' employment recruitment efforts. Upon receipt of the plan, the congressional committees shall have 60 days to submit comments to the Director of National Intelligence before such plan shall be implemented.

TITLE XXIV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

SEC. 2401. AUTHORITY FOR PROTECTION OF CURRENT AND FORMER EMPLOYEES OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.

Section 5(a)(4) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3506(a)(4)) is amended by striking "such personnel of the Office of the Director of National Intelligence as the Director of National Intelligence may designate;" and inserting "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;".

SEC. 2402. DESIGNATION OF THE PROGRAM MANAGER-INFORMATION SHARING ENVIRONMENT.

(a) INFORMATION SHARING ENVIRONMENT.—Section 1016(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(b)) is amended—

(1) in paragraph (1), by striking "President" and inserting "Director of National Intelligence"; and

(2) in paragraph (2), by striking "President" both places that term appears and inserting "Director of National Intelligence".

(b) PROGRAM MANAGER.—Section 1016(f)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(f)(1)) is amended by striking "The individual designated as the program manager shall serve as program manager until removed from service or replaced by the President (at the President's sole discretion)." and inserting "Beginning on the date of the enactment of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019 and 2020, each individual designated as the program manager shall be appointed by the Director of National Intelligence.".

SEC. 2403. TECHNICAL MODIFICATION TO THE EXECUTIVE SCHEDULE.

Section 5315 of title 5, United States Code, is amended by adding at the end the following:

"Director of the National Counterintelligence and Security Center.".

SEC. 2404. CHIEF FINANCIAL OFFICER OF THE INTELLIGENCE COMMUNITY.

Section 103I(a) of the National Security Act of 1947 (50 U.S.C. 3034(a)) is amended by adding at the end the following new sentence: "The Chief Financial Officer shall report directly to the Director of National Intelligence.".

SEC. 2405. CHIEF INFORMATION OFFICER OF THE INTELLIGENCE COMMUNITY.

Section 103G(a) of the National Security Act of 1947 (50 U.S.C. 3032(a)) is amended by adding at the end the following new sentence: "The Chief Information Officer shall report directly to the Director of National Intelligence.".

Subtitle B—Central Intelligence Agency

SEC. 2411. CENTRAL INTELLIGENCE AGENCY SUBSISTENCE FOR PERSONNEL ASSIGNED TO AUSTERE LOCATIONS.

Subsection (a) of section 5 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3506) is amended—

(1) in paragraph (1), by striking "(50 U.S.C. 403–4a).," and inserting "(50 U.S.C. 403–4a),";

(2) in paragraph (6), by striking "and" at the end;

(3) in paragraph (7), by striking the period at the end and inserting "; and"; and

(4) by adding at the end the following new paragraph (8):

"(8) Upon the approval of the Director, provide, during any fiscal year, with or without reimbursement, subsistence to any personnel assigned to an overseas location designated by the Agency as an austere location.".

SEC. 2412. SPECIAL RULES FOR CERTAIN MONTHLY WORKERS' COMPENSATION PAYMENTS AND OTHER PAYMENTS FOR CENTRAL INTELLIGENCE AGENCY PERSONNEL.

(a) IN GENERAL.—The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.) is amended by inserting after section 19 the following new section:

"SEC. 19A. SPECIAL RULES FOR CERTAIN INDIVIDUALS INJURED BY REASON OF WAR, INSURGENCY, HOSTILE ACT, OR TERRORIST ACTIVITIES.

"(a) DEFINITIONS.—In this section:

"(1) COVERED DEPENDENT.—The term 'covered dependent' means a family member (as defined by the Director) of a covered employee who, on or after September 11, 2001—

"(A) accompanies the covered employee to an assigned duty station in a foreign country; and

"(B) becomes injured by reason of a qualifying injury.

"(2) COVERED EMPLOYEE.—The term 'covered employee' means an officer or employee of the Central Intelligence Agency who, on or after September 11, 2001, becomes injured by reason of a qualifying injury.

"(3) COVERED INDIVIDUAL.—The term 'covered individual' means an individual who—

"(A)(i) is detailed to the Central Intelligence Agency from other agencies of the United States Government or from the Armed Forces; or

"(ii) is affiliated with the Central Intelligence Agency, as determined by the Director; and

"(B) who, on or after September 11, 2001, becomes injured by reason of a qualifying injury.

"(4) QUALIFYING INJURY.—The term 'qualifying injury' means the following:

"(A) With respect to a covered dependent, an injury incurred—

"(i) during a period in which the covered dependent is accompanying the covered employee to an assigned duty station in a foreign country;

"(ii) in connection with war, insurgency, hostile act, terrorist activity, or other incident designated by the Director; and

"(iii) that was not the result of the willful misconduct of the covered dependent.

"(B) With respect to a covered employee or a covered individual, an injury incurred—

"(i) during a period of assignment to a duty station in a foreign country;

"(ii) in connection with a war, insurgency, hostile act, terrorist activity, or other incident designated by the Director; and

"(iii) that was not the result of the willful misconduct of the covered employee or the covered individual.

"(b) ADJUSTMENT OF COMPENSATION FOR CERTAIN INJURIES.—

"(1) INCREASE.—The Director may increase the amount of monthly compensation paid to a covered employee under section 8105 of title 5, United States Code. Subject to paragraph (2), the Director may determine the amount of each such increase by taking into account—

"(A) the severity of the qualifying injury;

"(B) the circumstances by which the covered employee became injured; and

"(C) the seniority of the covered employee.

"(2) MAXIMUM.—Notwithstanding chapter 81 of title 5, United States Code, the total amount of monthly compensation increased under paragraph (1) may not exceed the monthly pay of the maximum rate of basic pay for GS–15 of the General Schedule under section 5332 of such title.

"(c) COSTS FOR TREATING QUALIFYING INJURIES.—The Director may pay the costs of treating a qualifying injury of a covered employee, a covered individual, or a covered dependent, or may reimburse a covered employee, a covered individual, or a covered dependent for such costs, that are not otherwise covered by chapter 81 of title 5, United States Code, or other provision of Federal law.

"(d) TREATMENT OF AMOUNTS.—For purposes of section 104 of the Internal Revenue Code of 1986, amounts paid pursuant to this section shall be treated as amounts paid under chapter 81 of title 5, United States Code.".

(b) REGULATIONS.—Not later than 120 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall—

(1) prescribe regulations ensuring the fair and equitable implementation of section 19A of the Central Intelligence Agency Act of 1949, as added by subsection (a); and

(2) submit to the congressional intelligence committees such regulations.

(c) APPLICATION.—Section 19A of the Central Intelligence Agency Act of 1949, as added by subsection (a), shall apply with respect to—

(1) payments made to covered employees (as defined in such section) under section 8105 of title 5, United States Code, beginning on or after the date of the enactment of this Act; and

(2) treatment described in subsection (b) of such section 19A occurring on or after the date of the enactment of this Act.

SEC. 2413. EXPANSION OF SECURITY PROTECTIVE SERVICE JURISDICTION OF THE CENTRAL INTELLIGENCE AGENCY.

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

(1) in subparagraph (B), by striking "500 feet;" and inserting "500 yards;"; and

(2) in subparagraph (D), by striking "500 feet." and inserting "500 yards.".

SEC. 2414. REPEAL OF FOREIGN LANGUAGE PROFICIENCY REQUIREMENT FOR CERTAIN SENIOR LEVEL POSITIONS IN THE CENTRAL INTELLIGENCE AGENCY.

(a) REPEAL OF FOREIGN LANGUAGE PROFICIENCY REQUIREMENT.—Section 104A of the National Security Act of 1947 (50 U.S.C. 3036) is amended by striking subsection (g).

(b) CONFORMING REPEAL OF REPORT REQUIREMENT.—Section 611 of the Intelligence Authorization Act for Fiscal Year 2005 (Public Law 108–487) is amended by striking subsection (c).

Subtitle C—Office of Intelligence and Counterintelligence of Department of Energy

SEC. 2421. CONSOLIDATION OF DEPARTMENT OF ENERGY OFFICES OF INTELLIGENCE AND COUNTERINTELLIGENCE.

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

"OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

"SEC. 215. (a) DEFINITIONS.—In this section, the terms 'intelligence community' and 'National Intelligence Program' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

"(b) IN GENERAL.—There is in the Department an Office of Intelligence and Counterintelligence. Such office shall be under the National Intelligence Program.

"(c) DIRECTOR.—(1) The head of the Office shall be the Director of the Office of Intelligence and Counterintelligence, who shall be an employee in the Senior Executive Service, the Senior Intelligence Service, the Senior National Intelligence Service, or any other Service that the Secretary, in coordination with the Director of National Intelligence, considers appropriate. The Director of the Office shall report directly to the Secretary.

"(2) The Secretary shall select an individual to serve as the Director from among individuals who have substantial expertise in matters relating to the intelligence community, including foreign intelligence and counterintelligence.

"(d) DUTIES.—(1) Subject to the authority, direction, and control of the Secretary, the Director shall perform such duties and exercise such powers as the Secretary may prescribe.

"(2) The Director shall be responsible for establishing policy for intelligence and counterintelligence programs and activities at the Department.".

(b) CONFORMING REPEAL.—Section 216 of the Department of Energy Organization Act (42 U.S.C. 7144c) is hereby repealed.

(c) CLERICAL AMENDMENT.—The table of contents at the beginning of the Department of Energy Organization Act is amended by striking the items relating to sections 215 and 216 and inserting the following new item:

"Sec. 215. Office of Intelligence and Counterintelligence.".

SEC. 2422. ESTABLISHMENT OF ENERGY INFRASTRUCTURE SECURITY CENTER.

Section 215 of the Department of Energy Organization Act (42 U.S.C. 7144b), as amended by section 2421, is further amended by adding at the end the following:

"(e) ENERGY INFRASTRUCTURE SECURITY CENTER.—(1)(A) The President shall establish an Energy Infrastructure Security Center, taking into account all appropriate government tools to analyze and disseminate intelligence relating to the security of the energy infrastructure of the United States.

"(B) The Director of Intelligence and Counterintelligence shall appoint the head of the Energy Infrastructure Security Center.

"(C) The Energy Infrastructure Security Center shall be located within the Office of Intelligence and Counterintelligence.

"(2) In establishing the Energy Infrastructure Security Center, the Director of the Office of Intelligence and Counterintelligence shall address the following missions

and objectives to coordinate and disseminate intelligence relating to the security of the energy infrastructure of the United States:

"(A) Establishing a primary organization within the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to the security of the energy infrastructure of the United States.

"(B) Ensuring that appropriate departments and agencies have full access to and receive intelligence support needed to execute the plans or activities of the agencies, and perform independent, alternative analyses.

"(C) Establishing a central repository on known and suspected foreign threats to the energy infrastructure of the United States, including with respect to any individuals, groups, or entities engaged in activities targeting such infrastructure, and the goals, strategies, capabilities, and networks of such individuals, groups, or entities.

"(D) Disseminating intelligence information relating to the security of the energy infrastructure of the United States, including threats and analyses, to the President, to the appropriate departments and agencies, and to the appropriate committees of Congress.

"(3) The President may waive the requirements of this subsection, and any parts thereof, if the President determines that such requirements do not materially improve the ability of the United States Government to prevent and halt attacks against the energy infrastructure of the United States. Such waiver shall be made in writing to Congress and shall include a description of how the missions and objectives in paragraph (2) are being met.

"(4) If the President decides not to exercise the waiver authority granted by paragraph (3), the President shall submit to Congress from time to time updates and plans regarding the establishment of an Energy Infrastructure Security Center.".

SEC. 2423. REPEAL OF DEPARTMENT OF ENERGY INTELLIGENCE EXECUTIVE COMMITTEE AND BUDGET REPORTING REQUIREMENT.

Section 214 of the Department of Energy Organization Act (42 U.S.C. 7144a) is amended—

(1) by striking "(a)"; and

(2) by striking subsections (b) and (c).

Subtitle D—Other Elements

SEC. 2431. PLAN FOR DESIGNATION OF COUNTERINTELLIGENCE COMPONENT OF DEFENSE SECURITY SERVICE AS AN ELEMENT OF INTELLIGENCE COMMUNITY.

Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence and Under Secretary of Defense for Intelligence, in coordination with the Director of the National Counterintelligence and Security Center, shall submit to the congressional intelligence committees, the Committee on Armed Services of the Senate, and the Committee on Armed Services of the House of Representatives a plan to designate the counterintelligence component of the Defense Security Service of the Department of Defense as an element of the intelligence community by not later than January 1, 2020. Such plan shall—

(1) address the implications of such designation on the authorities, governance, personnel, resources, information technology, collection, analytic products, information sharing, and business processes of the Defense Security Service and the intelligence community; and

(2) not address the personnel security functions of the Defense Security Service.

SEC. 2432. NOTICE NOT REQUIRED FOR PRIVATE ENTITIES.

Section 3553 of title 44, United States Code, is amended—

(1) by redesignating subsection (j) as subsection (k); and

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

"(j) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Secretary to provide notice to any private entity before the Secretary issues a binding operational directive under subsection (b)(2).".

SEC. 2433. ESTABLISHMENT OF ADVISORY BOARD FOR NATIONAL RECONNAISSANCE OFFICE.

(a) ESTABLISHMENT.—Section 106A of the National Security Act of 1947 (50 U.S.C. 3041a) is amended by adding at the end the following new subsection:

"(d) ADVISORY BOARD.—

"(1) ESTABLISHMENT.—There is established in the National Reconnaissance Office an advisory board (in this section referred to as the 'Board').

"(2) DUTIES.—The Board shall—

"(A) study matters relating to the mission of the National Reconnaissance Office, including with respect to promoting innovation, competition, and resilience in space, overhead reconnaissance, acquisition, and other matters; and

"(B) advise and report directly to the Director with respect to such matters.

"(3) MEMBERS.—

"(A) NUMBER AND APPOINTMENT.—

"(i) IN GENERAL.—The Board shall be composed of 5 members appointed by the Director from among individuals with demonstrated academic, government, business, or other expertise relevant to the mission and functions of the National Reconnaissance Office.

"(ii) NOTIFICATION.—Not later than 30 days after the date on which the Director appoints a member to the Board, the Director shall notify the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) of such appointment.

"(B) TERMS.—Each member shall be appointed for a term of 2 years. Except as provided by subparagraph (C), a member may not serve more than 3 terms.

"(C) VACANCY.—Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has taken office.

"(D) CHAIR.—The Board shall have a Chair, who shall be appointed by the Director from among the members.

"(E) TRAVEL EXPENSES.—Each member shall 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.

"(F) EXECUTIVE SECRETARY.—The Director may appoint an executive secretary, who shall be an employee of the National Reconnaissance Office, to support the Board.

"(4) MEETINGS.—The Board shall meet not less than quarterly, but may meet more frequently at the call of the Director.

"(5) REPORTS.—Not later than March 31 of each year, the Board shall submit to the Director and to the congressional intelligence committees a report on the activities and significant findings of the Board during the preceding year.

"(6) NONAPPLICABILITY OF CERTAIN REQUIREMENTS.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Board.

"(7) TERMINATION.—The Board shall terminate on the date that is 3 years after the date of the first meeting of the Board.".

(b) INITIAL APPOINTMENTS.—Not later than 180 days after the date of the enactment of this Act, the Director of the National Reconnaissance Office shall appoint the initial 5 members to the advisory board under subsection (d) of section 106A of the National Security Act of 1947 (50 U.S.C. 3041a), as added by subsection (a).

SEC. 2434. COLLOCATION OF CERTAIN DEPARTMENT OF HOMELAND SECURITY PERSONNEL AT FIELD LOCATIONS.

(a) IDENTIFICATION OF OPPORTUNITIES FOR COLLOCATION.—Not later than 60 days after the date of the enactment of this Act, the Under Secretary of Homeland Security for Intelligence and Analysis shall identify, in consultation with the Commissioner of U.S. Customs and Border Protection, the Administrator of the Transportation Security Administration, the Director of U.S. Immigration and Customs Enforcement, and the heads of such other elements of the Department of Homeland Security as the Under Secretary considers appropriate, opportunities for collocation of officers of the Office of Intelligence and Analysis in the field outside of the greater Washington, District of Columbia, area in order to support operational units from U.S. Customs and Border Protection, the Transportation Security Administration, U.S. Immigration and Customs Enforcement, and other elements of the Department of Homeland Security.

(b) PLAN FOR COLLOCATION.—Not later than 120 days after the date of the enactment of this Act, the Under Secretary shall submit to the congressional intelligence committees a report that includes a plan for collocation as described in subsection (a).

TITLE XXV—ELECTION MATTERS

SEC. 2501. REPORT ON CYBER ATTACKS BY FOREIGN GOVERNMENTS AGAINST UNITED STATES ELECTION INFRASTRUCTURE.

(a) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

(C) the Committee on Homeland Security of the House of Representatives;

(D) the Committee on Foreign Relations of the Senate; and

(E) the Committee on Foreign Affairs of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term "congressional leadership" includes the following:

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

(D) The minority leader of the House of Representatives.

(3) STATE.—The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(b) REPORT REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Under Secretary of Homeland Security for Intelligence and Analysis shall submit to congressional leadership and the appropriate congressional committees a report on cyber attacks and attempted cyber attacks by foreign governments on United States election infrastructure in States and localities in connection with the 2016 Presidential election in the United States and such cyber attacks or attempted cyber attacks as the Under Secretary anticipates against such infrastructure. Such report shall identify the States and localities affected and shall include cyber attacks and attempted cyber attacks against voter registration databases, voting machines, voting-related computer networks, and the networks of Secretaries of State and other election officials of the various States.

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

SEC. 2502. REVIEW OF INTELLIGENCE COMMUNITY'S POSTURE TO COLLECT AGAINST AND ANALYZE RUSSIAN EFFORTS TO INFLUENCE THE PRESIDENTIAL ELECTION.

(a) REVIEW REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence shall—

(1) complete an after action review of the posture of the intelligence community to collect against and analyze efforts of the Government of Russia to interfere in the 2016 Presidential election in the United States; and

(2) submit to the congressional intelligence committees a report on the findings of the Director with respect to such review.

(b) ELEMENTS.—The review required by subsection (a) shall include, with respect to the posture and efforts described in paragraph (1) of such subsection, the following:

(1) An assessment of whether the resources of the intelligence community were properly aligned to detect and respond to the efforts described in subsection (a)(1).

(2) An assessment of the information sharing that occurred within elements of the intelligence community.

(3) An assessment of the information sharing that occurred between elements of the intelligence community.

(4) An assessment of applicable authorities necessary to collect on any such efforts and any deficiencies in those authorities.

(5) A review of the use of open source material to inform analysis and warning of such efforts.

(6) A review of the use of alternative and predictive analysis.

(c) FORM OF REPORT.—The report required by subsection (a)(2) shall be submitted to the congressional intelligence committees in a classified form.

SEC. 2503. ASSESSMENT OF FOREIGN INTELLIGENCE THREATS TO FEDERAL ELECTIONS.

(a) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Homeland Security of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term "congressional leadership" includes the following:

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

(D) The minority leader of the House of Representatives.

(3) SECURITY VULNERABILITY.—The term "security vulnerability" has the meaning given such term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(b) IN GENERAL.—The Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the National Security Agency, the Director of the Federal Bureau of Investigation, the Secretary of Homeland Security, and the heads of other relevant elements of the intelligence community, shall—

(1) commence not later than 1 year before any regularly scheduled Federal election occurring after December 31, 2018, and complete not later than 180 days before such election, an assessment of security vulnerabilities of State election systems; and

(2) not later than 180 days before any regularly scheduled Federal election occurring after December 31, 2018, submit a report on such security vulnerabilities and an assessment of foreign intelligence threats to the election to—

(A) congressional leadership; and

(B) the appropriate congressional committees.

(c) UPDATE.—Not later than 90 days before any regularly scheduled Federal election occurring after December 31, 2018, the Director of National Intelligence shall—

(1) update the assessment of foreign intelligence threats to that election; and

(2) submit the updated assessment to—

(A) congressional leadership; and

(B) the appropriate congressional committees.

SEC. 2504. STRATEGY FOR COUNTERING RUSSIAN CYBER THREATS TO UNITED STATES ELECTIONS.

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

(1) The congressional intelligence committees.

(2) The Committee on Armed Services and the Committee on Homeland Security and Governmental Affairs of the Senate.

(3) The Committee on Armed Services and the Committee on Homeland Security of the House of Representatives.

(4) The Committee on Foreign Relations of the Senate.

(5) The Committee on Foreign Affairs of the House of Representatives.

(b) REQUIREMENT FOR A STRATEGY.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Secretary of Homeland Security, the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, the Secretary of State, the Secretary of Defense, and the Secretary of the Treasury, shall develop a whole-of-government strategy for countering the threat of Russian cyber attacks and attempted cyber attacks against electoral systems and processes in the United States, including Federal, State, and local election systems, voter registration databases, voting tabulation equipment, and equipment and processes for the secure transmission of election results.

(c) ELEMENTS OF THE STRATEGY.—The strategy required by subsection (b) shall include the following elements:

(1) A whole-of-government approach to protecting United States electoral systems and processes that includes the agencies and departments indicated in subsection (b) as well as any other agencies and departments of the United States, as determined appropriate by the Director of National Intelligence and the Secretary of Homeland Security.

(2) Input solicited from Secretaries of State of the various States and the chief election officials of the States.

(3) Technical security measures, including auditable paper trails for voting machines, securing wireless and Internet connections, and other technical safeguards.

(4) Detection of cyber threats, including attacks and attempted attacks by Russian government or nongovernment cyber threat actors.

(5) Improvements in the identification and attribution of Russian government or nongovernment cyber threat actors.

(6) Deterrence, including actions and measures that could or should be undertaken against or communicated to the Government of Russia or other entities to deter attacks against, or interference with, United States election systems and processes.

(7) Improvements in Federal Government communications with State and local election officials.

(8) Public education and communication efforts.

(9) Benchmarks and milestones to enable the measurement of concrete steps taken and progress made in the implementation of the strategy.

(d) CONGRESSIONAL BRIEFING.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence and the Secretary of Homeland Security shall jointly brief the appropriate congressional committees on the strategy developed under subsection (b).

SEC. 2505. ASSESSMENT OF SIGNIFICANT RUSSIAN INFLUENCE CAMPAIGNS DIRECTED AT FOREIGN ELECTIONS AND REFERENDA.

(a) RUSSIAN INFLUENCE CAMPAIGN DEFINED.—In this section, the term "Russian influence campaign" means any effort, covert or overt, and by any means, attributable to the Russian Federation directed at an election, referendum, or similar process in a country other than the Russian Federation or the United States.

(b) ASSESSMENT REQUIRED.—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 a report containing an analytical assessment of the most significant Russian influence campaigns, if any, conducted during the 3-year period preceding the date of the enactment of this Act, as well as the most significant current or planned such Russian influence campaigns, if any. Such assessment shall include—

(1) a summary of such significant Russian influence campaigns, including, at a minimum, the specific means by which such campaigns were conducted, are being conducted, or likely will be conducted, as appropriate, and the specific goal of each such campaign;

(2) a summary of any defenses against or responses to such Russian influence campaigns by the foreign state holding the elections or referenda;

(3) a summary of any relevant activities by elements of the intelligence community undertaken for the purpose of assisting the government of such foreign state in defending against or responding to such Russian influence campaigns; and

(4) an assessment of the effectiveness of such defenses and responses described in paragraphs (2) and (3).

(c) FORM.—The report required by subsection (b) may be submitted in classified form, but if so submitted, shall contain an unclassified summary.

SEC. 2506. INFORMATION SHARING WITH STATE ELECTION OFFICIALS.

(a) STATE DEFINED.—In this section, the term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(b) SECURITY CLEARANCES.—

(1) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall support the Under Secretary of Homeland Security for Intelligence and Analysis, and any other official of the Department of Homeland Security designated by the Secretary of Homeland Security, in sponsoring a security clearance up to the top secret level for each eligible chief election official of a State or the District of Columbia, and additional eligible designees of such election official as appropriate, at the time that such election official assumes such position.

(2) INTERIM CLEARANCES.—Consistent with applicable policies and directives, the Director of National Intelligence may issue interim clearances, for a period to be determined by the Director, to a chief election official as described in paragraph (1) and up to 1 designee of such official under such paragraph.

(c) INFORMATION SHARING.—

(1) IN GENERAL.—The Director of National Intelligence shall assist the Under Secretary of Homeland Security for Intelligence and Analysis and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department (as specified in section 103(a)(1)(H) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)(H))) with sharing any appropriate classified information related to threats to election systems and to the integrity of the election process with chief election officials and such designees who have received a security clearance under subsection (b).

(2) COORDINATION.—The Under Secretary of Homeland Security for Intelligence and Analysis shall coordinate with the Director of National Intelligence and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department (as specified in section 103(a)(1)(H) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)(H))) to facilitate the sharing of information to the affected Secretaries of State or States.

SEC. 2507. NOTIFICATION OF SIGNIFICANT FOREIGN CYBER INTRUSIONS AND ACTIVE MEASURES CAMPAIGNS DIRECTED AT ELECTIONS FOR FEDERAL OFFICES.

(a) DEFINITIONS.—In this section:

(1) ACTIVE MEASURES CAMPAIGN.—The term "active measures campaign" means a foreign semi-covert or covert intelligence operation.

(2) CANDIDATE, ELECTION, AND POLITICAL PARTY.—The terms "candidate", "election", and "political party" have the meanings given those terms in section 301 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101).

(3) CONGRESSIONAL LEADERSHIP.—The term "congressional leadership" includes the following:

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

(D) The minority leader of the House of Representatives.

(4) CYBER INTRUSION.—The term "cyber intrusion" means an electronic occurrence that actually or imminently jeopardizes, without lawful authority, electronic election infrastructure, or the integrity, confidentiality, or availability of information within such infrastructure.

(5) ELECTRONIC ELECTION INFRASTRUCTURE.—The term "electronic election infrastructure" means an electronic information system of any of the following that is related to an election for Federal office:

(A) The Federal Government.

(B) A State or local government.

(C) A political party.

(D) The election campaign of a candidate.

(6) FEDERAL OFFICE.—The term "Federal office" has the meaning given that term in section 301 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101).

(7) HIGH CONFIDENCE.—The term "high confidence", with respect to a determination, means that the determination is based on high-quality information from multiple sources.

(8) MODERATE CONFIDENCE.—The term "moderate confidence", with respect to a determination, means that a determination is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.

(9) OTHER APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "other appropriate congressional committees" means—

(A) the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(b) DETERMINATIONS OF SIGNIFICANT FOREIGN CYBER INTRUSIONS AND ACTIVE MEASURES CAMPAIGNS.—The Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Secretary of Homeland Security shall jointly carry out subsection (c) if such Directors and the Secretary jointly determine—

(1) that on or after the date of the enactment of this Act, a significant foreign cyber intrusion or active measures campaign intended to influence an upcoming election for any Federal office has occurred or is occurring; and

(2) with moderate or high confidence, that such intrusion or campaign can be attributed to a foreign state or to a foreign nonstate person, group, or other entity.

(c) BRIEFING.—

(1) IN GENERAL.—Not later than 14 days after making a determination under subsection (b), the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Secretary of Homeland Security shall jointly provide a briefing to the congressional leadership, the congressional intelligence committees and, consistent with the protection of sources and methods, the other appropriate congressional committees. The briefing shall be classified and address, at a minimum, the following:

(A) A description of the significant foreign cyber intrusion or active measures campaign, as the case may be, covered by the determination.

(B) An identification of the foreign state or foreign nonstate person, group, or other entity, to which such intrusion or campaign has been attributed.

(C) The desirability and feasibility of the public release of information about the cyber intrusion or active measures campaign.

(D) Any other information such Directors and the Secretary jointly determine appropriate.

(2) ELECTRONIC ELECTION INFRASTRUCTURE BRIEFINGS.—With respect to a significant foreign cyber intrusion covered by a determination under subsection (b), the Secretary of Homeland Security, in consultation with the Director of National Intelligence and the Director of the Federal Bureau of Investigation, shall offer to the owner or operator of any electronic election infrastructure directly affected by such intrusion, a briefing on such intrusion, including steps that may be taken to mitigate such intrusion. Such briefing may be classified and made available only to individuals with appropriate security clearances.

(3) PROTECTION OF SOURCES AND METHODS.—This subsection shall be carried out in a manner that is consistent with the protection of sources and methods.

SEC. 2508. DESIGNATION OF COUNTERINTELLIGENCE OFFICER TO LEAD ELECTION SECURITY MATTERS.

(a) IN GENERAL.—The Director of National Intelligence shall designate a national counterintelligence officer within the National Counterintelligence and Security Center to lead, manage, and coordinate counterintelligence matters relating to election security.

(b) ADDITIONAL RESPONSIBILITIES.—The person designated under subsection (a) shall also lead, manage, and coordinate counterintelligence matters relating to risks posed by interference from foreign powers (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)) to the following:

(1) The Federal Government election security supply chain.

(2) Election voting systems and software.

(3) Voter registration databases.

(4) Critical infrastructure related to elections.

(5) Such other Government goods and services as the Director of National Intelligence considers appropriate.

TITLE XXVI—SECURITY CLEARANCES

SEC. 2601. DEFINITIONS.

In this title:

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

(A) the congressional intelligence committees;

(B) the Committee on Armed Services of the Senate;

(C) the Committee on Appropriations of the Senate;

(D) the Committee on Homeland Security and Governmental Affairs of the Senate;

(E) the Committee on Armed Services of the House of Representatives;

(F) the Committee on Appropriations of the House of Representatives;

(G) the Committee on Homeland Security of the House of Representatives; and

(H) the Committee on Oversight and Reform of the House of Representatives.

(2) APPROPRIATE INDUSTRY PARTNERS.—The term "appropriate industry partner" means a contractor, licensee, or grantee (as defined in section 101(a) of Executive Order 12829 (50 U.S.C. 3161 note; relating to National Industrial Security Program)) that is participating in the National Industrial Security Program established by such Executive Order.

(3) CONTINUOUS VETTING.—The term "continuous vetting" has the meaning given such term in Executive Order 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for government employment, fitness for contractor employees, and eligibility for access to classified national security information).

(4) COUNCIL.—The term "Council" means the Security, Suitability, and Credentialing Performance Accountability Council established pursuant to such Executive Order, or any successor entity.

(5) SECURITY EXECUTIVE AGENT.—The term "Security Executive Agent" means the officer serving as the Security Executive Agent pursuant to section 803 of the National Security Act of 1947, as added by section 2605.

(6) SUITABILITY AND CREDENTIALING EXECUTIVE AGENT.—The term "Suitability and Credentialing Executive Agent" means the Director of the Office of Personnel Management acting as the Suitability and Credentialing Executive Agent in accordance with Executive Order 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for government employment, fitness for contractor employees, and eligibility for access to classified national security information), or any successor entity.

SEC. 2602. REPORTS AND PLANS RELATING TO SECURITY CLEARANCES AND BACKGROUND INVESTIGATIONS.

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

(1) ensuring the trustworthiness and security of the workforce, facilities, and information of the Federal Government is of the highest priority to national security and public safety;

(2) the President and Congress should prioritize the modernization of the personnel security framework to improve its efficiency, effectiveness, and accountability;

(3) the current system for security clearance, suitability and fitness for employment, and credentialing lacks efficiencies and capabilities to meet the current threat environment, recruit and retain a trusted workforce, and capitalize on modern technologies; and

(4) changes to policies or processes to improve this system should be vetted through the Council to ensure standardization, portability, and reciprocity in security clearances across the Federal Government.

(b) ACCOUNTABILITY PLANS AND REPORTS.—

(1) PLANS.—Not later than 90 days after the date of the enactment of this Act, the Council shall submit to the appropriate congressional committees and make available to appropriate industry partners the following:

(A) A plan, with milestones, to reduce the background investigation inventory to 200,000, or an otherwise sustainable steady-level, by the end of year 2020. Such plan shall include notes of any required changes in investigative and adjudicative standards or resources.

(B) A plan to consolidate the conduct of background investigations associated with the processing for security clearances in the most effective and efficient manner between the National Background Investigation Bureau and the Defense Security Service, or a successor organization. Such plan shall address required funding, personnel, contracts, information technology, field office structure, policy, governance, schedule, transition costs, and effects on stakeholders.

(2) REPORT ON THE FUTURE OF PERSONNEL SECURITY.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Chairman of the Council, in coordination with the members of the Council, shall submit to the appropriate congressional committees and make available to appropriate industry partners a report on the future of personnel security to reflect changes in threats, the workforce, and technology.

(B) CONTENTS.—The report submitted under subparagraph (A) shall include the following:

(i) A risk framework for granting and renewing access to classified information.

(ii) A discussion of the use of technologies to prevent, detect, and monitor threats.

(iii) A discussion of efforts to address reciprocity and portability.

(iv) A discussion of the characteristics of effective insider threat programs.

(v) An analysis of how to integrate data from continuous evaluation, insider threat programs, and human resources data.

(vi) Recommendations on interagency governance.

(3) PLAN FOR IMPLEMENTATION.—Not later than 180 days after the date of the enactment of this Act, the Chairman of the Council, in coordination with the members of the Council, shall submit to the appropriate congressional committees and make available to appropriate industry partners a plan to implement the report's framework and recommendations submitted under paragraph (2)(A).

(4) CONGRESSIONAL NOTIFICATIONS.—Not less frequently than quarterly, the Security Executive Agent shall make available to the public a report regarding the status of the disposition of requests received from departments and agencies of the Federal Government for a change to, or approval under, the Federal investigative standards, the national adjudicative guidelines, continuous evaluation, or other national policy regarding personnel security.

SEC. 2603. IMPROVING THE PROCESS FOR SECURITY CLEARANCES.

(a) REVIEWS.—Not later than 180 days after the date of the enactment of this Act, the Security Executive Agent, in coordination with the members of the Council, shall submit to the appropriate congressional committees and make available to appropriate industry partners a report that includes the following:

(1) A review of whether the information requested on the Questionnaire for National Security Positions (Standard Form 86) and by the Federal Investigative Standards prescribed by the Office of Personnel Management and the Office of the Director of National Intelligence appropriately supports the adjudicative guidelines under Security Executive Agent Directive 4 (known as the "National Security Adjudicative Guidelines"). Such review shall include identification of whether any such information currently collected is unnecessary to support the adjudicative guidelines.

(2) An assessment of whether such Questionnaire, Standards, and guidelines should be revised to account for the prospect of a holder of a security clearance becoming an insider threat.

(3) Recommendations to improve the background investigation process by—

(A) simplifying the Questionnaire for National Security Positions (Standard Form 86) and increasing customer support to applicants completing such Questionnaire;

(B) using remote techniques and centralized locations to support or replace field investigation work;

(C) using secure and reliable digitization of information obtained during the clearance process;

(D) building the capacity of the background investigation labor sector; and

(E) replacing periodic reinvestigations with continuous evaluation techniques in all appropriate circumstances.

(b) POLICY, STRATEGY, AND IMPLEMENTATION.—Not later than 180 days after the date of the enactment of this Act, the Security Executive Agent shall, in coordination with the members of the Council, establish the following:

(1) A policy and implementation plan for the issuance of interim security clearances.

(2) A policy and implementation plan to ensure contractors are treated consistently in the security clearance process across agencies and departments of the United States as compared to employees of such agencies and departments. Such policy shall address—

(A) prioritization of processing security clearances based on the mission the contractors will be performing;

(B) standardization in the forms that agencies issue to initiate the process for a security clearance;

(C) digitization of background investigation-related forms;

(D) use of the polygraph;

(E) the application of the adjudicative guidelines under Security Executive Agent Directive 4 (known as the "National Security Adjudicative Guidelines");

(F) reciprocal recognition of clearances across agencies and departments of the United States, regardless of status of periodic reinvestigation;

(G) tracking of clearance files as individuals move from employment with an agency or department of the United States to employment in the private sector;

(H) collection of timelines for movement of contractors across agencies and departments;

(I) reporting on security incidents and job performance, consistent with section 552a of title 5, United States Code (commonly known as the "Privacy Act of 1974"), that may affect the ability to hold a security clearance;

(J) any recommended changes to the Federal Acquisition Regulations (FAR) necessary to ensure that information affecting contractor clearances or suitability is appropriately and expeditiously shared between and among agencies and contractors; and

(K) portability of contractor security clearances between or among contracts at the same agency and between or among contracts at different agencies that require the same level of clearance.

(3) A strategy and implementation plan that—

(A) provides for periodic reinvestigations as part of a security clearance determination only on an as-needed, risk-based basis;

(B) includes actions to assess the extent to which automated records checks and other continuous evaluation methods may be used to expedite or focus reinvestigations; and

(C) provides an exception for certain populations if the Security Executive Agent—

(i) determines such populations require reinvestigations at regular intervals; and

(ii) provides written justification to the appropriate congressional committees for any such determination.

(4) A policy and implementation plan for agencies and departments of the United States, as a part of the security clearance process, to accept automated records checks generated pursuant to a security clearance applicant's employment with a prior employer.

(5) A policy for the use of certain background materials on individuals collected by the private sector for background investigation purposes.

(6) Uniform standards for agency continuous evaluation programs to ensure quality and reciprocity in accepting enrollment in a continuous vetting program as a substitute for a periodic investigation for continued access to classified information.

SEC. 2604. GOALS FOR PROMPTNESS OF DETERMINATIONS REGARDING SECURITY CLEARANCES.

(a) RECIPROCITY DEFINED.—In this section, the term "reciprocity" means reciprocal recognition by Federal departments and agencies of eligibility for access to classified information.

(b) IN GENERAL.—The Council shall reform the security clearance process with the objective that, by December 31, 2021, 90 percent of all determinations, other than determinations regarding populations identified under section 2603(b)(3)(C), regarding—

(1) security clearances—

(A) at the secret level are issued in 30 days or fewer; and

(B) at the top secret level are issued in 90 days or fewer; and

(2) reciprocity of security clearances at the same level are recognized in 2 weeks or fewer.

(c) CERTAIN REINVESTIGATIONS.—The Council shall reform the security clearance process with the goal that by December 31, 2021, reinvestigation on a set periodicity is not required for more than 10 percent of the population that holds a security clearance.

(d) EQUIVALENT METRICS.—

(1) IN GENERAL.—If the Council develops a set of performance metrics that it certifies to the appropriate congressional committees should achieve substantially equivalent outcomes as those outlined in subsections (b) and (c), the Council may use those metrics for purposes of compliance within this provision.

(2) NOTICE.—If the Council uses the authority provided by paragraph (1) to use metrics as described in such paragraph, the Council shall, not later than 30 days after communicating such metrics to departments and agencies, notify the appropriate congressional committees that it is using such authority.

(e) PLAN.—Not later than 180 days after the date of the enactment of this Act, the Council shall submit to the appropriate congressional committees and make available to appropriate industry partners a plan to carry out this section. Such plan shall include recommended interim milestones for the goals set forth in subsections (b) and (c) for 2019, 2020, and 2021.

SEC. 2605. SECURITY EXECUTIVE AGENT.

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

(1) by redesignating sections 803 and 804 as sections 804 and 805, respectively; and

(2) by inserting after section 802 the following:

"SEC. 803. SECURITY EXECUTIVE AGENT.

"(a) IN GENERAL.—The Director of National Intelligence, or such other officer of the United States as the President may designate, shall serve as the Security Executive Agent for all departments and agencies of the United States.

"(b) DUTIES.—The duties of the Security Executive Agent are as follows:

"(1) To direct the oversight of investigations, reinvestigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information or eligibility to hold a sensitive position made by any Federal agency.

"(2) To review the national security background investigation and adjudication programs of Federal agencies to determine whether such programs are being implemented in accordance with this section.

"(3) To develop and issue uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations,

polygraphs, and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position.

"(4) Unless otherwise designated by law, to serve as the final authority to designate a Federal agency or agencies to conduct investigations of persons who are proposed for access to classified information or for eligibility to hold a sensitive position to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position, as applicable.

"(5) Unless otherwise designated by law, to serve as the final authority to designate a Federal agency or agencies to determine eligibility for access to classified information or eligibility to hold a sensitive position in accordance with Executive Order 12968 (50 U.S.C. 3161 note; relating to access to classified information).

"(6) To ensure reciprocal recognition of eligibility for access to classified information or eligibility to hold a sensitive position among Federal agencies, including acting as the final authority to arbitrate and resolve disputes among such agencies involving the reciprocity of investigations and adjudications of eligibility.

"(7) To execute all other duties assigned to the Security Executive Agent by law.

"(c) AUTHORITIES.—The Security Executive Agent shall—

"(1) issue guidelines and instructions to the heads of Federal agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and security in processes relating to determinations by such agencies of eligibility for access to classified information or eligibility to hold a sensitive position, including such matters as investigations, polygraphs, adjudications, and reciprocity;

"(2) have the authority to grant exceptions to, or waivers of, national security investigative requirements, including issuing implementing or clarifying guidance, as necessary;

"(3) have the authority to assign, in whole or in part, to the head of any Federal agency (solely or jointly) any of the duties of the Security Executive Agent described in subsection (b) or the authorities described in paragraphs (1) and (2), provided that the exercise of such assigned duties or authorities is subject to the oversight of the Security Executive Agent, including such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate; and

"(4) define and set standards for continuous evaluation for continued access to classified information and for eligibility to hold a sensitive position.".

(b) REPORT ON RECOMMENDATIONS FOR REVISING AUTHORITIES.—Not later than 30 days after the date on which the Chairman of the Council submits to the appropriate congressional committees the report required by section 2602(b)(2)(A), the Chairman shall submit to the appropriate congressional committees such recommendations as the Chairman may have for revising the authorities of the Security Executive Agent.

(c) CONFORMING AMENDMENT.—Section 103H(j)(4)(A) of such Act (50 U.S.C. 3033(j)(4)(A)) is amended by striking "in section 804" and inserting "in section 805".

(d) CLERICAL AMENDMENT.—The table of contents in the matter preceding section 2 of such Act (50 U.S.C. 3002) is amended by striking the items relating to sections 803 and 804 and inserting the following:

"Sec. 803. Security Executive Agent.
"Sec. 804. Exceptions.
"Sec. 805. Definitions.".

SEC. 2606. REPORT ON UNIFIED, SIMPLIFIED, GOVERNMENTWIDE STANDARDS FOR POSITIONS OF TRUST AND SECURITY CLEARANCES.

Not later than 90 days after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent, in coordination with the other members of the Council, shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a report regarding the advisability and the risks, benefits, and costs to the Government and to industry of consolidating to not more than 3 tiers for positions of trust and security clearances.

SEC. 2607. REPORT ON CLEARANCE IN PERSON CONCEPT.

(a) SENSE OF CONGRESS.—It is the sense of Congress that to reflect the greater mobility of the modern workforce, alternative methodologies merit analysis to allow greater flexibility for individuals moving in and out of positions that require access to classified information, while still preserving security.

(b) REPORT REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Security Executive Agent shall submit to the appropriate congressional committees and make available to appropriate industry partners a report that describes the requirements, feasibility, and advisability of implementing a clearance in person concept described in subsection (c).

(c) CLEARANCE IN PERSON CONCEPT.—The clearance in person concept—

(1) permits an individual who once held a security clearance to maintain his or her eligibility for access to classified information, networks, and facilities for up to 3 years after the individual's eligibility for access to classified information would otherwise lapse; and

(2) recognizes, unless otherwise directed by the Security Executive Agent, an individual's security clearance and background investigation as current, regardless of employment status, contingent on enrollment in a continuous vetting program.

(d) CONTENTS.—The report required under subsection (b) shall address—

(1) requirements for an individual to voluntarily remain in a continuous evaluation program validated by the Security Executive Agent even if the individual is not in a position requiring access to classified information;

(2) appropriate safeguards for privacy;

(3) advantages to government and industry;

(4) the costs and savings associated with implementation;

(5) the risks of such implementation, including security and counterintelligence risks;

(6) an appropriate funding model; and

(7) fairness to small companies and independent contractors.

SEC. 2608. REPORTS ON RECIPROCITY FOR SECURITY CLEARANCES INSIDE OF DEPARTMENTS AND AGENCIES.

(a) RECIPROCALLY RECOGNIZED DEFINED.—In this section, the term "reciprocally recognized" means reciprocal recognition by Federal departments and agencies of eligibility for access to classified information.

(b) REPORTS TO SECURITY EXECUTIVE AGENT.—The head of each Federal department or agency shall submit an annual report to the Security Executive Agent that—

(1) identifies the number of individuals whose security clearances take more than 2 weeks to be reciprocally recognized after such individuals move to another part of such department or agency; and

(2) breaks out the information described in paragraph (1) by type of clearance and the reasons for any delays.

(c) ANNUAL REPORT.—Not less frequently than once each year, the Security Executive Agent shall submit to the appropriate congressional committees and make available to industry partners an annual report that summarizes the information received pursuant to subsection (b) during the period covered by such report.

SEC. 2609. INTELLIGENCE COMMUNITY REPORTS ON SECURITY CLEARANCES.

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

(1) despite sustained efforts by Congress and the executive branch, an unacceptable backlog in processing and adjudicating security clearances persists, both within elements of the intelligence community and in other departments of the Federal Government, with some processing times exceeding a year or even more;

(2) the protracted clearance timetable threatens the ability of elements of the intelligence community to hire and retain highly qualified individuals, and thus to fulfill the missions of such elements;

(3) the prospect of a lengthy clearance process deters some such individuals from seeking employment with the intelligence community in the first place, and, when faced with a long wait time, those with conditional offers of employment may opt to discontinue the security clearance process and pursue different opportunities;

(4) now more than ever, therefore, the broken security clearance process badly needs fundamental reform; and

(5) in the meantime, to ensure the ability of elements of the intelligence community to hire and retain highly qualified personnel, elements should consider, to the extent possible and consistent with national security, permitting new employees to enter on duty immediately or nearly so, and to perform, on a temporary basis pending final adjudication of their security clearances, work that either does not require a security clearance or requires only a low-level interim clearance.

(b) IN GENERAL.—Section 506H of the National Security Act of 1947 (50 U.S.C. 3104) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A)(ii), by inserting "and" after the semicolon;

(B) in subparagraph (B)(ii), by striking "; and" and inserting a period; and

(C) by striking subparagraph (C);

(2) by redesignating subsection (b) as subsection (c);

(3) by inserting after subsection (a) the following new subsection (b):

"(b) INTELLIGENCE COMMUNITY REPORTS.—(1) Not later than March 1 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on the security clearances processed by each element of the intelligence community during the preceding fiscal year. Each such report shall separately identify security clearances processed for Federal employees and contractor employees sponsored by each such element.

"(2) Each report submitted under paragraph (1) shall include each of the following for each element of the intelligence community for the fiscal year covered by the report:

"(A) The total number of initial security clearance background investigations sponsored for new applicants.

"(B) The total number of security clearance periodic reinvestigations sponsored for existing employees.

"(C) The total number of initial security clearance background investigations for new applicants that were adjudicated with notice of a determination provided to the prospective applicant, including—

"(i) the total number that were adjudicated favorably and granted access to classified information; and

"(ii) the total number that were adjudicated unfavorably and resulted in a denial or revocation of a security clearance.

"(D) The total number of security clearance periodic background investigations that were adjudicated with notice of a determination provided to the existing employee, including—

"(i) the total number that were adjudicated favorably; and

"(ii) the total number that were adjudicated unfavorably and resulted in a denial or revocation of a security clearance.

"(E) The total number of pending security clearance background investigations, including initial applicant investigations and periodic reinvestigations, that were not adjudicated as of the last day of such year and that remained pending as follows:

"(i) For 180 days or less.

"(ii) For 180 days or longer, but less than 12 months.

"(iii) For 12 months or longer, but less than 18 months.

"(iv) For 18 months or longer, but less than 24 months.

"(v) For 24 months or longer.

"(F) In the case of security clearance determinations completed or pending during the year preceding the year for which the report is submitted that have taken longer than 12 months to complete—

"(i) an explanation of the causes for the delays incurred during the period covered by the report; and

"(ii) the number of such delays involving a polygraph requirement.

"(G) The percentage of security clearance investigations, including initial and periodic reinvestigations, that resulted in a denial or revocation of a security clearance.

"(H) The percentage of security clearance investigations that resulted in incomplete information.

"(I) The percentage of security clearance investigations that did not result in enough information to make a decision on potentially adverse information.

"(3) The report required under this subsection shall be submitted in unclassified form, but may include a classified annex."; and

(4) in subsection (c), as redesignated by paragraph (2), by striking "subsection (a)(1)" and inserting "subsections (a)(1) and (b)".

SEC. 2610. PERIODIC REPORT ON POSITIONS IN THE INTELLIGENCE COMMUNITY THAT CAN BE CONDUCTED WITHOUT ACCESS TO CLASSIFIED INFORMATION, NETWORKS, OR FACILITIES.

Not later than 180 days after the date of the enactment of this Act and not less frequently than once every 5 years thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a report that reviews the intelligence community for which positions can be conducted without access to classified information, networks, or facilities, or may only require a security clearance at the secret level.

SEC. 2611. INFORMATION SHARING PROGRAM FOR POSITIONS OF TRUST AND SECURITY CLEARANCES.

(a) PROGRAM REQUIRED.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall establish and implement a program to share between and among agencies of the Federal Government and industry partners of the Federal Government relevant background information regarding individuals applying for and currently occupying national security positions and positions of trust, in order to ensure the Federal Government maintains a trusted workforce.

(2) DESIGNATION.—The program established under paragraph (1) shall be known as the "Trusted Information Provider Program" (in this section referred to as the "Program").

(b) PRIVACY SAFEGUARDS.—The Security Executive Agent and the Suitability and Credentialing Executive Agent shall ensure that the Program includes such safeguards for privacy as the Security Executive Agent and the Suitability and Credentialing Executive Agent consider appropriate.

(c) PROVISION OF INFORMATION TO THE FEDERAL GOVERNMENT.—The Program shall include requirements that enable investigative service providers and agencies of the Federal Government to leverage certain pre-employment information gathered during the employment or military recruiting process, and other relevant security or human resources information obtained during employment with or for the Federal Government, that satisfy Federal investigative standards, while safeguarding personnel privacy.

(d) INFORMATION AND RECORDS.—The information and records considered under the Program shall include the following:

(1) Date and place of birth.
(2) Citizenship or immigration and naturalization information.
(3) Education records.
(4) Employment records.
(5) Employment or social references.
(6) Military service records.
(7) State and local law enforcement checks.
(8) Criminal history checks.
(9) Financial records or information.
(10) Foreign travel, relatives, or associations.
(11) Social media checks.
(12) Such other information or records as may be relevant to obtaining or maintaining national security, suitability, fitness, or credentialing eligibility.

(e) IMPLEMENTATION PLAN.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a plan for the implementation of the Program.

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

(A) Mechanisms that address privacy, national security, suitability or fitness, credentialing, and human resources or military recruitment processes.

(B) Such recommendations for legislative or administrative action as the Security Executive Agent and the Suitability and Credentialing Executive Agent consider appropriate to carry out or improve the Program.

(f) PLAN FOR PILOT PROGRAM ON TWO-WAY INFORMATION SHARING.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a plan for the implementation of a pilot program to assess the feasibility and advisability of expanding the Program to include the sharing of information held by the Federal Government related to contract personnel with the security office of the employers of those contractor personnel.

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

(A) Mechanisms that address privacy, national security, suitability or fitness, credentialing, and human resources or military recruitment processes.

(B) Such recommendations for legislative or administrative action as the Security Executive Agent and the Suitability and Credentialing Executive Agent consider appropriate to carry out or improve the pilot program.

(g) REVIEW.—Not later than 1 year after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a review of the plans submitted under subsections (e)(1) and (f)(1) and utility and effectiveness of the programs described in such plans.

SEC. 2612. REPORT ON PROTECTIONS FOR CONFIDENTIALITY OF WHISTLEBLOWER-RELATED COMMUNICATIONS.

Not later than 180 days after the date of the enactment of this Act, the Security Executive Agent shall, in coordination with the Inspector General of the Intelligence Community, submit to the appropriate congressional committees a report detailing the controls employed by the intelligence community to ensure that continuous vetting programs, including those involving user activity monitoring, protect the confidentiality of whistleblower-related communications.

TITLE XXVII—REPORTS AND OTHER MATTERS

Subtitle A—Matters Relating to Russia and Other Foreign Powers

SEC. 2701. LIMITATION RELATING TO ESTABLISHMENT OR SUPPORT OF CYBERSECURITY UNIT WITH THE RUSSIAN FEDERATION.

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

(1) the congressional intelligence committees;

(2) the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and

(3) the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(b) LIMITATION.—

(1) IN GENERAL.—No amount may be expended by the Federal Government, other than the Department of Defense, to enter into or implement any bilateral agreement between the United States and the Russian Federation regarding cybersecurity, including the establishment or support of any cybersecurity unit, unless, at least 30 days prior to the conclusion of any such agreement, the Director of National Intelligence submits to the appropriate congressional committees a report on such agreement that includes the elements required by subsection (c).

(2) DEPARTMENT OF DEFENSE AGREEMENTS.—Any agreement between the Department of Defense and the Russian Federation regarding cybersecurity shall be conducted in accordance with section 1232 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328), as amended by section 1231 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91).

(c) ELEMENTS.—If the Director submits a report under subsection (b) with respect to an agreement, such report shall include a description of each of the following:

(1) The purpose of the agreement.

(2) The nature of any intelligence to be shared pursuant to the agreement.

(3) The expected value to national security resulting from the implementation of the agreement.

(4) Such counterintelligence concerns associated with the agreement as the Director may have and such measures as the Director expects to be taken to mitigate such concerns.

(d) RULE OF CONSTRUCTION.—This section shall not be construed to affect any existing authority of the Director of National Intelligence, the Director of the Central Intelligence Agency, or another head of an element of the intelligence community, to share or receive foreign intelligence on a case-by-case basis.

SEC. 2702. REPORT ON RETURNING RUSSIAN COMPOUNDS.

(a) COVERED COMPOUNDS DEFINED.—In this section, the term "covered compounds" means the real property in New York, the real property in Maryland, and the real property in San Francisco, California, that were under the control of the Government of Russia in 2016 and were removed from such control in response to various transgressions by the Government of Russia, including the interference by the Government of Russia in the 2016 election in the United States.

(b) REQUIREMENT FOR 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, and the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives (only with respect to the unclassified report), a report on the intelligence risks of returning the covered compounds to Russian control.

(c) FORM OF REPORT.—The report required by this section shall be submitted in classified and unclassified forms.

SEC. 2703. ASSESSMENT OF THREAT FINANCE RELATING TO RUSSIA.

(a) THREAT FINANCE DEFINED.—In this section, the term "threat finance" means—

(1) the financing of cyber operations, global influence campaigns, intelligence service activities, proliferation, terrorism, or transnational crime and drug organizations;

(2) the methods and entities used to spend, store, move, raise, conceal, or launder money or value, on behalf of threat actors;

(3) sanctions evasion; and

(4) other forms of threat finance activity domestically or internationally, as defined by the President.

(b) REPORT REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Assistant Secretary of the Treasury for Intelligence and Analysis, shall submit to the congressional intelligence committees a report containing an assessment of Russian threat finance. The assessment shall be based on intelligence from all sources, including from the Office of Terrorism and Financial Intelligence of the Department of the Treasury.

(c) ELEMENTS.—The report required by subsection (b) shall include each of the following:

(1) A summary of leading examples from the 3-year period preceding the date of the submittal of the report of threat finance activities conducted by, for the benefit of, or at the behest of—

(A) officials of the Government of Russia;

(B) persons subject to sanctions under any provision of law imposing sanctions with respect to Russia;

(C) Russian nationals subject to sanctions under any other provision of law; or

(D) Russian oligarchs or organized criminals.

(2) An assessment with respect to any trends or patterns in threat finance activities relating to Russia, including common methods of conducting such activities and global nodes of money laundering used by Russian threat actors described in paragraph (1) and associated entities.

(3) An assessment of any connections between Russian individuals involved in money laundering and the Government of Russia.

(4) A summary of engagement and coordination with international partners on threat finance relating to Russia, especially in Europe, including examples of such engagement and coordination.

(5) An identification of any resource and collection gaps.

(6) An identification of—

(A) entry points of money laundering by Russian and associated entities into the United States;

(B) any vulnerabilities within the United States legal and financial system, including specific sectors, which have been or could be exploited in connection with Russian threat finance activities; and

(C) the counterintelligence threat posed by Russian money laundering and other forms of threat finance, as well as the threat to the United States financial system and United States efforts to enforce sanctions and combat organized crime.

(7) Any other matters the Director determines appropriate.

(d) FORM OF REPORT.—The report required under subsection (b) may be submitted in classified form.

SEC. 2704. NOTIFICATION OF AN ACTIVE MEASURES CAMPAIGN.

(a) DEFINITIONS.—In this section:

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

(A) the congressional intelligence committees;

(B) the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and

(C) the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term "congressional leadership" includes the following:

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

(D) The minority leader of the House of Representatives.

(b) REQUIREMENT FOR NOTIFICATION.—The Director of National Intelligence, in cooperation with the Director of the Federal Bureau of Investigation and the head of any other relevant agency, shall notify the congressional leadership and the Chairman and Vice Chairman or Ranking Member of each of the appropriate congressional committees, and of other relevant committees of jurisdiction, each time the Director of National Intelligence determines there is credible information that a foreign power has, is, or will attempt to employ a covert influence or active measures campaign with regard to the modernization, employment, doctrine, or force posture of the nuclear deterrent or missile defense.

(c) CONTENT OF NOTIFICATION.—Each notification required by subsection (b) shall include information concerning actions taken by the United States to expose or halt an attempt referred to in subsection (b).

SEC. 2705. NOTIFICATION OF TRAVEL BY ACCREDITED DIPLOMATIC AND CONSULAR PERSONNEL OF THE RUSSIAN FEDERATION IN THE UNITED STATES.

In carrying out the advance notification requirements set out in section 502 of the Intelligence Authorization Act for Fiscal Year 2017 (division N of Public Law 115–31; 131 Stat. 825; 22 U.S.C. 254a note), the Secretary of State shall—

(1) ensure that the Russian Federation provides notification to the Secretary of State at least 2 business days in advance of all travel that is subject to such requirements by accredited diplomatic and consular personnel of the Russian Federation in the United States, and take necessary action to secure full compliance by Russian personnel and address any noncompliance; and

(2) provide notice of travel described in paragraph (1) to the Director of National Intelligence and the Director of the Federal Bureau of Investigation within 1 hour of receiving notice of such travel.

SEC. 2706. REPORT ON OUTREACH STRATEGY ADDRESSING THREATS FROM UNITED STATES ADVERSARIES TO THE UNITED STATES TECHNOLOGY SECTOR.

(a) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term "appropriate committees of Congress" means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(3) the Committee on Armed Services, Committee on Homeland Security, and the Committee on Oversight and Reform of the House of Representatives.

(b) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report detailing outreach by the intelligence community and the Defense Intelligence Enterprise to United States industrial, commercial, scientific, technical, and academic communities on matters relating to the efforts of adversaries of the United States to acquire critical United States technology, intellectual property, and research and development information.

(c) CONTENTS.—The report required by subsection (b) shall include the following:

(1) A review of the current outreach efforts of the intelligence community and the Defense Intelligence Enterprise described in subsection (b), including the type of information conveyed in the outreach.

(2) A determination of the appropriate element of the intelligence community to lead such outreach efforts.

(3) An assessment of potential methods for improving the effectiveness of such outreach, including an assessment of the following:

(A) Those critical technologies, infrastructure, or related supply chains that are at risk from the efforts of adversaries described in subsection (b).

(B) The necessity and advisability of granting security clearances to company or community leadership, when necessary and appropriate, to allow for tailored classified briefings on specific targeted threats.

(C) The advisability of partnering with entities of the Federal Government that are not elements of the intelligence community and relevant regulatory and industry groups described in subsection (b), to convey key messages across sectors targeted by United States adversaries.

(D) Strategies to assist affected elements of the communities described in subparagraph (C) in mitigating, deterring, and protecting against the broad range of threats from the efforts of adversaries described in subsection (b),

with focus on producing information that enables private entities to justify business decisions related to national security concerns.

(E) The advisability of the establishment of a United States Government-wide task force to coordinate outreach and activities to combat the threats from efforts of adversaries described in subsection (b).

(F) Such other matters as the Director of National Intelligence may consider necessary.

(d) CONSULTATION ENCOURAGED.—In preparing the report required by subsection (b), the Director is encouraged to consult with other government agencies, think tanks, academia, representatives of the financial industry, or such other entities as the Director considers appropriate.

(e) FORM.—The report required by subsection (b) shall be submitted in unclassified form, but may include a classified annex as necessary.

SEC. 2707. REPORT ON IRANIAN SUPPORT OF PROXY FORCES IN SYRIA AND LEBANON.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means—

(A) the Committee on Armed Services, the Committee on Foreign Relations, and the Select Committee on Intelligence of the Senate; and

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

(2) ARMS OR RELATED MATERIAL.—The term "arms or related material" means—

(A) nuclear, biological, chemical, or radiological weapons or materials or components of such weapons;

(B) ballistic or cruise missile weapons or materials or components of such weapons;

(C) destabilizing numbers and types of advanced conventional weapons;

(D) defense articles or defense services, as those terms are defined in paragraphs (3) and (4), respectively, of section 47 of the Arms Export Control Act (22 U.S.C. 2794);

(E) defense information, as that term is defined in section 644 of the Foreign Assistance Act of 1961 (22 U.S.C. 2403); or

(F) items designated by the President for purposes of the United States Munitions List under section 38(a)(1) of the Arms Export Control Act (22 U.S.C. 2778(a)(1)).

(b) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report on Iranian support of proxy forces in Syria and Lebanon and the threat posed to Israel, other United States regional allies, and other specified interests of the United States as a result of such support.

(c) MATTERS FOR INCLUSION.—The report required under subsection (b) shall include information relating to the following matters with respect to both the strategic and tactical implications for the United States and its allies:

(1) A description of arms or related materiel transferred by Iran to Hizballah since March 2011, including the number of such arms or related materiel and whether such transfer was by land, sea, or air, as well as financial and additional technological capabilities transferred by Iran to Hizballah.

(2) A description of Iranian and Iranian-controlled personnel, including Hizballah, Shiite militias, and Iran's Revolutionary Guard Corps forces, operating within Syria, including the number and geographic distribution of such personnel operating within 30 kilometers of the Israeli borders with Syria and Lebanon.

(3) An assessment of Hizballah's operational lessons learned based on its recent experiences in Syria.

(4) A description of any rocket-producing facilities in Lebanon for nonstate actors, including whether such facilities were assessed to be built at the direction of Hizballah leadership, Iranian leadership, or in consultation between Iranian leadership and Hizballah leadership.

(5) An analysis of the foreign and domestic supply chains that significantly facilitate, support, or otherwise aid Hizballah's acquisition or development of missile production facilities, including the geographic distribution of such foreign and domestic supply chains.

(6) An assessment of the provision of goods, services, or technology transferred by Iran or its affiliates to Hizballah to indigenously manufacture or otherwise produce missiles.

(7) An identification of foreign persons that are based on credible information, facilitating the transfer of significant financial support or arms or related materiel to Hizballah.

(8) A description of the threat posed to Israel and other United States allies in the Middle East by the transfer of arms or related material or other support offered to Hizballah and other proxies from Iran.

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

SEC. 2708. ANNUAL REPORT ON IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.

(a) ANNUAL REPORT REQUIRED.—Not later than 90 days after the date of the enactment of this Act and not less frequently than once each year thereafter, the Director of National Intelligence shall submit to Congress a report describing Iranian expenditures in the previous calendar year on military and terrorist activities outside the country, including each of the following:

(1) The amount spent in such calendar year on activities by the Islamic Revolutionary Guard Corps, including activities providing support for—

(A) Hizballah;

(B) Houthi rebels in Yemen;

(C) Hamas;

(D) proxy forces in Iraq and Syria; or

(E) any other entity or country the Director determines to be relevant.

(2) The amount spent in such calendar year for ballistic missile research and testing or other activities that the Director determines are destabilizing to the Middle East region.

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

SEC. 2709. EXPANSION OF SCOPE OF COMMITTEE TO COUNTER ACTIVE MEASURES AND REPORT ON ESTABLISHMENT OF FOREIGN MALIGN INFLUENCE CENTER.

(a) SCOPE OF COMMITTEE TO COUNTER ACTIVE MEASURES.—

(1) IN GENERAL.—Section 501 of the Intelligence Authorization Act for Fiscal Year 2017 (Public Law 115–31; 50 U.S.C. 3001 note) is amended—

(A) in subsections (a) through (h)—

(i) by inserting ", the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state" after "Russian Federation" each place it appears; and

(ii) by inserting ", China, Iran, North Korea, or other nation state" after "Russia" each place it appears; and

(B) in the section heading, by inserting "**, THE PEOPLE'S REPUBLIC OF CHINA, THE ISLAMIC REPUBLIC OF IRAN, THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA, OR OTHER NATION STATE**" after "**RUSSIAN FEDERATION**".

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 501 and inserting the following new item:

"Sec. 501. Committee to counter active measures by the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation states to exert covert influence over peoples and governments.".

(b) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with such elements of the intelligence community as the Director considers relevant, shall submit to the congressional intelligence committees a report on the feasibility and advisability of establishing a center, to be known as the "Foreign Malign Influence Response Center", that—

(A) is comprised of analysts from all appropriate elements of the intelligence community, including elements with related diplomatic and law enforcement functions;

(B) has access to all intelligence and other reporting acquired by the United States Government on foreign efforts to influence, through overt and covert malign activities, United States political processes and elections;

(C) provides comprehensive assessment, and indications and warning, of such activities; and

(D) provides for enhanced dissemination of such assessment to United States policy makers.

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

(A) A discussion of the desirability of the establishment of such center and any barriers to such establishment.

(B) Such recommendations and other matters as the Director considers appropriate.

Subtitle B—Reports

SEC. 2711. TECHNICAL CORRECTION TO INSPECTOR GENERAL STUDY.

Section 11001(d) of title 5, United States Code, is amended—

(1) in the subsection heading, by striking "AUDIT" and inserting "REVIEW";

(2) in paragraph (1), by striking "audit" and inserting "review"; and

(3) in paragraph (2), by striking "audit" and inserting "review".

SEC. 2712. REPORTS ON AUTHORITIES OF THE CHIEF INTELLIGENCE OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means—

(A) the congressional intelligence committees;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Homeland Security of the House of Representatives.

(2) HOMELAND SECURITY INTELLIGENCE ENTERPRISE.—The term "Homeland Security Intelligence Enterprise" has the meaning given such term in Department of Homeland Security Instruction Number 264–01–001, or successor authority.

(b) REPORT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security, in consultation with the Under Secretary of Homeland Security for Intelligence and Analysis, shall submit to the appropriate committees of Congress a report on the authorities of the Under Secretary.

(c) ELEMENTS.—The report required by subsection (b) shall include each of the following:

(1) An analysis of whether the Under Secretary has the legal and policy authority necessary to organize and lead the Homeland Security Intelligence Enterprise, with respect to intelligence, and, if not, a description of—

(A) the obstacles to exercising the authorities of the Chief Intelligence Officer of the Department and the Homeland Security Intelligence Council, of which the Chief Intelligence Officer is the chair; and

(B) the legal and policy changes necessary to effectively coordinate, organize, and lead intelligence activities of the Department of Homeland Security.

(2) A description of the actions that the Secretary has taken to address the inability of the Under Secretary to require components of the Department, other than the Office of Intelligence and Analysis of the Department to—

(A) coordinate intelligence programs; and

(B) integrate and standardize intelligence products produced by such other components.

SEC. 2713. REVIEW OF INTELLIGENCE COMMUNITY WHISTLEBLOWER MATTERS.

(a) REVIEW OF WHISTLEBLOWER MATTERS.—The Inspector General of the Intelligence Community, in consultation with the inspectors general for the Central Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the Defense Intelligence Agency, and the National Reconnaissance Office, shall conduct a review of the authorities, policies, investigatory standards, and other practices and procedures relating to intelligence community whistleblower matters, with respect to such inspectors general.

(b) OBJECTIVE OF REVIEW.—The objective of the review required under subsection (a) is to identify any discrepancies, inconsistencies, or other issues, which frustrate the timely and effective reporting of intelligence community whistleblower matters to appropriate inspectors general and to the congressional intelligence committees, and the fair and expeditious investigation and resolution of such matters.

(c) CONDUCT OF REVIEW.—The Inspector General of the Intelligence Community shall take such measures as the Inspector General determines necessary in order to ensure that the review required by subsection (a) is conducted in an independent and objective fashion.

(d) REPORT.—Not later than 270 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community shall submit to the congres-

sional intelligence committees a written report containing the results of the review required under subsection (a), along with recommendations to improve the timely and effective reporting of intelligence community whistleblower matters to inspectors general and to the congressional intelligence committees and the fair and expeditious investigation and resolution of such matters.

SEC. 2714. REPORT ON ROLE OF DIRECTOR OF NATIONAL INTELLIGENCE WITH RESPECT TO CERTAIN FOREIGN INVESTMENTS.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community determined appropriate by the Director, shall submit to the congressional intelligence committees a report on the role of the Director in preparing analytic materials in connection with the evaluation by the Federal Government of national security risks associated with potential foreign investments into the United States.

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

(1) a description of the current process for the provision of the analytic materials described in subsection (a);

(2) an identification of the most significant benefits and drawbacks of such process with respect to the role of the Director, including the sufficiency of resources and personnel to prepare such materials; and

(3) recommendations to improve such process.

SEC. 2715. REPORT ON SURVEILLANCE BY FOREIGN GOVERNMENTS AGAINST UNITED STATES TELECOMMUNICATIONS NETWORKS.

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

(1) The congressional intelligence committees.

(2) The Committee on the Judiciary and the Committee on Homeland Security and Governmental Affairs of the Senate.

(3) The Committee on the Judiciary and the Committee on Homeland Security of the House of Representatives.

(b) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in coordination with the Director of the Central Intelligence Agency, the Director of the National Security Agency, the Director of the Federal Bureau of Investigation, and the Secretary of Homeland Security, submit to the appropriate congressional committees a report describing—

(1) any attempts known to the intelligence community by foreign governments to exploit cybersecurity vulnerabilities in United States telecommunications networks (including Signaling System No. 7) to target for surveillance United States persons, including employees of the Federal Government; and

(2) any actions, as of the date of the enactment of this Act, taken by the intelligence community to protect agencies and personnel of the United States Government from surveillance conducted by foreign governments.

SEC. 2716. BIENNIAL REPORT ON FOREIGN INVESTMENT RISKS.

(a) INTELLIGENCE COMMUNITY INTERAGENCY WORKING GROUP.—

(1) REQUIREMENT TO ESTABLISH.—The Director of National Intelligence shall establish an intelligence community interagency working group to prepare the biennial reports required by subsection (b).

(2) CHAIRPERSON.—The Director of National Intelligence shall serve as the chairperson of such interagency working group.

(3) MEMBERSHIP.—Such interagency working group shall be composed of representatives of each element of the intelligence community that the Director of National Intelligence determines appropriate.

(b) BIENNIAL REPORT ON FOREIGN INVESTMENT RISKS.—

(1) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on foreign investment risks prepared by the interagency working group established under subsection (a).

(2) ELEMENTS.—Each report required by paragraph (1) shall include identification, analysis, and explanation of the following:

(A) Any current or projected major threats to the national security of the United States with respect to foreign investment.

(B) Any strategy used by a foreign country that such interagency working group has identified to be a country of special concern to use foreign invest-

ment to target the acquisition of critical technologies, critical materials, or critical infrastructure.

(C) Any economic espionage efforts directed at the United States by a foreign country, particularly such a country of special concern.

SEC. 2717. MODIFICATION OF CERTAIN REPORTING REQUIREMENT ON TRAVEL OF FOREIGN DIPLOMATS.

Section 502(d)(2) of the Intelligence Authorization Act for Fiscal Year 2017 (Public Law 115–31) is amended by striking "the number" and inserting "a best estimate".

SEC. 2718. SEMIANNUAL REPORTS ON INVESTIGATIONS OF UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION.

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

"SEC. 1105. SEMIANNUAL REPORTS ON INVESTIGATIONS OF UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION.

"(a) DEFINITIONS.—In this section:

"(1) COVERED OFFICIAL.—The term 'covered official' means—

"(A) the heads of each element of the intelligence community; and

"(B) the inspectors general with oversight responsibility for an element of the intelligence community.

"(2) INVESTIGATION.—The term 'investigation' means any inquiry, whether formal or informal, into the existence of an unauthorized public disclosure of classified information.

"(3) UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION.—The term 'unauthorized disclosure of classified information' means any unauthorized disclosure of classified information to any recipient.

"(4) UNAUTHORIZED PUBLIC DISCLOSURE OF CLASSIFIED INFORMATION.—The term 'unauthorized public disclosure of classified information' means the unauthorized disclosure of classified information to a journalist or media organization.

"(b) INTELLIGENCE COMMUNITY REPORTING.—

"(1) IN GENERAL.—Not less frequently than once every 6 months, each covered official shall submit to the congressional intelligence committees a report on investigations of unauthorized public disclosures of classified information.

"(2) ELEMENTS.—Each report submitted under paragraph (1) shall include, with respect to the preceding 6-month period, the following:

"(A) The number of investigations opened by the covered official regarding an unauthorized public disclosure of classified information.

"(B) The number of investigations completed by the covered official regarding an unauthorized public disclosure of classified information.

"(C) Of the number of such completed investigations identified under subparagraph (B), the number referred to the Attorney General for criminal investigation.

"(c) DEPARTMENT OF JUSTICE REPORTING.—

"(1) IN GENERAL.—Not less frequently than once every 6 months, the Assistant Attorney General for National Security of the Department of Justice, in consultation with the Director of the Federal Bureau of Investigation, shall submit to the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives a report on the status of each referral made to the Department of Justice from any element of the intelligence community regarding an unauthorized disclosure of classified information made during the most recent 365-day period or any referral that has not yet been closed, regardless of the date the referral was made.

"(2) CONTENTS.—Each report submitted under paragraph (1) shall include, for each referral covered by the report, at a minimum, the following:

"(A) The date the referral was received.

"(B) A statement indicating whether the alleged unauthorized disclosure described in the referral was substantiated by the Department of Justice.

"(C) A statement indicating the highest level of classification of the information that was revealed in the unauthorized disclosure.

"(D) A statement indicating whether an open criminal investigation related to the referral is active.

"(E) A statement indicating whether any criminal charges have been filed related to the referral.

"(F) A statement indicating whether the Department of Justice has been able to attribute the unauthorized disclosure to a particular entity or individual.

"(d) FORM OF REPORTS.—Each report submitted under this section shall be submitted in unclassified form, but may have a classified annex.".

(b) CLERICAL AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by inserting after the item relating to section 1104 the following new item:

"Sec. 1105. Semiannual reports on investigations of unauthorized disclosures of classified information.".

SEC. 2719. CONGRESSIONAL NOTIFICATION OF DESIGNATION OF COVERED INTELLIGENCE OFFICER AS PERSONA NON GRATA.

(a) COVERED INTELLIGENCE OFFICER DEFINED.—In this section, the term "covered intelligence officer" means—

(1) a United States intelligence officer serving in a post in a foreign country; or

(2) a known or suspected foreign intelligence officer serving in a United States post.

(b) REQUIREMENT FOR REPORTS.—Not later than 72 hours after a covered intelligence officer is designated as a persona non grata, the Director of National Intelligence, in consultation with the Secretary of State, shall submit to the congressional intelligence committees, the Committee on Foreign Relations of the Senate, and the Committee on Foreign Affairs of the House of Representatives a notification of that designation. Each such notification shall include—

(1) the date of the designation;

(2) the basis for the designation; and

(3) a justification for the expulsion.

SEC. 2720. REPORTS ON INTELLIGENCE COMMUNITY PARTICIPATION IN VULNERABILITIES EQUITIES PROCESS OF FEDERAL GOVERNMENT.

(a) DEFINITIONS.—In this section:

(1) VULNERABILITIES EQUITIES POLICY AND PROCESS DOCUMENT.—The term "Vulnerabilities Equities Policy and Process document" means the executive branch document entitled "Vulnerabilities Equities Policy and Process" dated November 15, 2017.

(2) VULNERABILITIES EQUITIES PROCESS.—The term "Vulnerabilities Equities Process" means the interagency review of vulnerabilities, pursuant to the Vulnerabilities Equities Policy and Process document or any successor document.

(3) VULNERABILITY.—The term "vulnerability" means a weakness in an information system or its components (for example, system security procedures, hardware design, and internal controls) that could be exploited or could affect confidentiality, integrity, or availability of information.

(b) REPORTS ON PROCESS AND CRITERIA UNDER VULNERABILITIES EQUITIES POLICY AND PROCESS.—

(1) IN GENERAL.—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 written report describing—

(A) with respect to each element of the intelligence community—

(i) the title of the official or officials responsible for determining whether, pursuant to criteria contained in the Vulnerabilities Equities Policy and Process document or any successor document, a vulnerability must be submitted for review under the Vulnerabilities Equities Process; and

(ii) the process used by such element to make such determination; and

(B) the roles or responsibilities of that element during a review of a vulnerability submitted to the Vulnerabilities Equities Process.

(2) CHANGES TO PROCESS OR CRITERIA.—Not later than 30 days after any significant change is made to the process and criteria used by any element of the intelligence community for determining whether to submit a vulnerability for review under the Vulnerabilities Equities Process, such element shall submit to the congressional intelligence committees a report describing such change.

(3) FORM OF REPORTS.—Each report submitted under this subsection shall be submitted in unclassified form, but may include a classified annex.

(c) ANNUAL REPORTS.—

(1) IN GENERAL.—Not less frequently than once each calendar year, the Director of National Intelligence shall submit to the congressional intelligence committees a classified report containing, with respect to the previous year—

(A) the number of vulnerabilities submitted for review under the Vulnerabilities Equities Process;

(B) the number of vulnerabilities described in subparagraph (A) disclosed to each vendor responsible for correcting the vulnerability, or to the public, pursuant to the Vulnerabilities Equities Process; and

(C) the aggregate number, by category, of the vulnerabilities excluded from review under the Vulnerabilities Equities Process, as described in paragraph 5.4 of the Vulnerabilities Equities Policy and Process document.

(2) UNCLASSIFIED INFORMATION.—Each report submitted under paragraph (1) shall include an unclassified appendix that contains—

(A) the aggregate number of vulnerabilities disclosed to vendors or the public pursuant to the Vulnerabilities Equities Process; and

(B) the aggregate number of vulnerabilities disclosed to vendors or the public pursuant to the Vulnerabilities Equities Process known to have been patched.

(3) NON-DUPLICATION.—The Director of National Intelligence may forgo submission of an annual report required under this subsection for a calendar year, if the Director notifies the intelligence committees in writing that, with respect to the same calendar year, an annual report required by paragraph 4.3 of the Vulnerabilities Equities Policy and Process document already has been submitted to Congress, and such annual report contains the information that would otherwise be required to be included in an annual report under this subsection.

SEC. 2721. INSPECTORS GENERAL REPORTS ON CLASSIFICATION.

(a) REPORTS REQUIRED.—Not later than October 1, 2019, each Inspector General listed in subsection (b) shall submit to the congressional intelligence committees a report that includes, with respect to the department or agency of the Inspector General, analyses of the following:

(1) The accuracy of the application of classification and handling markers on a representative sample of finished reports, including such reports that are compartmented.

(2) Compliance with declassification procedures.

(3) The effectiveness of processes for identifying topics of public or historical importance that merit prioritization for a declassification review.

(b) INSPECTORS GENERAL LISTED.—The Inspectors General listed in this subsection are as follows:

(1) The Inspector General of the Intelligence Community.

(2) The Inspector General of the Central Intelligence Agency.

(3) The Inspector General of the National Security Agency.

(4) The Inspector General of the Defense Intelligence Agency.

(5) The Inspector General of the National Reconnaissance Office.

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

SEC. 2722. REPORTS ON GLOBAL WATER INSECURITY AND NATIONAL SECURITY IMPLICATIONS AND BRIEFING ON EMERGING INFECTIOUS DISEASE AND PANDEMICS.

(a) REPORTS ON GLOBAL WATER INSECURITY AND NATIONAL SECURITY IMPLICATIONS.—

(1) REPORTS REQUIRED.—Not later than 180 days after the date of the enactment of this Act and not less frequently than once every 5 years thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the implications of water insecurity on the national security interest of the United States, including consideration of social, economic, agricultural, and environmental factors.

(2) ASSESSMENT SCOPE AND FOCUS.—Each report submitted under paragraph (1) shall include an assessment of water insecurity described in such subsection with a global scope, but focus on areas of the world—

(A) of strategic, economic, or humanitarian interest to the United States—

(i) that are, as of the date of the report, at the greatest risk of instability, conflict, human insecurity, or mass displacement; or

(ii) where challenges relating to water insecurity are likely to emerge and become significant during the 5-year or the 20-year period beginning on the date of the report; and

(B) where challenges relating to water insecurity are likely to imperil the national security interests of the United States or allies of the United States.

(3) CONSULTATION.—In researching a report required by paragraph (1), the Director shall consult with—

(A) such stakeholders within the intelligence community, the Department of Defense, and the Department of State as the Director considers appropriate; and

(B) such additional Federal agencies and persons in the private sector as the Director considers appropriate.

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

(b) BRIEFING ON EMERGING INFECTIOUS DISEASE AND PANDEMICS.—

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

(A) the congressional intelligence committees;

(B) the Committee on Foreign Affairs, the Committee on Armed Services, and the Committee on Appropriations of the House of Representatives; and

(C) the Committee on Foreign Relations, the Committee on Armed Services, and the Committee on Appropriations of the Senate.

(2) BRIEFING.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall provide to the appropriate congressional committees a briefing on the anticipated geopolitical effects of emerging infectious disease (including deliberate, accidental, and naturally occurring infectious disease threats) and pandemics, and their implications on the national security of the United States.

(3) CONTENT.—The briefing under paragraph (2) shall include an assessment of—

(A) the economic, social, political, and security risks, costs, and impacts of emerging infectious diseases on the United States and the international political and economic system;

(B) the economic, social, political, and security risks, costs, and impacts of a major transnational pandemic on the United States and the international political and economic system; and

(C) contributing trends and factors to the matters assessed under subparagraphs (A) and (B).

(4) EXAMINATION OF RESPONSE CAPACITY.—In examining the risks, costs, and impacts of emerging infectious disease and a possible transnational pandemic under paragraph (3), the Director of National Intelligence shall also examine in the briefing under paragraph (2) the response capacity within affected countries and the international system. In considering response capacity, the Director shall include—

(A) the ability of affected nations to effectively detect and manage emerging infectious diseases and a possible transnational pandemic;

(B) the role and capacity of international organizations and nongovernmental organizations to respond to emerging infectious disease and a possible pandemic, and their ability to coordinate with affected and donor nations; and

(C) the effectiveness of current international frameworks, agreements, and health systems to respond to emerging infectious diseases and a possible transnational pandemic.

(5) FORM.—The briefing under paragraph (2) may be classified.

SEC. 2723. ANNUAL REPORT ON MEMORANDA OF UNDERSTANDING BETWEEN ELEMENTS OF INTELLIGENCE COMMUNITY AND OTHER ENTITIES OF THE UNITED STATES GOVERNMENT REGARDING SIGNIFICANT OPERATIONAL ACTIVITIES OR POLICY.

Section 311 of the Intelligence Authorization Act for Fiscal Year 2017 (50 U.S.C. 3313) is amended—

(1) by redesignating subsection (b) as subsection (c); and

(2) by striking subsection (a) and inserting the following:

"(a) IN GENERAL.—Each year, concurrent with the annual budget request submitted by the President to Congress under section 1105 of title 31, United States Code, each head of an element of the intelligence community shall submit to the congressional intelligence committees a report that lists each memorandum of understanding or other agreement regarding significant operational activities or policy entered into during the most recently completed fiscal year between or among such element and any other entity of the United States Government.

"(b) PROVISION OF DOCUMENTS.—Each head of an element of an intelligence community who receives a request from the Select Committee on Intelligence of the Senate or the Permanent Select Committee on Intelligence of the House of Representatives for a copy of a memorandum of understanding or other document listed in a report submitted by the head under subsection (a) shall submit to such committee the requested copy as soon as practicable after receiving such request.".

SEC. 2724. STUDY ON THE FEASIBILITY OF ENCRYPTING UNCLASSIFIED WIRELINE AND WIRELESS TELEPHONE CALLS.

(a) STUDY REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall complete a study on the feasi-

bility of encrypting unclassified wireline and wireless telephone calls between personnel in the intelligence community.

(b) REPORT.—Not later than 90 days after the date on which the Director completes the study required by subsection (a), the Director shall submit to the congressional intelligence committees a report on the Director's findings with respect to such study.

SEC. 2725. MODIFICATION OF REQUIREMENT FOR ANNUAL REPORT ON HIRING AND RETENTION OF MINORITY EMPLOYEES.

(a) EXPANSION OF PERIOD OF REPORT.—Subsection (a) of section 114 of the National Security Act of 1947 (50 U.S.C. 3050) is amended by inserting "and the preceding 5 fiscal years" after "fiscal year".

(b) CLARIFICATION ON DISAGGREGATION OF DATA.—Subsection (b) of such section is amended, in the matter before paragraph (1), by striking "disaggregated data by category of covered person from each element of the intelligence community" and inserting "data, disaggregated by category of covered person and by element of the intelligence community,".

SEC. 2726. REPORTS ON INTELLIGENCE COMMUNITY LOAN REPAYMENT AND RELATED PROGRAMS.

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

(1) there should be established, through the issuing of an Intelligence Community Directive or otherwise, an intelligence community-wide program for student loan repayment, student loan forgiveness, financial counseling, and related matters, for employees of the intelligence community;

(2) creating such a program would enhance the ability of the elements of the intelligence community to recruit, hire, and retain highly qualified personnel, including with respect to mission-critical and hard-to-fill positions;

(3) such a program, including with respect to eligibility requirements, should be designed so as to maximize the ability of the elements of the intelligence community to recruit, hire, and retain highly qualified personnel, including with respect to mission-critical and hard-to-fill positions; and

(4) to the extent possible, such a program should be uniform throughout the intelligence community and publicly promoted by each element of the intelligence community to both current employees of the element as well as to prospective employees of the element.

(b) REPORT ON POTENTIAL INTELLIGENCE COMMUNITY-WIDE PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in cooperation with the heads of the elements of the intelligence community and the heads of any other appropriate department or agency of the Federal Government, shall submit to the congressional intelligence committees a report on potentially establishing and carrying out an intelligence community-wide program for student loan repayment, student loan forgiveness, financial counseling, and related matters, as described in subsection (a).

(2) MATTERS INCLUDED.—The report under paragraph (1) shall include, at a minimum, the following:

(A) A description of the financial resources that the elements of the intelligence community would require to establish and initially carry out the program specified in paragraph (1).

(B) A description of the practical steps to establish and carry out such a program.

(C) The identification of any legislative action the Director determines necessary to establish and carry out such a program.

(c) ANNUAL REPORTS ON ESTABLISHED PROGRAMS.—

(1) COVERED PROGRAMS DEFINED.—In this subsection, the term "covered programs" means any loan repayment program, loan forgiveness program, financial counseling program, or similar program, established pursuant to title X of the National Security Act of 1947 (50 U.S.C. 3191 et seq.) or any other provision of law that may be administered or used by an element of the intelligence community.

(2) ANNUAL REPORTS REQUIRED.—Not less frequently than once each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the covered programs. Each such report shall include, with respect to the period covered by the report, the following:

(A) The number of personnel from each element of the intelligence community who used each covered program.

(B) The total amount of funds each element expended for each such program.

(C) A description of the efforts made by each element to promote each covered program pursuant to both the personnel of the element of the intelligence community and to prospective personnel.

SEC. 2727. REPEAL OF CERTAIN REPORTING REQUIREMENTS.

(a) CORRECTING LONG-STANDING MATERIAL WEAKNESSES.—Section 368 of the Intelligence Authorization Act for Fiscal Year 2010 (Public Law 110–259; 50 U.S.C. 3051 note) is hereby repealed.

(b) INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP.—Section 210D of the Homeland Security Act of 2002 (6 U.S.C. 124k) is amended—

(1) by striking subsection (c); and

(2) by redesignating subsections (d) through (i) as subsections (c) through (h), respectively; and

(3) in subsection (c), as so redesignated—

(A) in paragraph (8), by striking "; and" and inserting a period; and

(B) by striking paragraph (9).

(c) INSPECTOR GENERAL REPORT.—Section 8H of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

(1) by striking subsection (g); and

(2) by redesignating subsections (h) and (i) as subsections (g) and (h), respectively.

SEC. 2728. INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY REPORT ON SENIOR EXECUTIVES OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.

(a) SENIOR EXECUTIVE SERVICE POSITION DEFINED.—In this section, the term "Senior Executive Service position" has the meaning given that term in section 3132(a)(2) of title 5, United States Code, and includes any position above the GS–15, step 10, level of the General Schedule under section 5332 of such title.

(b) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community shall submit to the congressional intelligence committees a report on the number of Senior Executive Service positions in the Office of the Director of National Intelligence.

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

(1) The number of required Senior Executive Service positions for the Office of the Director of National Intelligence.

(2) Whether such requirements are reasonably based on the mission of the Office.

(3) A discussion of how the number of the Senior Executive Service positions in the Office compare to the number of senior positions at comparable organizations.

(d) COOPERATION.—The Director of National Intelligence shall provide to the Inspector General of the Intelligence Community any information requested by the Inspector General of the Intelligence Community that is necessary to carry out this section by not later than 14 calendar days after the date on which the Inspector General of the Intelligence Community makes such request.

SEC. 2729. BRIEFING ON FEDERAL BUREAU OF INVESTIGATION OFFERING PERMANENT RESIDENCE TO SOURCES AND COOPERATORS.

Not later than 30 days after the date of the enactment of this Act, the Director of the Federal Bureau of Investigation shall provide to the congressional intelligence committees a briefing on the ability of the Federal Bureau of Investigation to offer, as an inducement to assisting the Bureau, permanent residence within the United States to foreign individuals who are sources or cooperators in counterintelligence or other national security-related investigations. The briefing shall address the following:

(1) The extent to which the Bureau may make such offers, whether independently or in conjunction with other agencies and departments of the United States Government, including a discussion of the authorities provided by section 101(a)(15)(S) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(S)), section 7 of the Central Intelligence Agency Act (50 U.S.C. 3508), and any other provision of law under which the Bureau may make such offers.

(2) An overview of the policies and operational practices of the Bureau with respect to making such offers.

(3) The sufficiency of such policies and practices with respect to inducing individuals to cooperate with, serve as sources for such investigations, or both.

(4) Whether the Director recommends any legislative actions to improve such policies and practices, particularly with respect to the counterintelligence efforts of the Bureau.

SEC. 2730. INTELLIGENCE ASSESSMENT OF NORTH KOREA REVENUE SOURCES.

(a) ASSESSMENT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Assistant Secretary of State for Intelligence and Research and the Assistant Secretary of the Treasury for Intelligence and Analysis, shall produce an intelligence assessment of the revenue sources of the North Korean regime. Such assessment shall include revenue from the following sources:

(1) Trade in coal, iron, and iron ore.

(2) The provision of fishing rights to North Korean territorial waters.

(3) Trade in gold, titanium ore, vanadium ore, copper, silver, nickel, zinc, or rare earth minerals, and other stores of value.

(4) Trade in textiles.

(5) Sales of conventional defense articles and services.

(6) Sales of controlled goods, ballistic missiles, and other associated items.

(7) Other types of manufacturing for export, as the Director of National Intelligence considers appropriate.

(8) The exportation of workers from North Korea in a manner intended to generate significant revenue, directly or indirectly, for use by the government of North Korea.

(9) The provision of nonhumanitarian goods (such as food, medicine, and medical devices) and services by other countries.

(10) The provision of services, including banking and other support, including by entities located in the Russian Federation, China, and Iran.

(11) Online commercial activities of the Government of North Korea, including online gambling.

(12) Criminal activities, including cyber-enabled crime and counterfeit goods.

(b) ELEMENTS.—The assessment required under subsection (a) shall include an identification of each of the following:

(1) The sources of North Korea's funding.

(2) Financial and non-financial networks, including supply chain management, transportation, and facilitation, through which North Korea accesses the United States and international financial systems and repatriates and exports capital, goods, and services; and

(3) the global financial institutions, money services business, and payment systems that assist North Korea with financial transactions.

(c) SUBMITTAL TO CONGRESS.—Upon completion of the assessment required under subsection (a), the Director of National Intelligence shall submit to the congressional intelligence committees a copy of such assessment.

SEC. 2731. REPORT ON POSSIBLE EXPLOITATION OF VIRTUAL CURRENCIES BY TERRORIST ACTORS.

(a) SHORT TITLE.—This section may be cited as the "Stop Terrorist Use of Virtual Currencies Act".

(b) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Secretary of the Treasury, shall submit to Congress a report on the possible exploitation of virtual currencies by terrorist actors. Such report shall include the following elements:

(1) An assessment of the means and methods by which international terrorist organizations and State sponsors of terrorism use virtual currencies.

(2) An assessment of the use by terrorist organizations and State sponsors of terrorism of virtual currencies compared to the use by such organizations and States of other forms of financing to support operations, including an assessment of the collection posture of the intelligence community on the use of virtual currencies by such organizations and States.

(3) A description of any existing legal impediments that inhibit or prevent the intelligence community from collecting information on or helping prevent the use of virtual currencies by international terrorist organizations and State sponsors of terrorism and an identification of any gaps in existing law that could be exploited for illicit funding by such organizations and States.

(c) FORM OF REPORT.—The report required by subsection (b) shall be submitted in unclassified form, but may include a classified annex.

Subtitle C—Other Matters

SEC. 2741. PUBLIC INTEREST DECLASSIFICATION BOARD.

Section 710(b) of the Public Interest Declassification Act of 2000 (Public Law 106–567; 50 U.S.C. 3161 note) is amended by striking "December 31, 2018" and inserting "December 31, 2028".

SEC. 2742. TECHNICAL AND CLERICAL AMENDMENTS TO THE NATIONAL SECURITY ACT OF 1947.

(a) TABLE OF CONTENTS.—The table of contents at the beginning of the National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended—

(1) by inserting after the item relating to section 2 the following new item:

"Sec. 3. Definitions.";

(2) by striking the item relating to section 107;

(3) by striking the item relating to section 113B and inserting the following new item:

"Sec. 113B. Special pay authority for science, technology, engineering, or mathematics positions.";

(4) by striking the items relating to sections 202, 203, 204, 208, 209, 210, 211, 212, 213, and 214; and

(5) by inserting after the item relating to section 311 the following new item:

"Sec. 312. Repealing and saving provisions.".

(b) OTHER TECHNICAL CORRECTIONS.—Such Act is further amended—

(1) in section 102A—

(A) in subparagraph (G) of paragraph (1) of subsection (g), by moving the margins of such subparagraph 2 ems to the left; and

(B) in paragraph (3) of subsection (v), by moving the margins of such paragraph 2 ems to the left;

(2) in section 106—

(A) by inserting "SEC. 106." before "(a)"; and

(B) in subparagraph (I) of paragraph (2) of subsection (b), by moving the margins of such subparagraph 2 ems to the left;

(3) by striking section 107;

(4) in section 108(c), by striking "in both a classified and an unclassified form" and inserting "to Congress in classified form, but may include an unclassified summary";

(5) in section 112(c)(1), by striking "section 103(c)(7)" and inserting "section 102A(i)";

(6) by amending section 201 to read as follows:

"SEC. 201. DEPARTMENT OF DEFENSE.

"Except to the extent inconsistent with the provisions of this Act or other provisions of law, the provisions of title 5, United States Code, shall be applicable to the Department of Defense.";

(7) in section 205, by redesignating subsections (b) and (c) as subsections (a) and (b), respectively;

(8) in section 206, by striking "(a)";

(9) in section 207, by striking "(c)";

(10) in section 308(a), by striking "this Act" and inserting "sections 2, 101, 102, 103, and 303 of this Act";

(11) by redesignating section 411 as section 312;

(12) in section 503—

(A) in paragraph (5) of subsection (c)—

(i) by moving the margins of such paragraph 2 ems to the left; and

(ii) by moving the margins of subparagraph (B) of such paragraph 2 ems to the left; and

(B) in paragraph (2) of subsection (d), by moving the margins of such paragraph 2 ems to the left; and

(13) in subparagraph (B) of paragraph (3) of subsection (a) of section 504, by moving the margins of such subparagraph 2 ems to the right.

SEC. 2743. TECHNICAL AMENDMENTS RELATED TO THE DEPARTMENT OF ENERGY.

(a) NATIONAL NUCLEAR SECURITY ADMINISTRATION ACT.—

(1) CLARIFICATION OF FUNCTIONS OF THE ADMINISTRATOR FOR NUCLEAR SECURITY.—Subsection (b) of section 3212 of the National Nuclear Security Administration Act (50 U.S.C. 2402(b)) is amended—

(A) by striking paragraphs (11) and (12); and

(B) by redesignating paragraphs (13) through (19) as paragraphs (11) through (17), respectively.

(2) COUNTERINTELLIGENCE PROGRAMS.—Section 3233(b) of the National Nuclear Security Administration Act (50 U.S.C. 2423(b)) is amended—

(A) by striking "Administration" and inserting "Department"; and

(B) by inserting "Intelligence and" after "the Office of".

(b) ATOMIC ENERGY DEFENSE ACT.—Section 4524(b)(2) of the Atomic Energy Defense Act (50 U.S.C. 2674(b)(2)) is amended by inserting "Intelligence and" after "The Director of".

(c) NATIONAL SECURITY ACT OF 1947.—Paragraph (2) of section 106(b) of the National Security Act of 1947 (50 U.S.C. 3041(b)(2)) is amended—

(1) in subparagraph (E), by inserting "and Counterintelligence" after "Office of Intelligence";

(2) by striking subparagraph (F); and

(3) by redesignating subparagraphs (G), (H), and (I) as subparagraphs (F), (G), and (H), respectively.

SEC. 2744. SENSE OF CONGRESS ON NOTIFICATION OF CERTAIN DISCLOSURES OF CLASSIFIED INFORMATION.

(a) DEFINITIONS.—In this section:

(1) ADVERSARY FOREIGN GOVERNMENT.—The term "adversary foreign government" means the government of any of the following foreign countries:

(A) North Korea.

(B) Iran.

(C) China.

(D) Russia.

(E) Cuba.

(2) COVERED CLASSIFIED INFORMATION.—The term "covered classified information" means classified information that was—

(A) collected by an element of the intelligence community; or

(B) provided by the intelligence service or military of a foreign country to an element of the intelligence community.

(3) ESTABLISHED INTELLIGENCE CHANNELS.—The term "established intelligence channels" means methods to exchange intelligence to coordinate foreign intelligence relationships, as established pursuant to law by the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the National Security Agency, or other head of an element of the intelligence community.

(4) INDIVIDUAL IN THE EXECUTIVE BRANCH.—The term "individual in the executive branch" means any officer or employee of the executive branch, including individuals—

(A) occupying a position specified in article II of the Constitution;

(B) appointed to a position by an individual described in subparagraph (A); or

(C) serving in the civil service or the Senior Executive Service (or similar service for senior executives of particular departments or agencies).

(b) FINDINGS.—Congress finds that section 502 of the National Security Act of 1947 (50 U.S.C. 3092) requires elements of the intelligence community to keep the congressional intelligence committees "fully and currently informed" about all "intelligence activities" of the United States, and to "furnish to the congressional intelligence committees any information or material concerning intelligence activities * * * which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.".

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

(1) section 502 of the National Security Act of 1947 (50 U.S.C. 3092), together with other intelligence community authorities, obligates an element of the intelligence community to submit to the congressional intelligence committees written notification, by not later than 7 days after becoming aware, that an individual in the executive branch has disclosed covered classified information to an official of an adversary foreign government using methods other than established intelligence channels; and

(2) each such notification should include—

(A) the date and place of the disclosure of classified information covered by the notification;

(B) a description of such classified information;

(C) identification of the individual who made such disclosure and the individual to whom such disclosure was made; and

(D) a summary of the circumstances of such disclosure.

SEC. 2745. SENSE OF CONGRESS ON CONSIDERATION OF ESPIONAGE ACTIVITIES WHEN CONSIDERING WHETHER OR NOT TO PROVIDE VISAS TO FOREIGN INDIVIDUALS TO BE ACCREDITED TO A UNITED NATIONS MISSION IN THE UNITED STATES.

It is the sense of the Congress that the Secretary of State, in considering whether or not to provide a visa to a foreign individual to be accredited to a United Nations mission in the United States, should consider—

(1) known and suspected intelligence activities, espionage activities, including activities constituting precursors to espionage, carried out by the individual against the United States, foreign allies of the United States, or foreign partners of the United States; and

(2) the status of an individual as a known or suspected intelligence officer for a foreign adversary.

Amend the title so as to read:

A bill to authorize appropriations for fiscal years 2018, 2019, and 2020 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

PURPOSE

The purpose of H.R. 3494 is to authorize the intelligence and intelligence-related activities of the United States Government for Fiscal Years (FY) 2018, 2019, and 2020.

CLASSIFIED ANNEX AND COMMITTEE INTENT

The classified annex to this report includes the classified schedule of authorizations and associated explanatory and directive language. The classified schedule of authorizations is incorporated directly into the legislation by Sections 102 and 2102 of the bill. It is the Committee's intent that elements of the Intelligence Community shall strictly comply with all Committee direction and other guidance set forth in the classified annex.

The classified annex and classified schedule of authorizations have been made available for review by all Members of the House of Representatives, on conditions set by the Committee at the time of its consideration of H.R. 3494.

SCOPE OF COMMITTEE REVIEW

The bill authorizes U.S. intelligence and intelligence-related activities within the jurisdiction of the Committee, including the National Intelligence Program (NIP) and the Military Intelligence Program (MIP), the Homeland Security Intelligence Program (HSIP), and the Information Systems Security Program (ISSP). The NIP consists of all activities of the Office of the Director of National Intelligence (ODNI), as well as intelligence, intelligence-related, and counterintelligence activities conducted by: the Central Intelligence Agency; the Department of Defense, including the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and certain activities of the Departments of the Army, Navy, and Air Force; the Department of Energy; the Department of Justice, including the Federal Bureau of Investigation and the Drug Enforcement Administration; the Department of Homeland Security, including the U.S. Coast Guard and intelligence elements of DHS; Department of State; and the Department of the Treasury. The Committee has exclusive or concurrent legislative, authorizing, and oversight jurisdiction of these activities—and exclusive jurisdiction to study the sources and methods of the Intelligence Community.

COMMITTEE STATEMENT, VIEWS, AND UNCLASSIFIED DIRECTION

H.R. 3494, the Intelligence Authorization Act for FY 2020 (the Act) authorizes the activities of, and funding for, the 17 agencies

that comprise the U.S. Intelligence Community (IC). Because most of the intelligence budget involves classified programs, the bulk of the Committee's recommendations each year are found in the classified annex accompanying the bill.

The Act's unclassified legislative text is divided into two divisions: Division A and Division B. Division A contains the FY20 Intelligence Authorization Act. Division B contains the FY18 and FY19 Intelligence Authorization Acts. Unclassified direction for both Division A and Division B is set out below.

Unclassified Direction to Accompany Division A: The Intelligence Authorization Act for Fiscal Year 2020

Increasing Data Security

The Committee is aware the Intelligence Community (IC) faces challenges while trying to balance mission and enterprise needs with IT modernization, including the migration of data and applications to the cloud. With this in mind, the Committee encourages the IC to identify and implement technologies that increase the security posture of data and workloads and reduce cyber risks.

The Committee further recommends that:

1. IC elements identify, develop, and implement tools for bi-directional data migration and division interoperability between data center and cloud environments;

2. these tools include, but not be limited to, encryption of data while both at rest and in motion, and micro-segmentation of networks and workloads; and

3. IC elements prioritize shifting resources towards automation as a way to respond more quickly to cyber threats.

Anonymous Annual Survey Regarding Workplace Climate

Intelligence Community elements obtain mission-critical information from the results of anonymous, annual surveys of their employees, on issues related to workplace climate and retention. As necessary as they are to the elements' own activities, survey results are also vital to the Committee's continuing oversight of elements' efforts to address workplace climate and retention issues, and to propose legislative and other remedies where appropriate.

The need for reliable information is especially acute with respect to sexual harassment and discrimination, given that—established policy and legal protections notwithstanding—an employee may fear that directly raising concerns about such matters risks exposing the employee to retaliatory personnel, security clearance, or other actions. The anonymous survey affords the element, and the committee, a mechanism for inquiring further about the extent of this well-documented chilling effect against reporting; and about the effectiveness (or not) of ongoing programs to uncover and stamp out sexual harassment, discrimination, and other illegal and/or inappropriate activities at the workplace.

Therefore, the Committee directs that no later than 180 days after enactment of this Act, the Director of National Intelligence must certify in writing to the congressional intelligence committees that:

(1) at least once a year, each element of the Intelligence Community submits a survey to its employees regarding work-

place climate and retention matters, and affords employees completing such surveys the option to remain anonymous;

(2) such survey includes questions regarding employees' experiences with sexual assault, discrimination, harassment, including sexual harassment, and related retaliation, including, at a minimum, the following questions:

a. Have you witnessed sexual harassment or sexual assault?

i. Did you report it?

ii. If not, why not?

b. Have you experienced sexual harassment or sexual assault?

i. Did you report it?

ii. If not, why not?

c. Have you experienced retaliation for reporting harassment, discrimination, or sexual assault?

i. Have you faced retribution for taking leave for family, medical, or other personal reasons?

ii. Did you fear retribution for taking leave?

(3) each element includes in its survey questions regarding the job series, position, age, gender, race or ethnicity, field, and job location at the time of the survey's completion;

(4) each element tracks employees' responses according to job series, position, age, gender, race or ethnicity, field, and location at the time of the survey's completion; and

(5) each element reports the results of its survey annually to the congressional intelligence committees.

Report to Congress on the Representation of Women and Minorities in the Workforce

The Committee continues to strongly support Intelligence Community (IC) efforts to identify, recruit, and retain a highly diverse and highly qualified workforce—including, in particular, its efforts to increase the representation within elements of the Intelligence Community of women and minorities.

This is a data driven exercise. Bolstering and adjusting IC workforce diversity programs depends in part on the Committee's regularly obtaining current, detailed and reliable information, and about specific matters relevant to the broader subject of workforce diversity—such as rates and areas of promotion of women and minority employees. But some elements may produce such information only from time to time; others may make regular submissions to the Committee but include only general information.

Therefore, the Committee directs that every six months, the head of each element of the Intelligence Community shall submit to the Committee a written report which shall include, at a minimum:

1. The total number of women and minorities hired by that element during the reporting period and a calculation of that figure as a percentage of the agency's total hiring for that period;

2. The distribution of women and minorities at that element by grade level and by job series in the element's total workforce during the reporting period, together with comparisons from the immediately preceding two years;

3. The number of women and minorities who applied for promotion at the element and the final number selected for promotion during the reporting period;

4. The proportion of the total workforce of the element occupied by each group or class protected by law, as of the last day of the reporting period;

5. The numbers of minorities and women serving in positions at the element requiring advanced, specialized training or certification and the proportion of the workforce those groups occupy; and

To the extent that such element deploys civilian employees to hazardous duty locations, the number of women and minority employees who departed government service subsequent to a deployment undertaken by an employee in the previous two years. *Report on Geospatial Commercial Activities for Basic and Applied Research and Development*

The Committee directs the Director of NGA, in coordination with the DNI, the Director of the Central Intelligence Agency, and the Director of the National Reconnaissance Office, within 90 days of enactment of this Act, to submit to the congressional intelligence and defense committees a report on the feasibility, risks, costs, and benefits of providing the private sector and academia, on a need-driven and limited basis—consistent with the protection of sources and methods, as well as privacy and civil liberties—access to data in the possession of the NGA for the purpose of assisting the efforts of the private sector and academia in basic research, applied research, data transfers, and the development of automation, artificial intelligence, and associated algorithms. Such report shall include:

1. Identification of any additional authorities that the Director of NGA would require to provide the private sector and academia with access to relevant data on a need-driven and limited basis, consistent with applicable laws and procedures relating to the protection of sources, methods, privacy and civil liberties; and

2. Market research to assess the commercial and academic interest in such data and determine likely private-sector entities and institutions of higher education interested in public-private partnerships relating to such data.

NRO Contracting Restrictions

The Committee continues to be very concerned that NRO imposes unnecessary contractual restrictions that prohibits or discourages a contractor from contacting or meeting with a congressional intelligence committee or intelligence committee Member offices. Therefore, the Committee directs NRO to remove all restrictions that impacts contractors from contacting or meeting with the congressional intelligence committees or member offices in all current and future contracts to include pre-coordination with executive branch agencies.

Enhancing Automation at the National Geospatial-Intelligence Agency

The Committee strongly supports efforts to leverage commercial advances in automation of imagery such as electro-optical, infrared,

Wide Area Motion Imagery (WAMI), Full Motion Video (FMV), and Synthetic Aperture Radar (SAR) products to reduce manual processing and improve information flow to users. However, the Committee is concerned that NGA does not dedicate adequate resources to integrate new automation techniques which have resulted in years of research into the issue, but limited operation gains during day to day imagery processing.

Therefore, the Committee directs NGA, within 90 days of enactment of this Act, to brief the congressional intelligence and defense committees on an updated plan to reduce manual processing of imagery such as electro-optical, infrared, WAMI, FMV, and SAR to improve information flow to users. The briefing shall also address:

1. NGA's strategy to leverage commercial advances;
2. The various GEOINT automated exploitation development programs across the National System for Geospatial-Intelligence, and the associated funding and specific purpose of said programs;
3. Any similar efforts by government entities outside the National System for Geospatial-Intelligence of which NGA is aware; and
4. Which of these efforts are duplicative?

Redundant Organic Software Development

The Committee is concerned that NGA is developing software solutions that are otherwise available for purchase on the commercial market. This practice most always, increases the time it takes to deliver new capabilities to the warfighter; increases the overall cost of the solution through expensive operational and maintenance costs; and undermines the U.S. software industrial base.

Therefore, the Committee directs NGA, within 60 days of enactment of this Act, to brief the congressional intelligence committees, to identify all NGA developed software programs and explain why they are being developed organically instead of leveraging commercially available products.

Critical Skills Recruiting for Automation

Although cutting edge sensors have provided the Intelligence Community and Department of Defense with exquisite imagery, full motion video (FMV), and wide area motion imagery (WAMI), intelligence analysts are unable to keep pace with the volume of data being generated. This demands a transformation in the way the intelligence enterprise processes, organizes, and presents data. For that reason, the committee fully supports the NGA's efforts to attract, recruit, and retain a highly competent workforce that can acquire and integrate new data automation tools.

Therefore, the Committee directs NGA, within 60 days of enactment of this Act, to brief the congressional intelligence and defense committees on NGA's efforts to recruit critical skills such as mathematicians, data scientists, and software engineers that possess critical skills needed to support NGA's objectives in automation.

Common Sensitive Compartmented Information Facility

The Committee has become aware of several major impediments for companies to perform work for agencies and organizations like the NRO. For example, businesses without ownership of a Sensitive

Compartmented Information Facility (SCIF) find it very difficult to perform classified work. Additionally, these small businesses are challenged with basic obstacles such as becoming aware of classified work opportunities because it is difficult to obtain access to the IC's and DoD's classified marketplaces such as the Acquisition Resource Center (ARC). Construction and accreditation of SCIF spaces is cost-prohibitive for my small business and non-traditional government contractors. Additionally, construction timeline often exceeds the period of performance of a contract.

A modern trend for innovative and non-traditional government contractors is the increase use of co-working space environments. Additionally, public and private entities are partnering to create emerging regional innovation hubs to help identify technology solutions and products in the private sector that can be utilized by the IC and DoD. These innovation hubs currently produce an agile, neutral, but largely unclassified development environment.

Therefore, the Committee directs DNI, within 90 days of enactment of this Act, to brief the congressional intelligence committees on the following:

1. Steps necessary to establish new 'Common SCIFs' in areas of high demand;
2. What approaches allow for SCIF spaces to be certified and accredited outside of a traditional contractual arrangement;
3. Analysis of the advantages and disadvantages of issuing Department of Defense Contract Security Specification (DD Form 254s) to "Facilities" as opposed to "Contracts";
4. Options for classified co-use and shared workspace environments such as: innovation, incubation, catalyst, and accelerator environments;
5. Pros and cons for public, private, government, or combination owned classified neutral facilities; and
6. Any other opportunities to support hose without ownership of a SCIF effective access to a neutral SCIF.

Improving Use of the Unclassified Marketplaces

Another area where the Committee has become aware of major impediments for companies to perform work for agencies and organizations like the NRO are unclassified marketplaces such as the Acquisition Resource Center (ARC). Instead of posting data to unclassified marketplaces, unclassified NRO postings often refer to the classified side for critical yet unclassified information. If the NRO is serious about embracing commercial innovation, unclassified marketplace postings should remain on the unclassified side.

Therefore, the Committee directs NRO, within 90 days of enactment of this Act, to brief the congressional intelligence committees on options for improving the unclassified marketplace process.

Satellite Servicing

No later than one year after the date of the enactment of this Act, the Director of national Intelligence, in consultation with the Secretary of Defense, shall jointly provide the Intelligence Community and to the congressional defense committees upon request, a briefing detailing the costs, risks, and operation benefits of leveraging commercial satellite servicing capabilities for national security satellite systems. The briefing shall include the following:

1. A prioritized list, with a rationale, of operational and planned assets of the Intelligence Community that could be enhanced by satellite servicing missions.
2. The costs, risks, and benefits of integrating satellite servicing capabilities as part of operational resilience.
3. Potential strategies that could allow future national security space systems to leverage commercial in-orbit servicing capabilities where appropriate and feasible.

Commercial RF Mapping and SAR

U.S. commercial companies are now offering space-based geolocation and GEOINT analysis of radio frequency (RF) emitters as well as synthetic aperture radar (SAR) products. These companies can identify, locate, and analyze previously undetected activity, providing new insights for U.S. national security and defense. The Intelligence Community currently has contracts that leverage commercial electro-optical satellites, however it does not have a program in place to take full advantage of these emerging commercial space-based RF GEOINT and SAR capabilities.

Therefore, the Committee directs the NRO and NGA to brief the committee on how it will leverage these commercial companies in the FY20 and beyond timeframe, to include funding for, as well as test and evaluation efforts.

Commercial Remote Sensing

The Committee supports efforts to establish a light-touch regulatory structure that enables the rapidly evolving commercial space-based imagery, radio-frequency (RF) sensing and radar industry markets promote U.S. leadership in these areas. However, the Committee also supports the needs of the USG to protect both IC and DoD personnel and assets. The Committee believes there can be a balance that supports both national security interests and the promotion of U.S. innovation and leadership.

Therefore, the Committee directs the DNI, in consultation with the Secretary of Defense, to brief the Committee by 1 Dec 2019, on efforts that help address this balance and which streamline the IC and DoD involvement in the rapidly evolving U.S. commercial space-based imagery, radio-frequency (RF) sensing and radar industries.

Deception detection techniques

The U.S. Government does not have sufficient security screening capabilities available to determine deception in individuals that intend to harm the United States. Polygraph has been the most effective investigative tool at our disposal to detect deception, but the cost and time required to administer a polygraph examination is a major cause for security clearance backlogs, and often limits the frequency of periodic examinations to every 5–7 years. Entities within DoD/IC including DIA, SOCOM, NGA, DSS, Air Force and others have expressed a desire to begin piloting new systems such as ocular deception detection systems. However, progress is being hindered by DoD Directive 5210.91 and ODNI Security Agent Directive 2, which direct some oversight of new deception detection technologies to the DoD National Center of Credibility Assessment

(NCCA), which does not have sufficient budget or resources to expeditiously evaluate non-polygraph technologies.

Therefore, the Committee directs the DNI in coordination with the DoD a briefing on what steps they are taking to ensure pilot programs are established to evaluate these new technologies to help reduce our backlog, improve efficiency and reduce overall cost. Pilots program shall evaluate current and emerging technologies to efficiently and rapidly verify the accuracy and truthfulness of statements of candidates for employment within the DoD/IC, including for interim security clearances, for periodic screening of cleared DoD/IC personnel, to screen foreign national collaborators and contractors overseas to prevent Green-on-Blue attacks, for immigration screening and for other purposes.

IC Industry Rotational Program

The Education With Industry (EWI) Program is a highly selective, competitive, non-degree educational assignment within an industry related to the fellow's career field. EWI supports the USAF mission by providing Air Force officers and civil service employees with on-the-job education, experience, and exposure to private sectors of the economy or other government agencies not available through formal courses of instruction.

The EWI program is designed to improve the technical, professional, and management competencies of participating students by partnering with top tier public and private sector innovative companies. During the ten-month tour, students are embedded within an industry team to meet their career specific desired learning objectives. Through hands on exposure to industry best practices, students develop the necessary competencies, skills, knowledge, and abilities to build, sustain and retain a mission-ready workforce. In addition to this, students learn how to better partner with industry, thus developing Air Force leaders with greater business acumen and empathy. The ultimate goal of the program is to provide students the expertise to implement innovative practices when they return to the Air Force as well as understand how to better partner with industry in the future. Upon completion, graduates are assigned to Air Force duty consistent with the education. Unfortunately, the IC does not leverage this program to its fullest extent.

Therefore, the Committee directs the DNI to establish a more robust EWI program for IC personnel. This would entail sending IC technically skilled ambassadors (GS11–GS14) to be embedded in U.S. companies for a one to two-year rotation. The Committee further directs the DNI to brief the Committee on its plans by 1 December 2019.

List of Foreign Entities That Pose a Threat to Critical Technologies

The Committee directs the Director of National Intelligence, in consultation with the Secretary of Defense, to identify, compose, and maintain a list of foreign entities, including governments, corporations, nonprofit and for-profit organizations, and any subsidiary or affiliate of such an entity, that the Director determines pose a threat of espionage with respect to critical technologies or research projects, including research conducted at institutions of higher education.

Maintenance of this list will be critical to ensuring the security of the most sensitive projects relating to U.S. national security, such as defense and intelligence-related research projects. The initial list shall be available to the head of each qualified agency funding applicable projects and will include the following entities already identified as threatening: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, Kaspersky Lab. The Director of National Intelligence and the Secretary of Defense, or a delegate from both agencies, shall brief the findings to the House Committee on Armed Services and the House Permanent Select Committee on Intelligence no later than six months following the enactment of this provision.

Airborne Intelligence, Surveillance, and Reconnaissance Operational Assessment

The Committee recognizes the critical role that Department of Defense airborne intelligence, surveillance, and reconnaissance (ISR) capabilities play supporting military operations worldwide. The committee understands that responsive, persistent, and precise collection of operational information from the air will continue to provide an asymmetric and decisive advantage to operational commanders and tactical forces. The committee also recognizes that to meet the objectives described in the National Defense Strategy, the Department of Defense must modernize and adapt its ISR operating concepts and joint force structure to ensure it can maneuver, fight, and prevail in highly contested environments. However, the committee notes that there is an apparent lack of an integrated joint approach to the Department's ISR modernization strategy. The committee is concerned by recent military service decisions to reduce certain airborne ISR collection platforms without a clear transition plan or approved risk mitigation strategy, despite facing significant deficiencies in collection capacity.

The Committee directs the Secretary of Defense to conduct a stress test of joint intelligence, surveillance, and reconnaissance enterprise capabilities required to achieve the operational objectives of its highest priority global campaign plans and evaluate the capability and capacity of existing service programs of record to satisfy joint force requirements for critical categories of intelligence. The committee also directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by March 1, 2020, on the results of this stress test. The briefing shall include capability and capacity shortfalls in platforms, sensors, and personnel, as well as address proposed risk mitigation strategies to address critical deficiencies.

Protection of National Security Research

The Committee believes that institutes of higher learning, laboratories, and other entities and organizations play critical roles in advancing national security within the U.S. science and technology ecosystem that is charged with delivering the best capabilities to the warfighter in the near, mid, and long-term. The Committee understands that near-peer competitors such as China and Russia attempt to exploit and benefit from the open and collaborative global

research environment created by the Reagan Administration's National Security Decision Directive 189 on the National Policy on the transfer of Scientific, Technical and Engineering Information, which established that the products of "fundamental research"—defined as "basic and applied research in science and engineering, the results of which ordinarily are published and shared"—should remain unrestricted.

The Committee is also aware that academia is not always kept apprised by the interagency of a complete picture of potential activities and threats in the research community, such as improper technology transfer, intellectual property theft, and cyber-attacks directly affiliated with nation-state governments. Elsewhere in this bill and report, the Committee includes measures to promote increased information sharing across the interagency and with academia.

The Committee therefore directs the Secretary of Defense to provide to the Committees on Armed Services of the Senate and House of Representatives and Congressional Intelligence Committees, not later than January 1, 2020, a report listing Chinese and Russian academic institutions that have a history of improper technology transfer, intellectual property theft, cyber espionage, or operate under the direction of their respective armed forces or intelligence agencies. The report should be in unclassified form, though it may contain a classified annex.

Congressional Notification

The Secretary of Defense maintains a responsibility to keep the congressional intelligence and defense committees fully and currently informed of all defense intelligence capabilities and activities to support DOD operational strategic requirements. The Committee is aware that the Under Secretary of Defense for Intelligence (USDI) issued a memorandum in January 2017 providing guidance to defense intelligence components on the necessity of providing timely and accurate notification to Congress of all defense intelligence and counterintelligence activities.

The Committee supports additional efforts to enhance the Department's ability to provide timely, comprehensive, and accurate congressional intelligence notification of intelligence and counterintelligence activities by the defense intelligence components listed in the January 2017 memorandum, to include; the Deputy Chief of staff for Intelligence, U.S. Army; Deputy Chief of staff for Intelligence, Surveillance and reconnaissance, U.S. Air Force; Director of Naval Intelligence, U.S. Navy; Directors of Intelligence, Combatant Commands; Director, NSA; Director, DIA; Director, NGA; Director, NRO; Director, Defense Security Service; and designated DOD officials as reporting officials for defense intelligence and counterintelligence.

Therefore, the Committee directs each of the Defense Intelligence Components listed in the January 2017 memo to provide, in writing, their internal guidance and delineated compliance to the principles of timeliness of reporting, means of reporting, completeness and accuracy of reporting as well as to outline any restrictions, complications or limiting factors, in fully satisfying the direction and intent of the Defense Intelligence Component Reporting of Defense Intelligence and Counterintelligence Activities Memorandum.

For those elements that are also IC elements, written explanation shall include relevant processes and coordination with the ODNI.

The Committee further directs the USD(I) to provide a briefing to the intelligence and defense committees by October 4, 2019, on DOD's current congressional notification policies and procedures regarding defense intelligence activities and support by defense intelligence components supporting DOD. The briefing shall include:

1. Plans to strengthen this notification process by the defense intelligence components, to include notification of new and updated intelligence-sharing arrangements and basic exchange and cooperation agreements with second- and third-party international allies and partners to support DOD requirements; and

2. A description of current and planned coordination efforts with the interagency, specifically the ODNI, to include any dispute resolution processes in regard to conflicting use of defense intelligence capabilities to support defense priorities and objectives.

Strengthening the Integrity of the MIP

The Committee recognizes the Department of Defense's (DOD) efforts to comply with the direction in the committee report accompanying the National Defense Authorization Act for Fiscal Year 2019 (H. Rept. 115–676) to review the Military Intel1igence Program (MIP) budget to more clearly define guidance about which programs, projects, or activities should be assigned to the MIP. The Committee supports the Under Secretary of Defense for Intelligence's action to enhance DOD's ability to make more informed decisions to balance appropriate resourcing against program, projects, or activities on behalf of the Secretary of Defense, while strengthening the overall integrity of the MIP.

Reviewing the Integrated Defense Intelligence Priorities

The committee notes that the Department of Defense is a major provider of intelligence capabilities to the intelligence community, as well as a major consumer of intelligence information. The committee is aware of the operational constraints on the joint force that using the National Intelligence Priorities Framework to guide the allocation of Defense Intelligence Enterprise assets presents, especially for those that are integral to warfighting functions. The committee is concerned that the Integrated Defense Intelligence Priorities (IDIP) activity is not providing the intelligence support to defense operations that section 922 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66) intended.

Therefore, the committee directs the Under Secretary of Defense for Intelligence to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by December 27, 2019, with the current status of the IDIP activity, how the IDIP highlights gaps in defense and national intelligence priorities, and the measures in place to mitigate these gaps. The briefing shall also include details on why the IDIP is distinct from the National Intelligence Priorities Framework, an activity in which IDIP customers currently participate. Finally, the briefing shall also include a recommendation on whether the De-

partment of Defense will continue or suspend the IDIP requirement.

Section 804 Authority

The Fiscal Year 2018 National Defense Amendments Act provided DOD accelerated acquisition authority under Section 804. This authority enhances the ability to streamline a number of processes within the acquisition structure.

The Committee supports effective and efficient acquisition of military intelligence platforms, though wants to ensure this authority is being used in instances where it can be most effective.

Therefore, the Committee directs DOD to provide a list of those acquisition programs funded in whole or in part with MIP that are utilizing authorities under Section 804. The list should be provided to the intelligence and defense committees by December 15, 2019.

Budget Track Presentation

It is important the military services have visibility on all Congressional action which may impact their programs and platforms. The Committee supports a robust and continuing dialog with DOD on intelligence programs.

The budget roll outs are an important inflection point in the dialog between the Congress and DOD. It has been the case that DOD and the Services have not had the complete picture of Congressional action and intent.

Therefore, the Committee directs that budget presentation materials track action from all committees on jurisdiction, be they within the MIP or NIP. Materials should be updated as necessary and ready for the Fiscal Year (FY) 2021 budget cycle and presentations.

Comprehensive Assessment of the Roles, Responsibilities, and Organization of the Office of the Under Secretary of Defense for Intelligence

The Committee recognizes the importance of the Under Secretary of Defense for Intelligence's (USD(I)) management and oversight of the Defense Intelligence Enterprise, and commends the Under Secretary's continued efforts to mature the organization's support to the operational requirements and strategic priorities of the Secretary of Defense. However, the committee notes the shift in priorities and focus of the Office of the Under Secretary of Defense for Intelligence (OUSD(I)), and potential impacts to the organization's ability to effectively execute oversight of the policy, processes, and procedures that guide the Department of Defense's intelligence organizations. The committee further acknowledges that the USD(I) is the principal advisor to the Secretary of Defense and the Deputy Secretary of Defense for all intelligence, intelligence-related, counterintelligence, and security matters, and is responsible for exercising authority, direction, and control over all associated defense intelligence organizations and activities.

Since the establishment of the Under Secretary of Defense for Intelligence (USD(I)) by the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (Public Law 107–314), the roles and responsibilities assigned to the position and office continue to evolve. In 2018, the Deputy Secretary of Defense augmented the responsibilities of USD(I) to include the protection of Department of

Defense physical properties and personnel. Additionally, the committee further clarified the security related responsibilities of USD(I) in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) to include enterprise-wide management and execution of the planning and resourcing for the personnel, physical, and industrial security components of the Department of Defense, as well as the protections required of Department classified information and controlled unclassified information. Most recently, in April 2019, the President directed the transfer of personnel background investigations from the National Background Investigations Bureau to the Office of the Under Secretary of Defense for Intelligence (OUSD(I)), inclusive of the transition of associated operations, personnel, and resources.

As a result, the Defense Security Service, an organization responsible to the USD(I), will be renamed the Defense Counterintelligence and Security Agency (DCSA) and will serve as the primary federal entity for conducting background investigations for the federal government. DCSA will also execute the responsibilities relating to continuous evaluation, insider threat programs, and any other responsibilities assigned to it by the Secretary of Defense. As such, the committee is interested in better understanding how these recent developments might impact the roles and responsibilities of OUSD(I), and the ability of the organization to execute objective oversight and management of the Defense Intelligence Enterprise, as the organization continues to balance the range of priorities specified by the National Defense Strategy.

Accordingly, the committee directs the Comptroller General of the United States provide the congressional defense and intelligence committees with an assessment of the roles, missions, and responsibilities of Office of the Under Secretary of Defense for Intelligence. The assessment should include details regarding USD(I)'s roles and responsibilities, if and how they have changed, and how the USD(I) addressed these changes; to what extent has the USD(I) developed processes for exercising authority, direction, and control over the Defense Intelligence Enterprise (DIE); actions the USD(I) has taken to adapt its approach to executing oversight and governance of the DIE, to include resource management across the aligned defense intelligence agencies; and to what extent the USD(I) has identified any misalignment of its roles and responsibilities regarding the DIE and efforts made to address such mismatch.

The committee further directs the Comptroller General of the United States to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence on preliminary findings with a report to follow to the congressional defense and intelligence committees no later than April 30, 2020.

Development and Integration of Project MAVEN Services

The Committee believes in the importance of developing artificial intelligence capabilities to enhance and augment execution of Defense Intelligence Enterprise (DIE) activities in support of DOD priorities. Activities such as Project MAVEN are important efforts to modernize intelligence tradecraft and develop capabilities that can create efficiencies across the DIE and enhance effectiveness of

defense operations. However, the Committee is concerned about the broad scope of Project MAVEN, and the totality of requirements increasingly levied against the activity, without a comprehensive understanding of the key milestones to track and measure progress and alignment of MAVEN accomplishments against evolving DOD capabilities and activities.

Therefore, the Committee directs the USD(I) to provide a briefing to the congressional intelligence and defense committees by January 3, 2020 on Project MAVEN's strategy for tracking and aligning the activity's milestones against key DIE efforts, such as the Defense Intelligence Agency's Machine-assisted Analytic Rapid-repository System (MARS) and the service-wide Distributed Common Ground System (DCGS), and continued development of Department of Defense advanced analytic tradecraft and foundational intelligence against advance weapons systems and capabilities.

Governance of Data and Service Acquisitions Supporting Defense Intelligence Requirements

The committee recognizes initiatives across the Defense Intelligence Enterprise to collect, analyze, and share data to support critical foundation intelligence mission needs through various modernization initiatives like Project Maven and the Machine-assisted Analytic Rapid-repository System (MARS). However, the committee is concerned there is a lack of coordination and alignment of individual activities ongoing throughout the enterprise.

The committee lacks a comprehensive understanding of how data, information, and services procured in support of defense intelligence requirements are tracked, governed, and made available across the enterprise. The committee is concerned that as defense intelligence organizations move to cloud-based data management infrastructures, there is not enough emphasis on deconflicting these efforts to maximize investment and use across the enterprise and foreign partner coalitions. The committee notes that every effort should be made to ensure acquisition strategies that support these procurements make these products and services available to the entire enterprise, including U.S. allies and partners.

Therefore, the committee directs the Under Secretary of Defense for Intelligence to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence not later than December 6, 2019, on an enterprise level strategy for data, information, and services acquisitions. The briefing shall detail a strategy to ensure these acquisitions are widely available across the Defense Intelligence Enterprise, thus reducing duplicative investments and creating efficiencies in the acquisition and capability management process.

MAVEN Senior Steering Group

Project MAVEN is one of the leading US government programs leveraging commercial technology, however neither the MAVEN Senior Steering Group or the MAVEN Executive Steering Group have representatives from the commercial sector.

Therefore, the Committee directs the MAVEN team to establish a position for a senior commercial executive as an advisor on the Senior Steering Group. The appointment shall be for no longer than a period of two years. Such individual shall comply with

MAVEN conflict of interest protocols, file necessary and required documents, and may not maintain a financial interest in any company with a current MAVEN contract.

Investments in Scientific and Technological Intelligence

The Committee remains interested in the continued efforts of the Department of Defense to improve scientific and technological intelligence (S&TI) capabilities and tradecraft across the Defense Intelligence Enterprise. The Committee recognizes S&TI is critical to strategic competition with near-peer competitors by ensuring comprehensive understanding of adversary capabilities and ability to inform development of joint force fifth-generation advanced weapons systems and other emerging technologies.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence in collaboration with the Director of the Defense Intelligence Agency, to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by December 6, 2019, on the alignment of current and planned Defense Intelligence Enterprise S&TI investments and activities to Department of Defense operational and strategic requirements.

The briefing shall also include information on how the Department of Defense will continue the maturation of S&TI capabilities and tradecraft across the Defense Intelligence Enterprise.

Tactical Exploitation of National Capabilities Program

The Tactical Exploitation of National Capabilities Program (TENCAP) services as the centralized lead to identify and execute national intelligence cross-agency solutions to evaluate, enhance, prototype, and transition technologies across the national intelligence enterprise into military service systems and architectures to create tactical intelligence effects. The Committee supports TENCAP and the flexibility these programs require to mature, but believes that DOD must develop metrics for measuring the impact of affiliated and incubated programs, to more accurately capture which activities and capabilities have successfully transitioned to programs of record and substantiate effectiveness of the joint force. Further, the Committee notes that failure is an intrinsic, and sometimes necessary component of the innovation process, and does not necessarily view failure to transition to a program of record as a negative issue.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence, in coordination with the directors of the military service TENCAP offices, to provide a briefing to the intelligence and defense committees by October 29, 2019 on the plan to develop track, and evaluate metrics associated with the TENCAP program for those projects which transition to a program of record.

Intelligence Support to Defense Operations in the Information Environment

The committee supports Department of Defense efforts to improve capabilities and tradecraft to operate in the information environment. The committee is concerned about the Defense Intelligence Enterprise's (DIE) ability to provide the information oper-

ations community with all-source intelligence support, consistent with the support provided to operations in other domains.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence, in coordination with the Joint Staff Director for Intelligence and the Director of National Intelligence, to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by November 1, 2019, on intelligence support to information operations. The briefing should include standardized defense intelligence lexicon for intelligence preparation of the battlefield for information operations, efforts to develop a process to ensure the full scope of emerging defense information operations threat requirements are structured to be addressed through the entirety of DIE capabilities, and how the Department perceives the future of defense operations in the information environment.

The briefing shall also include a description of how the national intelligence community, through the National Intelligence Priorities Framework, will account for a more dynamic use of defense intelligence capabilities to augment and enhance support to Department of Defense operations in the information environment.

ROTC IC Recruitment Trial Program

The Senior Reserve Officers' Training Corps (ROTC) program, with units or affiliates at approximately 1,600 U.S. colleges and universities, is DOD's largest commissioning source, providing approximately 6,500 new active duty officers to the military each year.

Officer candidates enrolled in ROTC programs must meet all graduation requirements of their academic institutions, enroll in military, naval, or aerospace education courses, and attend summer military training, making them ideal candidates for IC placement. Currently, ROTC cadets only have the option to utilize their training by joining one of the military services. The Committee believes the government can find cost savings and provide a wider range of opportunities to ROTC recruits by leveraging the ROTC's existing training program for the IC.

Therefore, the Committee directs the USDI, in coordination with ODNI, to conduct a feasibility study on creating a pathway for ROTC recruits to find job placement in the IC, on a reimbursable basis. The study should examine:

1. Pros and cons of instituting an ROTC IC recruitment pipeline;
2. Approximate reimbursement cost per recruit; and
3. Legislative requirements for program execution.

The study results must be submitted via report to the intelligence and defense committees by December 15, 2019.

Explosive Ordinance Disposal Intelligence

The Committee is concerned that the expertise of Explosive Ordinance Disposal (EOD) personnel is not adequately accessible and therefore, not sufficiently utilized by the Defense Intelligence Enterprise and IC to provide the combatant commands with the required intelligence to identify, combat, and deter violent extremism and other asymmetric threats.

Explosive ordnance includes all munitions, improvised explosive devices, devices containing explosives, propellants, nuclear fission or fusion materials, biological, and chemical agents. The primary consumer of this information are military tactical explosive ordnance disposal units that employ the data for threat identification and neutralization. However, the required analysis to determine appropriate render-safe capabilities requires operational and strategic intelligence to process and analyze the data, and data management processes to promulgate the resulting information. The Committee believes DOD should modernize the processes and procedures to more comprehensively track, manage, and coordinate the capability and capacity of EOD intelligence within the IC and the DIE to support all levels of render-safe capabilities.

Therefore, the Committee directs the Undersecretary of Defense for Intelligence, in coordination with the DNI, to provide a briefing to the congressional intelligence and defense committees by March 6, 2020 on the capability and capacity of EOD intelligence expertise across the DIE and IC. The briefing shall include:

1. An assessment of the coordination and integration of defense and national intelligence capabilities against EOD intelligence requirements, to include a mitigation strategy to address any identified gaps or deficiencies, information-sharing challenges, or any other impediments to integration of EOD expertise across the defense and intelligence communities; and

2. An assessment of the technical skills needed to address EOD intelligence requirements, while identifying any gaps or deficiencies in current personnel hiring and training structures, and a long-term plan to develop proficiency of EOD intelligence expertise in the defense and intelligence communities.

Information-Sharing Arrangements with India, Japan, and the Republic of Korea

International alliances and partnerships are critical to the pursuit and sustainment of the United States national security objectives, built upon foundations of shared values and intent. The Committee recognizes the importance of the Department of Defense sharing information with international allies and partners in support of the planning and execution of the National Defense Strategy, as allies and third-party international partners enhance strategic stability across the Department's purview while increasing effectiveness of operations. The Committee believes the mechanisms to share information across the "Five Eyes" alliance continue to mature through established exercises, exchange of personnel, and virtual data sharing, while that cooperation is potentially less robust with third-party partners.

The Committee supports the roles and contributions of third-party partners such as India, Japan, and the Republic of Korea, and recognizes their ongoing contribution toward maintaining peace and stability in the Indo-Pacific region. The Committee is interested in understanding the policies and procedures governing the collaboration and information sharing with India, Japan, the Republic of Korea, and the "Five Eyes" alliance, and if opportunities exist to strengthen those arrangements.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of National Intel-

ligence, to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by December 1, 2019, on the benefits, challenges, and risks of broadening the information-sharing mechanisms between India, Japan, the Republic of Korea, and the "Five Eyes" alliance.

Transitioning the Function of Background Investigations to the Department of Defense

Presidential Executive Order 13869 transitions the background investigation functions of the Federal Government from the Office of Personnel Management (OPM), National Background Investigations Bureau, to the Department of Defense, Defense Counterintelligence and Security Agency. The committee recognizes the importance of ensuring timely and efficient background investigations to overcome workforce staffing challenges of cleared individuals across the whole of government and private sector, and to vet personnel who come into contact with the Department's personnel, installations, and technology. The committee is aware of the temporary establishment of the Personnel Vetting Transformation Office in the Office of the Under Secretary of Defense for Intelligence to manage the transition of this activity from OPM to the Department and improve the processes and procedures related to vetting personnel for clearances across the whole of government and private sector.

However, the Committee is concerned about the potential risks to personnel management and mission such a transfer may present, and believes that appropriate protections of civil liberties and privacy must be prioritized throughout the transition, through the implementation of modern and efficient vetting measures. The Committee recognizes the Department's leadership, through sharing best practices with the Office of the Director of National Intelligence, in reforming the vetting process using modern techniques such as continuous evaluation, and expects regular updates on the Department's progress in addressing the current background investigations backlog.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of the Defense Counterintelligence and Security Agency, to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by December 27, 2019, on how the Department of Defense will transfer the background investigation mission and establish an effective personnel vetting capability to provide for the security of the Department, while maintaining the civil liberties and privacy protections of personnel under consideration to receive a clearance.

Language Capability and Capacity

The Committee has long supported a robust Army training language capability and capacity and renews that support in light of the new National Defense Strategy and pivot to hard targets. As is the rest of DOD and the IC, the Army is challenged to meet the language requirement of 2+/2+ as set out by the National Language Board.

Therefore, the Committee directs DOD to prioritize language capability and fully execute the 2+/2+ Plan requirement. The Committee further directs that OSDPR brief the committee on any lim-

iting factors on implementing the 2+/2+ Plan and intended steps for mitigation which shall be briefed to the intelligence and defense committees by October 29, 2019.

Terrestrial Layer System

The Committee has questions about what capabilities the TLS will incorporate and how the platform will balance its signals intelligence, electronic warfare, and cyber operations capabilities.

Therefore, the Committee directs the Army to provide a report and briefing on changes to the Army's doctrine, organization, training, material, leadership, education, personnel and facilities required to develop, procure and employ the Terrestrial Layer System. The report and briefing should be provided to the intelligence and defense committees by December 15, 2019.

Triton Multi-Intelligence Fleet

Critical to the Triton unmanned aerial system is the milestone C update, which added multi-INT capability to the key system attributes. The FY 2020 funding supports aircraft and ground station kit procurements for the Triton Multi INT configuration and resources required to complete modification of the fleet to a Multi-INT capability.

Regrettably, the retrofit to Multi-INT for Low rate initial production 1 and Low rate initial production 2 slipped from 3QT FY18 to 4th QT 19. This slip represents an unacceptable delay of crucial Multi-INT capability for the fleet, particularly in the face of increasing focus on the Pacific. There is little which can be done to buy back the schedule; however, the Multi-INT capability remains a priority for the Committee and should be aggressively pursued by the Navy.

Therefore, the Committee directs the Navy to immediately notify the intelligence and defense committees of any potential delay fielding the Multi-INT capability to the Triton fleet.

Future of Cable Laying and Repair

The USNS ZEUS is the Navy's only cable laying and repair ship and is nearing the end of its service life. The USNS ZEUS is a key component of the Integrated Undersea Surveillance System with primary missions to transport, deploy, retrieve and repair submarine cables and test underwater sound devices and secondary missions to conduct acoustic, hydrographic and bathymetric surveys. The T–ARC(X) supports the fixed surveillance systems and are a key part of the IUSS.

A Cable Capacity Study in 2015 and Maritime Surveillance System Capacity Study completed in 2017 determined that two T–ARC's are required to meet US Government worldwide demand. However, the USNS ZEUS decommission date of 2026 and the bridging solution of a long term charter ships is only leased through 2024, leaving cable laying and ship repair requirements unmet.

Therefore, the Committee directs the Navy to provide to the intelligence and defense committees its plan to meet the current and future for cable laying and repair requirements by October 29, 2019.

Maritime Surveillance Evolution Plan

The Navy is undertaking a comprehensive review of the future of maritime surveillance. This plan is critical to understanding the needs of the Navy as they relate to maritime surveillance.

Therefore, the Committee directs the Navy to deliver the report to the congressional intelligence and defense committees within 30 days of completion and signature of the Maritime Surveillance Evolution Plan.

RQ–21 Blackjack

The Committee has long supported aggressive development and deployment of the RQ–21 Blackjack system, including approving reprogramming funds for development of a v3 next generation engine. The capability differences between the v2 and v3 engine are significant and delay in the v3 engine remains a limiting factor for more expansive deployment of the RQ–21 Blackjack. The Committee is additionally concerned about divergent requirements for capability for the RQ–21 which may be detracting from development of the next generation engine.

Therefore, the Committee directs the Navy to provide to the intelligence and defense committees the timeline for development, integration and deployment of the v3 engine noting limiting factors and suggested mitigation.

Recapitalization of Navy Reserve P–3C Squadrons

The budget request contained $1.2 billion for six P–8A Poseidon aircraft. The budget request for fiscal year 2020 did not take into account the increased warfighter requirement of 21 additional P—8A aircraft. This increase is driven by the proliferation of adversarial submarine fleets and their increasingly active operational tempo. The new requirement includes 12 aircraft to recapitalize the two maritime patrol and reconnaissance squadrons assigned to the Navy Reserve. These squadrons currently operate legacy P–3C Orion aircraft and the Chief of Navy Reserve estimates they will decommission by 2023 unless they are outfitted with new aircraft. The Committee is encouraged by the Navy's recognition of the Navy Reserve force and the contribution they can provide to the increased requirement for the P–8A. However, the Committee was discouraged that the Navy failed to budget for the additional aircraft to meet the warfighting requirement.

Therefore, the Committee directs the Secretary of the Navy to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by March 1, 2020, that outlines a plan to recapitalize the two Navy Reserve squadrons with P–8A aircraft prior to 2023. The briefing should include estimated acquisition costs, acquisition timelines, aircraft fielding schedules, and manpower impacts to the Navy Reserve. The committee also notes that this information should have been briefed at the beginning of the budget cycle.

Navy Research Lab FAR Requirements

The Committee is concerned that government programs too often compete with widely available commercial technological solutions, and in some cases work to duplicate existing and more advanced commercial capabilities. Often, government programs are underper-

forming, lacking capability, missing delivery milestones, and vastly more expensive than commercial solutions. Perhaps most concerning, this practice almost always increases the time it takes to deliver new capabilities to the warfighter.

In particular, Navy Research Labs (NRL) 7442 Geospatial Computing Section has several programs that are competing with commercial industry, even in some cases responding to mission user requirements to provide a "company X-like capability". The Committee is disturbed by such overt duplication of commercial capabilities. Not only does this create a barrier to entry for innovative small businesses and non-traditional companies, the markedly higher expense of organic government programs-which include labor, benefits, infrastructure, hardware, sustainment, operations and maintenance, and cybersecurity-does a disservice to the American taxpayer.

The Federal Acquisition Regulations System (FAR) aims to address this issue, by requiring participants in the acquisition process to deliver on a timely basis the best value product or service to the customer, while maintaining the public's trust and fulfilling policy objectives by: maximizing the use of commercial products and services; using contractors who have a track record of successful past performance or who demonstrate a current superior ability to perform; promoting competition; minimizing administrative operating costs; and conducting business with integrity, fairness, and openness.

Therefore, the Committee expects that authorities within the IC and DOD adhere to the FAR when making acquisition decisions.

Furthermore, the Committee directs NRL to brief the congressional intelligence and defense committees on its identification of all NRL developed software programs and elaborate reasoning for these organically developed programs, vice leveraging commercially available products. Briefing shall be completed by October 29, 2019.

Agile Operations Visualization

The Air Force has made great strides in utilizing agile operations development for a variety of their programs, including Distributed Common Ground System-Air Force. Agile Operations create a nimble model for acquisition and flexibility in programming and fielding capability.

However, the Air Force still struggles to represent the acquisition updates on the traditional waterfall chart. Failure to effectively display and explain the agile operations environment creates confusion and potentially a failure to accurately reflect changes in schedule and performance.

Therefore, the Committee directs the Air Force to create a new format to represent and visualize programs which utilize agile development models. Materials should be ready for the FY 2021 budget cycle and presentation.

Compass Call

The Air Force has made the decision to re-host the COMPASS CALL mission from a C–130 aircraft to a commercial aircraft. In addition, the mission will be 100% contractor logistics support.

The implications of the re-host include increased costs for logistics support, requirement of Federal Aviation Certificates and potential challenges from transitioning a large aircraft to a smaller platform. Additionally, there may be a capability or capacity decrease in the intervening years during the transition.

Therefore, the Committee directs a report on the transition between platforms for the COMPASS CALL mission, due to the intelligence and defense committees by December 15, 2019.

Unified Air Force Airborne Signals Intelligence Enterprise

The Committee notes the goal of the Air Force Airborne Signals Intelligence (SIGINT) Enterprise (ASE) program is to produce an integrated, service-wide, capability-focused SIGINT architecture and investment strategy for the U.S. Air Force (USAF). However, the committee observes that while investment in the ASE program has produced significant advances in Air Force SIGINT capability, particularly within the RC–135 Rivet Joint program, the establishment of a true integrated airborne SIGINT enterprise architecture continues to elude the USAF. The committee is aware that significant capability gaps exist in MQ–9 SIGINT sensor relevancy against current threats, and the Air Force has not yet successfully addressed vanishing vendor issues with the high-altitude Airborne Signals Intelligence Payload (ASIP) program. Additionally, the USAF has not yet achieved a unified enterprise for SIGINT processing, exploitation, and dissemination (PED), despite having a distributed technical architecture within both the RC–135 Rivet Joint and Air Force Distributed Common Ground System (AF–DCGS) programs. The committee believes the Under Secretary of Defense for Intelligence should lead synchronization efforts with the intelligence community to integrate like data sources to enable more comprehensive analysis and exploitation on behalf of the military services.

Therefore, the Committee directs the Air Force to provide a report to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by March 1, 2020, containing the Air Force's vision, strategy, and implementation plan to utilize Air Force airborne SIGINT program resources to establish a unified airborne SIGINT enterprise based on shared joint and intelligence community standards. The committee looks forward to additional clarification on how this enterprise will allow RC–135, U–2, RQ–4, MQ–9, Air Force DCGS SIGINT systems, and future SIGINT capabilities to operate as an integrated enterprise using cloud-based technologies and distributed crew concepts to directly deliver SIGINT data to the joint force from a global Air Force SIGINT system.

OC–135B Open Skies Treaty aircraft recapitalization

The Committee notes that the current fleet of OC–135B aircraft conducting the Open Skies Treaty flights are over 55 years old and experience significant sustainment and reliability issues, resulting in an average mission completion rate of 65 percent between 2007 and 2017. Further, the range of the legacy OC–135 aircraft is insufficient to fully execute mission options within the treaty's 96-hour in-country observation period. In addition to maintenance and range limitations, the current wet-film imaging used to collect data

will become obsolete sometime around 2022. To avoid any gap in Open Skies Treaty collection capability, the committee supports the Air Force's plan to upgrade the fleet with digital visual imaging systems (DVIS) for the near-term, and ultimately replace the OC–135 Open Skies aircraft with two commercially-available small airliner class aircraft with integrated DVIS sensors.

The committee supports recapitalization of the OC–35 but remains concerned about the Air Force's ability to stay on schedule and meet the fiscal year 2022 aircraft certification and treaty compliance date. Unanticipated technical challenges with the DVIS sensors have already affected the schedule and could cause additional delays if not remedied soon.

Therefore, the committee directs the Secretary of the Air Force to provide a report to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by October 1, 2019, on the Open Skies Treaty aircraft recapitalization. The report shall include:

1. an assessment of the DVIS data technical package maturity and the cost and feasibility of integrating it onto the replacement commercial aircraft;
2. the plan for and status of developing or acquiring associated ground processing systems;
3. the plan for management of programmatic risk and an assessment of the ability to meet the fiscal year 2022 deadline for an upgraded, treaty-compliant system;
4. existing or planned mitigation options should the Air Force not be able to achieve current DVIS and treaty compliance milestones, and should there be any future delay to the upgrade or replacement of the OC–135; and
5. a copy of any assessment conducted by an independent organization employed by the program for technical assistance.

Budget Implications of the C4 Restructure

The Committee supports the restructure of the Marines' C4 apparatus, which integrates intelligence and operations. However, the Committee has concerns about the impact on the agility of those intelligence activities.

Therefore, the Committee directs the Marine Corps to provide to the intelligence and defense committees for the implementation for the C4 Restructure to include budget implications for the future year defense plan by October 29, 2019.

Security Certificate Requirements for DCGS–MC

Distributed Common Ground System—Marine Corps provides core critical information for military intelligence corps. DCGS–MC must stay compliant with cyber security certifications and requirements to operate on the network. Schedule for waivers and tech refresh. Staying current with dynamic cyber threats and rapid updates to certifications can be accomplished, however may impact the ability to properly budget effectively to stay current in certifications.

Therefore, the Committee directs the Marines to provide and brief the DCGS cyber security certificate requirement for the future year defense plan (FYDP) to the congressional intelligence and defense committees by October 29, 2019.

Joint Intelligence Operations Center Staffing

The Committee recognizes the evolving operational and strategic priorities of the Department of Defense will impact Defense Intelligence Enterprise capabilities and resources. The committee recognizes the ongoing efforts by the Under Secretary for Intelligence (USDI) to comply with direction specified by the John. S. McCain National Defense Authorization Act for fiscal Year 2019 (Public Law 115–232) to reduce and prevent imbalances in priorities and mitigate against insufficient or misaligned resources within the Defense Intelligence Enterprise.

While the Committee supports the efforts by the USDI to create efficiencies across the Defense Intelligence Enterprise organizations, to include the Service Intelligence Centers and combatant command Joint Operations Intelligence Centers, and enable those elements to plan and posture staffing requirements accordingly, the committee is concerned that the shifts in current and future resourcing are lacking coherence to support the global mandate of the Department.

Therefore, the Committee directs the Undersecretary for Defense Intelligence, in coordination with DIA, to provide a briefing to the congressional intelligence and defense committees by December 27, 2019 on how the Office of the Under Secretary of Defense for Intelligence and DIA are managing resourcing requirements to the combatant command Joint Intelligence Operations Centers to meet current and future needs of the combatant commanders and DOD.

China's Biological Weapons Program

The Committee remains interested in ensuring the Defense Intelligence Enterprise is providing timely, accurate, and effective intelligence to support information needs of the Department of Defense, and is aware of a recent Government Accountability Office report on long-range emerging threats facing the United States that highlighted potential pursuit by near-peer competitors of biological weapons using genetic engineering and synthetic biology.

Therefore, the Committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of the Defense Intelligence Agency, to provide a briefing to the House Committee on Armed Services and House Permanent Select Committee on Intelligence by November 1, 2019, on an assessment of China's current and projected biological weapons program, the risks presented to the joint force, and the mitigation strategies to protect U.S. military forces against said threats.

Machine-assisted Analytic Rapid Repository System Government Accountability Office Review

The re-emergence of great power competition will stress DIA's ability to provide foundational military intelligence for the IC and warfighters. As such, the Committee is supportive of DIA's intent to replace the Modernized Integrated Database (MIDB) with the Machine-assisted Analytic Rapid Repository System (MARS).

However, the Committee is concerned that DIA has not completed an information technology development and procurement project of this scope in the thirty years since MIDB's adoption. MARS's development and procurement will entail a complex and

extensive transformation that will impact the DIA's delivery of foundational military intelligence.

Therefore, the Committee directs the Government Accountability Office (GAO) to provide a report to the congressional intelligence and defense committees no later than September 30, 2020 that describes:

1. The envisioned MIDB users and customer base and how they would use the repository;
2. The extent to which DIA has gathered input from current and historic MIDB users, as well as customers about the capabilities that will be needed for the transition to MARS;
3. The extent to which DIA has planned for MARS's expected new capabilities and the corresponding resources, to include funding and personnel implications;
4. DIA's acquisition strategy for MARS to include the use of any rapid acquisition or prototyping authorities;
5. The extent to which DIA has identified challenges, if any, that it will face in transitioning from MIDB to MARS, and whether it has developed mitigation plans for addressing any of these challenges.

The Committee expects DIA's full cooperation with the GAO study.

The National Intelligence University

In the 115th Congress, the Committee recommended that DIA transfer ancillary, though vital enterprise functions, such as operation of the National Intelligence University (NIU) to the Office of the Director of National Intelligence (ODNI). The Committee is aware the NIU will transfer to ODNI in FY 2021 and is supportive of that effort.

However, the Committee is concerned that DIA will be unable to complete the transfer during fiscal year 2021 due to the unique role NIU serves within DOD's officer education system.

Therefore, the Committee directs the DNI, in consultation with the USD(I) and Director of DIA, to submit a report with its FY 2021 budget request outlining the DIA to ODNI NIU transition plan. At a minimum the report must provide a timeline for the NIU transition, identify any statutory changes required to support the transition, and assess risks to completion of the transfer to include actions ODNI, DOD, or DIA have taken to mitigate identified risks.

Update on the DIA Strategic Approach

In September 2018, the Defense Intelligence Agency (DIA) adopted a Strategic Approach to enhance workforce development, improve foundational military intelligence data management, address perennial intelligence issues and realign roles and missions. Improvements in these issue areas will enhance the Agency's ability to support both the National Security Strategy and National Defense Strategy.

The Committee supports the DIA's initiative to improve those structures it assesses are critical to providing warfighters the information needed to prevent and, if necessary, decisively win wars, such as intelligence on foreign militaries' capabilities.

Therefore, the Committee directs DIA to provide quarterly briefings to the Congressional intelligence and defense committees on its efforts to enhance workforce development, improve foundational military intelligence data management, address perennial intelligence issues and realign roles and missions.

Report on Chinese Efforts Targeting Democratic Elections and U.S. Alliances and Partnerships and Strategy to Counter Chinese Election Interference

The committee directs the Director of National Intelligence in coordination with the Secretary of Defense, the Secretary of State, and the Secretary of Homeland Security, to provide a report to the congressional defense committees, the congressional intelligence committees, the House Committee on Foreign Affairs, the Senate Committee on Foreign Relations, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs on China's influence operations and campaigns targeting democratic elections.

The report shall be divided into two sections, which respectively address influence operations and campaigns targeting: (1) recent and upcoming elections in the United States (dating back to January 1, 2017), and (2) military alliances and partnerships of which the United States is a member. The report should also include a strategy to counter these activities. The committee further directs the Secretary of Defense to provide an interim report not later than November 5, 2019, and a final report not later than September 30, 2020.

The report shall be unclassified and appropriate for release to the public but may include a classified annex. At a minimum, the report should include:

1. An assessment of China's objectives in influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member, and how such objectives relate to the China's broader strategic aims;
2. The United States' strategy and capabilities for detecting, deterring, countering, and disrupting such Chinese influence operations (including recommended authorities and activities) and campaigns and a discussion of the Department of Defense's and intelligence community's respective roles in the strategy;
3. A comprehensive list of specific Chinese state and nonstate entities involved in supporting such Chinese influence operations and campaigns and the role of each entity in supporting them;
4. An identification of the tactics, techniques, and procedures used in previous Chinese influence operations and campaigns;
5. A comprehensive identification of countries with democratic election systems that have been targeted by Chinese influence operations and campaigns since January 1, 2017;
6. An assessment of the impact of previous Chinese influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member, including the views of senior Chinese officials about their effectiveness in achieving Chinese objectives;

7. An identification of countries with democratic elections systems that may be targeted in future Chinese influence operations and campaigns and an assessment of the likelihood that each such country will be targeted;

8. An identification of all U.S. military alliances and partnerships that have been targeted by Chinese influence operations and campaigns since January 1, 2017;

9. An identification of all U.S. military alliances and partnerships that may be targeted in future Chinese influence operations and campaigns and an assessment of the likelihood that each such country will be targeted; and

10. An identification of tactics, techniques, and procedures likely to be used in future Chinese influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member.

Report on Russian Efforts Targeting Democratic Elections and U.S. Alliances and Partnerships and Strategy to Counter Russian Election Interference

The Committee directs the Director of National Intelligence, in coordination with the Secretary of Defense, the Secretary of State, and the Secretary of Homeland Security, to provide a report to the congressional defense committees, the congressional intelligence committees, the House Committee on Foreign Affairs, the Senate Committee on Foreign Relations, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs on Russia's influence operations and campaigns targeting democratic elections.

The report shall be divided into two sections, which respectively address influence operations and campaigns targeting: (1) recent and upcoming elections in the United States (dating back to January 1, 2017), and (2) military alliances and partnerships of which the United States is a member. The report should also include a strategy to counter these activities. The committee further directs the Secretary of Defense to provide an interim report not later than November 5, 2019, and a final report not later than September 30, 2020.

The report shall be unclassified and appropriate for release to the public but may include a classified annex. At a minimum, the report should include:

1. An assessment of Russia's objectives in influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member, and how such objectives relate to Russia's broader strategic aims;

2. The United States strategy and capabilities for detecting, deterring, countering, and disrupting such Russian influence operations (including recommended authorities and activities) and campaigns and a discussion of the Department of Defense's and intelligence community's respective roles in the strategy;

3. A comprehensive list of specific Russian state and nonstate entities involved in supporting such Russian influence op-

erations and campaigns and the role of each entity in supporting them;

4. An identification of the tactics, techniques, and procedures used in previous Russian influence operations and campaigns;

5. A comprehensive identification of countries with democratic election systems that have been targeted by Russian influence operations and campaigns since January 1, 2017;

6. An assessment of the impact of previous Russian influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member, including the views of senior Russian officials about their effectiveness in achieving Russian objectives;

7. An identification of countries with democratic elections systems that may be targeted in future Russian influence operations and campaigns and an assessment of the likelihood that each such country will be targeted;

8. An identification of all U.S. military alliances and partnerships that have been targeted by Russian influence operations and campaigns since January 1, 2017;

9. An identification of all U.S. military alliances and partnerships that may be targeted in future Russian influence operations and campaigns and an assessment of the likelihood that each such country will be targeted; and

10. An identification of tactics, techniques, and procedures likely to be used in future Russian influence operations and campaigns targeting democratic elections and military alliances and partnerships of which the United States is a member.

Unclassified Direction to Accompany Division B: The Intelligence Authorization Acts for Fiscal Years 2018 and 2019

Management of Intelligence Community Workforce

The Committee repeats direction from the *Intelligence Authorization Act for Fiscal Year 2017* that IC elements should build, develop, and maintain a workforce appropriately balanced among its civilian, military, and contractor workforce sectors to meet the missions assigned to it in law and by the president. Starting in Fiscal Year 2019, the Committees no longer authorize position ceiling levels in the annual Schedule of Authorizations.

The Committees look forward to working with the Office of the Director of National Intelligence (ODNI) as it develops an implementation strategy and sets standards for workforce cost analysis tools.

Countering Russian Propaganda

The Committee supports the IC's role in countering Russian propaganda and other active measures. The Committee is committed to providing the appropriate legal authorities, financial resources, and personnel necessary to address these hostile acts. The Committee specifically finds that language capabilities are important to the IC's efforts in countering Russia's hostile acts. The Committee encourages the IC to commit considerable resources in the future to bolstering officers' existing Russian language skills, recruiting Russian language speakers, and training officers in Rus-

sian, in particular key technical language skills. This effort will require strategic planning both in recruiting and rotating officers through language training. The Committee expects to see these priorities reflected in future IC budget requests.

Protection of the Supply Chain in Intelligence Community Acquisition Decisions

The Committee continues to have significant concerns about risks to the supply chain in IC acquisitions. The report to accompany the *Intelligence Authorization Act for Fiscal Year 2017* directed the Director of National Intelligence (DNI) to review and consider changes to Intelligence Community Directive (ICD) 801 ("Acquisition") to reflect issuance in 2013 of ICD 731 ("Supply Chain Risk Management") and issues associated with cybersecurity. It specifically recommended the review examine whether to: expand risk management criteria in the acquisition process to include cyber and supply chain threats; require counterintelligence and security assessments as part of the acquisition and procurement process; propose and adopt new education requirements for acquisition professionals on cyber and supply chain threats; and factor in the cost of cyber and supply chain security. This review was due in November 2017, with a report on the process for updating ICD 801 in December 2017. The report was completed on June 18, 2018.

As a follow-on to this review, the Committees direct DNI to address three other considerations: changes in the Federal Acquisition Regulation that may be necessary; how changes should apply to all acquisition programs; and how security risks must be addressed across development, procurement, and operational phases of acquisition. The Committees further direct the DNI to submit a plan to implement necessary changes within 60 days of completion of this review.

National Geospatial-Intelligence Agency Use of VERA and VSIP Authorities

The Committee encourages the use by the National Geospatial-Intelligence Agency (NGA) of Voluntary Early Retirement Authority (VERA) and Voluntary Separation Incentive Program (VSIP) offers to meet future goals of building a workforce more attuned to automation of data production, automation of analytic processes, and establishment of development and operations ("DevOps") software development processes.

Therefore, the Committee directs the NGA to report to the congressional intelligence committees, within 120 days of enactment of the Act, on its use to date of VERA and VSIP incentives, to include how they have been used to develop an acquisition cadre skilled in "DevOps" software development processes, as well as a plan for further use of these incentives. The report should specify metrics for retooling its workforce, including how it measures data literacy and computational skills in potential hires, and an accounting of the numbers of new hires who have met these higher standards.

Report on Engagement of National Reconnaissance Office with University Community

The Committee recognizes that the survivability and resiliency of United States satellites is critically important to the United States intelligence and defense communities. While the National Reconnaissance Office (NRO) engages with the university community in support of basic research and developing an education workforce pipeline to help advance new technologies and produce skilled professionals, it can do more in this regard to focus on space survivability.

Therefore, the Committee directs the NRO to report, within 120 days of enactment of the Act, on NRO's current efforts and future strategies to engage with university partners that are strategically located, host secure information facilities, and offer a strong engineering curriculum, with a particular focus on space survivability and resiliency. This report should provide a summary of NRO's current and planned university engagement programs, levels of funding, and program research and workforce objectives and metrics. The report should also include an assessment of the strategic utility of chartering a University Affiliated Research Center in this domain.

Clarification of Oversight Responsibilities

The Committee reinforces the requirement for all IC agencies funded by the NIP to respond in a full, complete, and timely manner to any request for information made by a member of the congressional intelligence committees. In addition, the Committees direct the DNI to issue guidelines, within 90 days of enactment of the Act, to ensure that the intent of Section 501 of the National Security Act of 1947 (50 U.S.C. 3091) is carried out.

Clarification on Cooperation with Investigation on Russian Influence in the 2016 Election

The Committee continues to reinforce the obligation for all IC elements to cooperate in a full, complete, and timely manner with the Committee's ongoing investigation into Russian meddling in the 2016 Presidential election and related issues.

Supervisory Feedback as Part of Continuous Evaluation Program

The Committee directs the DNI to review the results of ongoing pilot programs regarding the use of supervisory feedback as part of the periodic reinvestigation and continuous evaluation process and report, within 180 days of enactment of the Act, on the establishment of a policy for its use across the IC.

National Security Threats to Critical Infrastructure

The Committee is aware of significant threats to our critical infrastructure and industrial control systems posed by foreign adversaries. The sensitive nature of the information related to these threats make the role of the IC of vital importance to United States defensive efforts. The Committee has grave concerns that current IC resources dedicated to analyzing and countering these threats are neither sufficient nor closely coordinated.

Framework for Cybersecurity and Intelligence Collection Doctrine

The Committees directs the ODNI, in coordination with appropriate IC elements, to develop an analytic framework that could support the eventual creation and execution of a Government-wide cybersecurity and intelligence collection doctrine. The ODNI shall provide this framework, which may contain a classified annex, to the congressional intelligence committees, within 180 days of enactment of the Act.

This framework shall include:

1. An assessment of the current and medium-term cyber threats to the protection of the United States' national security systems and critical infrastructure;
2. IC definitions of key cybersecurity concepts, to include cyberespionage, cyber theft, cyber acts of aggression, and cyber deterrence;
3. Intelligence collection requirements to ensure identification of cyber actors targeting U.S. national security interests, and to inform policy responses to cyberattacks and computer network operations directed against the United States;
4. The IC's methodology for assessing the impacts of cyberattacks and computer network operations incidents directed against the United States, taking into account differing levels of severity of incidents;
5. Capabilities that the IC could employ in response to cyberattacks and computer network operations incidents, taking into account differing levels of severity of incidents;
6. A policy and architecture for sharing cybersecurity-related intelligence with government, private sector, and international partners, including existing statutory and other authorities which may be exercised in pursuit of that goal; and
7. Any necessary changes in IC authorities, governance, technology, resources, and policy to provide more capable and agile cybersecurity.

Inspector General of the Intelligence Community Role and Responsibilities.

The position of the Inspector General of the Intelligence Community (IC IG) was codified by the *Intelligence Authorization Act for Fiscal Year 2010* to "conduct independent reviews investigations, inspections, audits, and reviews on programs and activities within the responsibility and authority of the Director of National Intelligence" and to lead the IC's IG community in its activities. The Committee is concerned that this intent is not fully exercised by the IC IG and reiterates the Congress's intent that the IC IG's role be over all IC-wide activities in addition to the ODNI. To support this intent, the Committee has directed a number of requirements to strengthen the IC IG's role and expects full cooperation from all Offices of Inspector General across the IC.

The Committee also remains concerned about the level of protection afforded to whistleblowers within the IC and the level of insight congressional committees have into their disclosures. It is the Committee's expectation that all Offices of IG across the IC will fully cooperate with the direction provided elsewhere in the bill to ensure both the DNI and the congressional committees have more

complete awareness of the disclosures made to any IG about any NIP-funded activity.

Space Launch Facilities

The Committee continues to believe it is critical to preserve a variety of launch range capabilities to support national security space missions, and encourages planned launches such as the U.S. Air Force Orbital/Sub-Orbital Program (OSP)-3 NRO–111 mission, to be launched in 2019 on a Minotaur 1 from the Mid-Atlantic Regional Spaceport at Wallops Flight Facility. In the *Intelligence Authorization Act for Fiscal Year 2017*, the Committee directed a brief from the ODNI, in consultation with the Department of Defense (DoD) and the U.S. Air Force, on their plans to utilize state-owned and operated spaceports, which leverage non-federal public and private investments to bolster United States launch capabilities and provide access to mid-to-low or polar-to-high inclination orbits for national security missions.

The Committee directs that the ODNI supplement this brief with how state investments in these spaceports may support infrastructure improvements, such as payload integration and launch capabilities, for national security launches.

Acquisition Research Center Postings

The Committee supports a flexible NRO acquisition process that allows the NRO to choose the most appropriate contracting mechanism, whether for small research and development efforts or large acquisitions. The NRO's Acquisition Research Center (ARC), a classified contracting and solicitation marketplace that NRO and other agencies use, enables this flexible acquisition process for classified efforts.

The Committee directs the NRO, within 60 days of enactment of the Act, to brief the congressional intelligence and defense committees on options for modifying ARC posting procedures to ensure fair and open competition. Those options should include ensuring that unclassified NRO solicitations are posted on the unclassified FEDBIZOPS site and identifying ways to better utilize the ARC to encourage contract opportunities for a more diverse industrial base that includes smaller and non-traditional companies.

Ensuring Strong Strategic Analytical Tradecraft

The DHS's Office of Intelligence and Analysis (I&A) has taken steps to improve the quality of its analysis, to identify its core customers, and to tailor its production to meet customer needs. The Committee concurs with I&A's implementation of analytic standards and review mechanisms that have improved the tradecraft behind I&A productions. The bedrock of these efforts has been the development of a yearly program of analysis (POA) and key intelligence questions, which are essential tools for providing a roadmap and boundaries for the office's production efforts.

Therefore, the Committee directs the Office of I&A to continue to prioritize, develop and hone its strategic intelligence capabilities and production, including the annual development of a POA. Within 90 day of enactment of the Act, and on an annual basis thereafter for two years, I&A shall brief the congressional intelligence committees on the development and execution of its POA. These

briefings should provide an overview of the POA, how customer needs have been incorporated into the POA, and an update on execution against the POA.

Cyber/Counterintelligence Analysis

DHS's Office of I&A's Counterintelligence Mission Center analysis focuses on counterintelligence threats posed by foreign technology companies and fills a gap in IC intelligence production. Advanced technologies are increasingly ubiquitous and necessary to the function of modern society. Consequently, the scope of the threats from countries intent on using these technologies as a vector for collecting intelligence from within the United States will continue to expand. The Office of I&A is well positioned to conduct a niche analysis critical to national security that combines foreign intelligence with domestic threat information.

The Committee strongly supports I&A's Counterintelligence Mission Center's continued focus on these topics and the increased resources the Fiscal Year 2019 dedicated to this analysis. Therefore, the Committee directs the I&A, in coordination with ODNI, to provide an update within 90 days of enactment of the Act on its recent analytic production related to counterintelligence threats posed by foreign technology companies, including a review of the countries and companies that present the greatest risks in this regard.

Intelligence Support to the Export Control Process

The Committee has significant concerns that China poses a growing threat to United States national security, due in part to its relentless efforts to acquire United States technology. China purposely blurs the distinction between its military and civilian activities through its policy of "military-civilian fusion," which compounds the risks of diversion of United States technology to the Chinese military.

The Committee concludes that the United States Government currently lacks a comprehensive policy and the tools needed to address this problem. China exploits weaknesses in existing U.S. mechanisms aimed at preventing dangerous technology transfers, including the U.S. export control system, which is run by the U.S. Department of Commerce's Bureau of Industry and Security (BIS). The Committee has specific concerns about the lack of adequate and effective IC support to BIS's export license application review process and believes more robust IC support could have prevented many of the ill-advised technology transfers that have occurred in recent years.

Therefore, the Committee directs the DNI to submit a plan, within 120 days of enactment of the Act, to describe how the IC will provide BIS with, at a minimum, basic but timely analysis of any threat to U.S. national security posed by any proposed export, reexport, or transfer of export-controlled technology. The plan shall include detailed information on the appropriate organizational structure, including how many IC personnel would be required, where they would be located (including whether they would be embedded at BIS to coordinate IC support), and the amounts of necessary funding. In formulating the plan, the DNI should study the "National Security Threat Assessment" process that the National Intelligence Council uses to inform the actions of the Committee on

Foreign Investment in the United States. The DNI shall submit the plan to the congressional intelligence committees in classified form.

Social Media

The Committees encourages the IC, notably the FBI, to both continue and enhance its efforts to assist in detecting, understanding, and warning about foreign influence operations using social media tools to target the United States. Additionally, within the scope of the IC's authorities, and with all necessary protections for U.S. person information, the Committees encourage the IC to augment and prioritize these ongoing efforts.

Trade-Based Money Laundering

Threats to our national security posed by trade-based money laundering are concerning. Therefore, the Committee directs the DNI, within 90 days of enactment of the Act, to submit a report to the congressional intelligence committees on these threats, including an assessment of the severity of the threats posed to the United States' national security by trade-based money laundering conducted inside and outside the United States; an assessment of the scope of the financial threats to the U.S. economy and financial systems posed by trade-based money laundering; a description of how terrorist financing and drug trafficking organizations are advancing their illicit activities through the use of licit trade channels; an assessment of the adequacy of the systems and tools available to the Federal Government for combating trade-based money laundering; and a description and assessment of the current structure and coordination between Federal agencies, as well as with foreign governments, to combat trade-based money laundering. The report shall be submitted in classified form with an unclassified summary to be made available to the public.

Expansions of Security Protective Service Jurisdiction of the Central Intelligence Agency

The Committee directs the Central Intelligence Agency, in connection with the expansion of its security protective service jurisdiction as set forth in Section 2413, to engage with Virginia state and local law enforcement authorities to ensure that a memorandum of understanding, akin to those in place at other agencies setting forth the appropriate allocation of duties and responsibilities, is in effect.

Unauthorized Disclosures of Classified Information

The Committee is concerned by the recent widespread media reports that purport to contain unauthorized disclosures of classified information. Protecting the nation's secrets from unauthorized disclosure is essential to safeguarding our nation's intelligence sources and methods. An unlawful disclosure of classified information can destroy sensitive collection capabilities and endanger American lives, including those individuals who take great personal risks to assist the United States in collecting vital foreign intelligence.

Federal law prohibits the unauthorized disclosure of classified information, but enforcement is often lacking or inconsistent. Accordingly, the Committee desires to better understand the number of potential unauthorized disclosures discovered and investigated on a

routine basis. Moreover, the Committee has little visibility into the number of investigations initiated by each IC agency or the number of criminal referrals to the Department of Justice. Accordingly, Section 2718 of the Act requires all IC agencies to provide the congressional intelligence committees with a semi-annual report of the number of investigations of unauthorized disclosures to journalists or media organizations, including subsequent referrals made to the United States Attorney General.

Additionally, the Committee wishes to better understand the role of Inspectors General (IGs) within elements of the IC, with respect to unauthorized disclosures of classified information at those elements.

Therefore, the Committee directs the IC IG, within 180 days of enactment of the Act, to provide the congressional intelligence committees with a report regarding the role of IGs with respect to investigating unauthorized disclosures. The report shall address: the roles of IC elements' security personnel and law enforcement regarding unauthorized disclosures; the current role of IGs within IC elements regarding such disclosures; what, if any, specific actions could be taken by such IGs to increase their involvement in the investigation of such matters; any laws, rules or procedures that currently prevent IGs from increasing their involvement; and the benefits and drawbacks of increased IG involvement, to include potential impacts to IG's roles and missions.

Presidential Policy Guidance

The Presidential Policy Guidance (PPG) dated May 22, 2013, and entitled "Procedures for Approving Direct Action Against Terrorist Targets Located Outside the United States and Areas of Active Hostilities" provides for the participation by elements of the IC in reviews of certain proposed counterterrorism operations. The Committees expect to remain fully and currently informed about the status of the PPG and its implementation.

Therefore, the Committee directs ODNI, within five days of any change to the PPG, or to any successor policy guidance, to submit to the congressional intelligence committees a written notification thereof, that shall include a summary of the change and the specific legal and policy justification(s) for the change.

Centers for Academic Excellence

The Committee commends the commitment demonstrated by ODNI's Centers for Academic Excellence (CAE) program managers, IC agencies that sponsored CAE interns, and all other personnel who contributed to the inaugural edition of the CAE Internship Program in recent summers.

The Committees expect the CAE Program to build on this foundation by showing measurable, swift progress, and ultimately fulfilling Congress's intent that the Program serve as a pipeline of the next generation of IC professionals.

Therefore, the Committee directs that the IC take all viable action to expand the CAE Program by increasing, to the fullest extent possible:

1. The number and racial and gender diversity of CAE interns;

2. The number of CAE academic institutions and their qualified internship candidates participating in the CAE Program; and

3. The number of IC elements that sponsor CAE interns.

Report on Violent Extremist Groups

Violent extremist groups like ISIS continue to exploit the Internet for nefarious purposes: to inspire lone wolves; to spread propaganda; to recruit foreign fighters; and to plan and publicize atrocities. As a former Director of the National Counterterrorism Center (NCTC) has stated publicly:

> [W]e need to counter our adversaries' successful use of social media platforms to advance their propaganda goals, raise funds, recruit, coordinate travel and attack plans, and facilitate operations. . . . Our future work must focus on denying our adversaries the capability to spread their messages to at-risk populations that they can reach through the use of these platforms.

Section 403 of the *Intelligence Authorization Act for Fiscal Year 2017* required the DNI, consistent with the protection of sources and methods, to assist public and private sector entities in recognizing online violent extremist content—specifically, by making publicly available a list of insignias and logos associated with foreign extremist groups designated by the Secretary of State. The Committees believe the IC can take additional steps.

Therefore, the Committee directs the Director of NCTC, in coordination with other appropriate officials designated by the DNI, within 180 days of enactment of the Act, to brief the congressional intelligence committees on options for a pilot program to develop and continually update best practices for private technology companies to quickly recognize and lawfully take down violent extremist content online. Such briefing shall address:

1. The feasibility, risks, costs, and benefits of such a program;

2. The U.S. Government agencies and private sector entities that would participate; and

3. Any additional authorities that would be required by the program's establishment.

South China Sea

The South China Sea is an area of great geostrategic importance to the United States and its allies. However, China's controversial territorial claims and other actions stand to undercut international norms and erode the region's stability. It is thus imperative the United States uphold respect for international law in the South China Sea. Fulfilling that objective in turn will require an optimal intelligence collection posture.

Therefore, the Committee directs the DoD, in coordination with DNI, within 30 days of enactment of the Act, to brief the congressional intelligence and defense committees on known intelligence collection gaps, if any, with respect to adversary operations and aims in the South China Sea. The briefing shall identify the gaps and whether those gaps are driven by lack of access, lack of necessary collection capabilities or legal or policy authorities, or by

other factors. The briefing shall also identify IC judgments that assess which intelligence disciplines would be best-suited to answer the existing gaps, and current plans to address the gaps over the Future Years Defense Program.

Military Occupational Specialty-to-Degree Program

The Committee supports the Military Occupational Specialty (MOS)-to-Degree program, which is an innovative framework that enables enlisted Marines to receive credits towards an associate's or a bachelor's degree while earning required MOS credentials. The program partners with colleges and universities to map a Marine's experience and training to equivalent credit, and provides Marines with an awareness of tuition assistance and scholarship programs to enable them to complete the remaining credits towards their degree. The Committees encourage the Marine Corps to expand the MOS-to-Degree program through further curriculum development and enhanced management of the program.

Therefore, the Committee directs the Marine Corps Intelligence Activity (MCIA), within 90 days of the enactment of the Act, to brief the congressional intelligence and defense committees on the Marine Corps' progress towards expanding the MOS-to-Degree program.

Unmanned Aircraft System Pilot Retention

The Committee supports the Marine Corps' vision to grow a more diverse, lethal, amphibious, and middleweight expeditionary force by leveraging emerging technologies, particularly in the area of unmanned and manned-unmanned teaming. Additionally, the Committee is enthusiastic about the Marine Corps' efforts to equip operating forces down to the squad level with a Small Unit Remote Scouting System Family of Small Unmanned Aerial Systems (UAS) capable of operating in all weather conditions across the full spectrum of conflict. The Committee is also aware of the service's concept for a Marine Air Ground Task Force Unmanned Expeditionary (MUX) capability.

However, the Committee is concerned with the projected cost and delays associated with developing this new technology and believe the Marine Corps is ill-prepared to address the growing deficiency in expertise and the manpower challenges that will accompany expansion of the unmanned fleet. Based on observations of the Air Force's and Army's efforts, the Committee believes the Marine Corps' UAS programs will experience pilot and maintainer shortages based on inadequate training, lack of reliable equipment, and the absence of incentive.

Therefore, the Committee directs the Deputy Commandant of Aviation, within 120 days of enactment of the Act, to brief the congressional intelligence and defense committees on potential interim solutions to the gap exposed by the long development time for MUX. Such briefing should also address the Marine Corps' UAS talent management plan, including a strategy for pilot retention and a plan to unify unmanned training that will build a base of instructors and encourage the professionalism of the community.

Remotely Piloted Aircraft Training Strategy

Referring to the directive language found in the committee report accompanying H.R. 2810, the House Armed Services Committee (HASC)-passed FY 2018 National Defense Authorization Act (NDAA) (H. Rept. 115–200), the Committee directs the Secretary of the Air Force, no later than 30 days after enactment of the Act, to brief the congressional intelligence and defense committees on the Air Force's approach to remotely piloted aircraft (RPA) aircrew training, with a particular focus on how the Air Force plans to field simulator capability and training capacity among active and reserve component units supporting RPA operations.

Wide-area Motion Imagery Intelligence Capability

Referring to the directive language found in the committee report accompanying H.R. 2810, the HASC-passed FY 2018 NDAA (H. Rept. 115–200), the Committee directs the Secretary of the Air Force no later than March 1, 2020, to provide to the congressional intelligence and defense committees a report that describes in detail the lifecycle weapon system sustainment and modernization strategy for maintaining an enduring wide-area motion imagery capability for the geographic combatant commanders.

MQ–4C Triton Unmanned Aircraft System

Referring to the directive language found in the committee report accompanying H.R. 2810, the HASC-passed FY 2018 NDAA (H. Rept. 115–200), the Committee directs the Secretary of the Navy, no later than 45 days after enactment of the Act, to brief the congressional intelligence and defense committees on MQ–4C mission execution and tasking, collection, processing, exploitation, and dissemination (TCPED) processes. The briefing shall include or explain:

1. A framework description of the manning, equipping, and training requirements for the MQ–4C system;
2. A description of the baseline architecture of the mission support infrastructure required to support MQ–4C operations;
3. How the Navy plans to support and execute the TCPED processes;
4. How the Navy plans to support flying operations from either line-of-sight or beyond-line-of-sight locations;
5. How many aircraft the Navy plans to dedicate annually to the ISR Global Force Management Allocation Process of the DoD; and
6. How many hours of collection the MQ–4C will be able to provide annually in each of the intelligence disciplines for combatant commanders.

E–8C Joint Surveillance and Target Attack Radar System

Referring to the directive language found in the committee report accompanying H.R. 2810, the HASC-passed FY 2018 NDAA (H. Rept. 115–200), the Committee directs the Secretary of the Air Force, no later than March 1, 2020, to provide to the congressional intelligence and defense committees a report that explains in detail all aspects of how and when the Air Force will transition from legacy Joint Surveillance and Target Attack Radar System (JSTARS) aircraft capability to JSTARS recapitalization aircraft capability.

Acceleration of Increment 2 of Warfighter Information Network-Tactical Program

Referring to Section 111 of H.R. 2810, the HASC-passed FY 2018 NDAA, the Committee directs the Secretary of the Army, no later than January 30, 2020, to submit to the congressional intelligence and defense committees a report detailing potential options for the acceleration of procurement and fielding of the Warfighter Information Network-Tactical Increment 2 program.

Cost-benefit Analysis of Upgrades to MQ–9

Referring to Section 134 of H.R. 2810, the HASC-passed FY 2018 NDAA, the Committee directs the Secretary of Defense, in coordination with the Secretary of the Air Force, within 180 days of enactment of the Act, to provide the congressional intelligence and defense committees an analysis that compares the costs and benefits of the following:

1. Upgrading fielded MQ–9 Reaper aircraft to a Block 5 configuration; and

2. Proceeding with the procurement of MQ–9B aircraft instead of upgrading fielded MQ–9 Reaper aircraft to a Block 5 configuration.

Policy on Minimum Insider Threat Standards

Executive Order 13587 and the National Insider Threat Task Force established minimum insider threat standards. Such standards are required for the sharing and safeguarding of classified information on computer networks while ensuring consistent, appropriate protections for privacy and civil liberties. The Committee understands there are policies in place to attempt implementation of such standards; however, the Committee has found that several elements of the IC have not fully implemented such standards. Therefore, given the several high-profile insider threat issues, the Committee emphasizes the importance of such minimums by statutorily requiring the DNI to establish a policy on minimum insider threat standards, consistent with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, and IC elements should expeditiously establish their own policies and implement the DNI guidance.

Further, referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-passed FY 2019 NDAA, the Committee directs the Chief Management Officer to provide a briefing to the congressional intelligence committees and the congressional armed services committees, no later than 90 days after enactment of the Act, on the outcomes of its cost and technical analyses required by this report, and the Department's efforts to implement enterprise-wide programs and policies for insider threat detection, user activity monitoring, and cyber-attack detection and remediation.

Intelligence Community Information Technology Environment

The Committee remains supportive of the goals of Intelligence Community Information Technology Environment (IC ITE) and the importance of the common, secure sharing infrastructure it creates. The Committee further understands that the path to implement a complex, technical environment such as IC ITE needs to be suffi-

ciently flexible and agile. However, the Committee remains concerned with the lack of consistency and substance in previous reports and briefings on IC ITE. Therefore, Section 2312 requires a long-term roadmap, business plan, and security plan that shall be reported to the congressional intelligence committees at least quarterly with additional notifications as necessary.

Intelligence Community Chief Financial Officer

The Chief Financial Officers (CFO) Act of 1990 mandated best practices for decision-making and accountability, as well as improved decision-makers' access to reliable and timely financial and performance information. The CFO Act, as amended, requires that the chief financial officers of 24 departments and agencies "report directly to the head of the agency regarding financial management matters." Section 2404 brings the ODNI in line with the best practices implemented in the CFO Act.

Intelligence Community Chief Information Officer

As codified in 44 U.S.C. 3506(a)(1)(A), each federal agency head is responsible for 'carrying out the information resources management activities to improve agency productivity, efficiency, and effectiveness.' Accordingly, Section 2405 expresses the Committee's intent to emphasize the importance of the IC Chief Information Officer (CIO), as defined in 50 U.S.C. 3032(a), in assisting the DNI with information resource management by requiring the IC CIO to report directly to the DNI.

Central Intelligence Agency Subsistence for Personnel Assigned to Austere Locations

Section 2411 permits the Director of the CIA to allow subsistence for personnel assigned to austere locations. Although the statute does not define "austere," the Committee believes that utilization of this authority should be minimal. Therefore, within 180 days after the enactment of the Act, the CIA shall brief the congressional intelligence committees on the CIA's definition of "austere" and the CIA regulations in place governing this authority.

Collocation of Certain Department of Homeland Security Personnel at Field Locations

The Committee supports DHS I&A's intent to integrate into operations across the broader DHS enterprise. Accordingly, Section 2434 requires I&A to identify opportunities for collocation of I&A field officers and to submit to the congressional intelligence committees a plan for deployment.

Limitations on Intelligence Community Elements' Communications with Congress

Effective oversight of the IC requires unencumbered communications between representatives of the agencies, members of Congress, and congressional staff. The Committee directs the DNI not to limit any element of the IC from having interactions with the congressional intelligence committees, including but not limited to, preclearance by the DNI of remarks, briefings, discussions of agency resources or authorities requirements, or mandatory reports to

the DNI on conversations with the congressional intelligence committees.

Intelligence Community Support to the National Vetting Center

On February 6, 2018, the President issued National Security Policy Memorandum (NSPM)–9, "Presidential Memorandum on Optimizing the Use of Federal Government Information in Support of National Vetting Enterprise." The memorandum directs the DHS, in coordination with the ODNI and other agencies, to establish the National Vetting Center. The memorandum also requires agencies to "provide the Center access to relevant biographic, biometric, and related derogatory information." It further directs DNI, in coordination with the heads of relevant IC elements, to "establish a support element to facilitate, guide, and coordinate all IC efforts to use classified intelligence and other relevant information within the IC holdings in support of the center." The Committee wishes to obtain regular updates and the most current information about the activities of that support element.

Therefore, no later than 180 days after the enactment of the Act and annually thereafter, the Committee directs the DNI and the Under Secretary for Intelligence and Analysis at DHS to brief the congressional intelligence committees on the status of IC support to the National Vetting Center, as established by NSPM–9.

Update on Status of Attorney General-approved U.S. Person Procedures under Executive Order 12333

The Committee acknowledges the difficult, labor-intensive work undertaken by certain IC elements, to ensure the current effectiveness of, and in some cases to substantially revise, final Attorney General-approved procedures regarding the collection, dissemination, and retention of United States persons information. The Committees wish to better understand the status of this project, throughout the IC.

Therefore, the Committee directs that, not later than 60 days after enactment of the Act, the DNI and the Attorney General shall brief the congressional intelligence committees on the issuance of final, Attorney General-approved procedures by elements of the IC. Specifically, the briefing shall identify (1) any such elements that have not yet issued final procedures; and (2) with respect to such elements, the status of the procedures' development, and any interim guidance or procedures on which those elements currently rely.

Homegrown Violent Extremists Imprisoned in Department of Defense Facilities

The Committee is concerned about an evident gap in information sharing about individuals imprisoned in DoD facilities who are categorized by the FBI as homegrown violent extremists (HVEs). A recent FBI report underscores this gap, highlighting the case of an individual who has been convicted and sentenced to death by a U.S. military court martial and remains incarcerated in a U.S. military facility. The Committee understands that, despite his incarceration, this inmate openly communicates with the outside world through written correspondence and has continued to inspire extremists throughout the world. The Committee further under-

stands that the FBI is unable to determine the full scope of this inmate's contacts with the outside world because only a portion of his communications have been provided by the DoD.

Therefore, no later than 180 days after the enactment of the Act, the Committee directs the FBI to work with the DoD to create a process by which the DoD provides to the FBI the complete communications of individuals imprisoned in DoD facilities and who are categorized by the FBI as HVEs.

Naming of Federal Bureau of Investigation Headquarters

According to statute enacted in 1972, the current FBI headquarters building in Washington, D.C. must be "known and designated" as the "J. Edgar Hoover FBI Building." That tribute has aged poorly. It should be reconsidered, in view of Hoover's record on civil liberties—including the effort to disparage and undermine Dr. Martin Luther King Jr. Even today, Hoover's name evokes the Bureau's sordid "COINTELPRO" activities.

The Committee believes Congress should consider repealing the provision requiring the existing Pennsylvania Avenue building to be known as the "J. Edgar Hoover FBI Building." A new name should be determined, through a joint dialogue among Bureau leadership, law enforcement personnel, elected officials, and civil rights leaders.

Foundational Intelligence Analysis Modernization

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-passed FY 2019 NDAA, the Committee directs the Joint Staff Director for Intelligence, in coordination with the USD(I) and the Director of the DIA, to develop a plan within 60 days of enactment of the Act, to modernize systems used to provide foundational intelligence.

Further, the Committee directs the Joint Staff Director for Intelligence, in coordination with the DIA Director, to provide a briefing to the congressional intelligence committees and the congressional armed services committees, within 90 days after enactment of the Act, on such plan to modernize foundational intelligence systems. If a determination is made that a new system is required, the Committees expect the Battlespace Awareness Functional Capabilities Board to validate the requirements for any new system, and that the acquisition plan will follow best practices for the rapid acquisition and improvement of technology dependent systems.

Science, Technology, Engineering, and Math careers in Defense Intelligence

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-passed FY 2019 NDAA, the Committee directs the Director of DIA to provide a briefing to the congressional intelligence committees and the congressional armed services committees, within 90 days after enactment of the Act, on a plan to develop a Science, Technology, Engineering, and Math career program that attracts and maintains the defense intelligence cadre of Science and Technical Intelligence analysts to meet tomorrow's threats.

Security and Intelligence Role in Export Control

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-passed FY 2019 NDAA, the Committee directs the Under Secretary of Defense for Policy, in coordination with the USD(I), within 60 days of enactment of the Act, to brief the congressional intelligence committees and the congressional armed services committees, on security support to export control.

Security Clearance Background Investigation Reciprocity

Referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-passed FY 2019 NDAA, the Committee directs the Secretary of Defense, in coordination with the DNI and the Director of the Office of Personnel Management, within 60 days of enactment of the Act, to brief the congressional intelligence committees and the congressional armed services committees on efforts to ensure seamless transition of investigations between authorized investigative agencies, as required by law.

Further, referring to the directive language found in the committee report accompanying H.R. 5515, the HASC-passed FY 2019 NDAA, the Committee directs the Secretary of Defense, in coordination with the DNI and the Director of the Office of Personnel Management, within 90 days of enactment of the Act, to brief the congressional intelligence committees on efforts to ensure reciprocity is a consideration for implementation of continuous evaluation and continuous vetting across the federal government.

Foreign Influence Task Force

The IC has warned of active measures taken by foreign actors to interfere with and undermine the U.S. democratic process, most recently and brazenly by the Russian Federation. The Committee appreciates FBI efforts to confront this challenge in part through creation of its Foreign Influence Task Force. The Committee believes that confronting foreign influence directed at the United States is of fundamental importance, and thus desires to engage in a close and regular dialogue with the FBI about the task force's activities.

Therefore, the Committee directs the FBI to provide detailed, quarterly briefings to the congressional intelligence committees, regarding the task force's activities, to include its progress and any significant challenges.

Joint System Integration Lab Annual Briefing

The Joint System Integration Lab (JSIL) at Redstone Arsenal, Alabama enables testing of critical military intelligence capabilities, including unmanned aerial system (UAS) sensors, modeling and simulation, and integration between and among service UASs. The Committee seeks to remain fully and currently informed about this important work.

Therefore, the Committee directs the JSIL, within 180 days of enactment and annually for two years thereafter, to brief the congressional intelligence and defense committees, on intelligence and intelligence-related activities conducted by the JSIL.

Enhanced Oversight of IC Contractors

A topic of sustained congressional intelligence committee interest has been improving the federal government's oversight of IC acquisition and procurement practices, including activities by poorly performing IC contractors.

A framework exists to ensure that IC elements do not award IC contracts to businesses that engage in negligence or even gross negligence, consistently fail to appropriately safeguard classified information, maintain poor financial practices, or other issues. For example, an IC element may maintain a list of contractors of concern, in order to ensure that proposals from such contractors are rejected or subjected to additional scrutiny. The Committee wishes to build on these practices and is concerned about the existing framework's adequacy.

Therefore, the Committee directs all elements of the IC, to the fullest extent consistent with applicable law and policy, to share with one another information about contractors with track records of concern—such as the commission of negligence or gross negligence in the performance of IC contracts, or the repeated failure to appropriately safeguard classified information in a fashion that the contractor reasonably could have been expected to prevent.

Additionally, no later than 30 days after enactment of the Act, the DNI shall brief the congressional intelligence committees on the authorities of IC elements with respect to contractors with track records of concern—before, during, and after procurement. An objective of the briefing will be to discuss information sharing practices in this regard, and to identify specific areas where the oversight framework can be strengthened.

COMMITTEE CONSIDERATION AND ROLL CALL VOTES

On June 27, 2019, the Committee met in open session to consider H.R. 3494 and ordered the bill favorably reported.

In open session, the Committee considered an amendment in the nature of a substitute, offered by Mr. Schiff to H.R. 3494. The amendment was adopted by unanimous voice vote.

Mr. Schiff then moved to make the classified Fiscal Year 2020 schedule of authorizations available for Members of the House to review. The motion was agreed to by a recorded vote of 20 ayes to 0 noes:

Voting aye: *Schiff; Himes; Sewell; Carson; Speier; Quigley; Heck; Welch; Maloney; Demings; Krishnamoorthi; Nunes; Conaway; Turner; Wenstrup; Stewart; Crawford; Stefanik; Hurd; Ratcliffe*

Voting no: *None*

The Committee then agreed to a motion by the Chairman to favorably report H.R. 3494, as amended, to the House, including by reference the classified schedules of authorizations. The motion was agreed to by a unanimous voice vote.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION OF AMENDMENT

Section 1—Short Title; Table of contents

Section 1 lists the short title of the Intelligence Authorization Act for Fiscal Year 2018, 2019, and 2020 (the Act).

Section 2—Divisions and table of contents

Section 2 sets out the divisions of the bill and the table of contents for the bill. Division A consists of authorizations for Fiscal Year 2020. Division B consists of authorizations that were previously introduced for Fiscal Year 2018 and Fiscal Year 2019.

Section 3—Definitions

Section 3 defines the terms "congressional intelligence committees" and the "Intelligence Community" (IC) that will be used in the Act.

DIVISION A

TITLE I—INTELLIGENCE ACTIVITIES

Section 101—Authorization of appropriations

Section 101 lists the U.S. Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for Fiscal Year 2020.

Section 102—Classified Schedule of Authorizations

Section 102 provides that the amounts authorized to be appropriated for intelligence and intelligence-related activities and the personnel levels for Fiscal Year 2020 are contained in the classified Schedule of Authorizations and that the classified Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

Section 103—Intelligence Community Management Account

Section 103 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the DNI.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201—Authorization of appropriations

Section 201 authorizes appropriations in the amount of $514,000,000 for Fiscal Year 2018 for the Central Intelligence Agency (CIA) Retirement and Disability Fund.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

Section 301—Restriction on conduct of intelligence activities

Section 301 provides that the authorization of appropriations by the Act shall not be deemed to constitute authority for the conduct of any intelligence activity that is not otherwise authorized by the Constitution or laws of the United States.

Section 302—Increase in employee compensation and benefits authorized by law

Section 302 provides that funds authorized to be appropriated by the 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 compensation or benefits authorized by law.

Section 303—Paid parental leave

Section 303 establishes a paid parental leave program for employees of elements of the IC. Each IC element that receives a request is required to grant that request unless the requested leave would unduly disrupt operations. The IC elements must each submit to the intelligence committees an implementation plan that reports on the changes in processes to implement the new benefit and explains how agencies contain a mix of IC and non-IC offices are implementing this IC benefit. The section requires the DNI to issue an Intelligence Community Directive (ICD) implementing this benefit within 180 days of the enactment of the statute.

Section 304—Unfunded requirements of the intelligence community

Section 304 requires the DNI, upon request, to provide a briefing to the congressional intelligence and appropriations committees about an IC element's unfunded priorities—*i.e.*, an element head's request that was not included in the DNI's budget request to the President or that was requested by the DNI but was not in the President's budget request that was sent to Congress.

Section 305—Extending the Intelligence Identities Protection Act of 1982

Section 305 amends the definition of "covert agent" in the National Security Act of 1947 (50 U.S.C. § 3126(4)) so as to protect all intelligence officers whose identities as such are currently classified, and all United States citizens whose relationship to the United States is currently classified—regardless of the location of the individuals' government service or activities or time since separation from service.

The Intelligence Identities Protection Act of 1982 (IIPA) had amended the National Security Act to permit prosecution *only* if, among other things, an individual disclosed the classified identities of intelligence officers who were currently serving overseas or had within the past five years; or those of U.S. citizens having a classified intelligence relationship to the United States and residing and acting for a U.S. intelligence agency overseas. Section 305 removes the IIPA's temporal and geographic limitations, both to account for a changing threat environment, and to address the fact that undercover IC officers and others assisting the IC can and often do perform highly sensitive work warranting protection by the IIPA—though without serving abroad in recent years.

Section 306—Intelligence community public-private talent exchange

Section 306 requires the Director of National Intelligence to develop policies, processes, and procedures to allow for the detail of IC employees to the private sector and the detail of private sector employees to the IC. The section also provides the heads of IC elements with authorities to detail employees under the terms of the DNI's policies.

Section 307—Assessment of contracting practices to identify certain security and counterintelligence concerns

Section 307 requires the Director of National Intelligence to conduct an assessment of the authorities, policies, processes, and standards used by the IC to ensure that the IC is weighing security

and counterintelligence risks in contracting with companies that contract—or carry out joint research and development—with the People's Republic of China, the Russian Federation, the Democratic People's Republic of Korea, or the Islamic Republic of Iran.

Section 308—Required counterintelligence briefings and notifications

Section 308 requires the Director of National Intelligence to post publicly advisory reports on foreign counterintelligence and cybersecurity threats to federal election campaigns. It also requires quarterly briefings regarding the Federal Bureau of Investigation's counterintelligence activities and prompt notification of an investigation carried out regarding a counterintelligence risk related to a federal election or campaign.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Section 401—Establishment of the Climate Security Advisory Council

Section 401 requires the Director of National Intelligence to establish an advisory council to assist analytic components of the IC with incorporating analysis of climate security into their work. The council will also facilitate coordination and sharing of data between the IC and non-IC elements related to climate change.

Section 402—Transfer of National Intelligence University to the Office of the Director of National Intelligence

Section 402 requires the Director of the Defense Intelligence Agency to transfer to the Director of National Intelligence the functions, personnel, assets, and liabilities of the National Intelligence University.

TITLE V—MATTERS RELATING TO FOREIGN COUNTRIES

Section 501—Annual reports on influence operations and campaigns in the United States by the Communist Party of China

Section 501 requires the Director of the National Counterintelligence and Security Center to submit an annual report to the congressional intelligence committees concerning the influence operations and campaigns in the United States conducted by the Communist Party of China.

Section 502—Report on repression of ethnic Muslim minorities in the Xinjiang region of the People's Republic of China

Section 502 requires the Director of National Intelligence to submit a report to the congressional intelligence committees concerning activity by the People's Republic of China to repress ethnic Muslim minorities in the Xinjiang region of China.

Section 503—Report on efforts by People's Republic of China to influence election in Taiwan

Section 503 requires the Director of National Intelligence to submit a report within 45 days of the 2020 Taiwan Presidential and Vice Presidential elections concerning any influence operations by

China to interfere in or undermine the election and efforts by the United States to disrupt those operations.

Section 504—Assessment of legitimate and illegitimate financial and other assets of Vladimir Putin

Section 504 expresses the sense of Congress that the United States should do more to expose the corruption of Russian President Vladimir Putin and directs the Director of National Intelligence to submit to appropriate congressional committees an assessment on the net worth and financial and other assets of President Putin and his family members.

Section 505—Assessments of intentions of political leadership of the Russian Federation

Section 505 directs the Intelligence Community to submit assessments to certain congressional committees of the current intentions of the political leadership of the Russian Federation concerning potential military action against members of the North Atlantic Treaty Organization (NATO), responses to an enlarged United States or NATO military presence in Eastern Europe, and potential actions taken for the purpose of exploiting perceived divisions among the governments of Russia's Western adversaries.

Section 506—Report on death of Jamal Khashoggi

Section 506 directs the Director of National Intelligence to submit a report to the congressional intelligence committees concerning the death of Jamal Khashoggi within thirty days of the enactment of the Intelligence Authorization Act.

TITLE VI—FEDERAL EFFORTS AGAINST DOMESTIC TERRORISM

Section 601—Definitions

Section 601 sets forth certain definitions that apply to Title VI.

Section 602—Annual strategic intelligence assessment of and comprehensive report on domestic terrorism

Section 602 requires the annual submission of a joint report to certain congressional committees on domestic terrorism by the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Under Secretary of Homeland Security for Intelligence and Analysis. The report must contain a strategic intelligence assessment on domestic terrorism; a discussion of the activities undertaken by the federal government related to domestic terrorism investigations; and data concerning domestic terrorism incidents, investigations, the filing of federal or non-federal charges against suspects, and the personnel levels and intelligence products produced by the executive branch. Finally, Section 602 requires the executive branch to provide to the congressional committees certain policy documents.

TITLE VII—REPORTS AND OTHER MATTERS

Section 701—Modification of requirements for submission to congress of certain reports

Section 701 amends or cancels numerous reporting requirements under current law.

Section 702—Increased transparency regarding counterterrorism budget of the United States

Section 702 makes several findings regarding the transparency of the IC's counterterrorism budget and directs a briefing from the executive branch on the feasibility of releasing additional information to the public concerning the IC's efforts on counterterrorism.

Section 703—Task force on illicit financing of espionage and foreign influence operations

Section 703 requires the Director of National Intelligence to establish a task force to study and assess the illicit financing of espionage and foreign influence operations directed at the United States and requires the task force to issue a report on this subject to the appropriate congressional committees.

Section 704—Study on role of retired and former personnel of intelligence community with respect to certain foreign intelligence operations

Section 704 requires the Director of National Intelligence to conduct a study on former intelligence community personnel providing intelligence assistance to or for the benefit of a foreign country and to provide the study to the congressional intelligence committees.

Section 705—Report by Director of National Intelligence on fifth-generation wireless network technology

Section 705 directs the Director of National Intelligence to submit to the intelligence committees a report on the threat to the national security of the United States posed by adoption of fifth-generation wireless network built by foreign companies and possible efforts to mitigate the threat.

Section 706—Establishment of 5G prize competition

Section 706 establishes a program to award prizes to stimulate research and development relevant to fifth-generation wireless technology.

Section 707—Establishment of deepfakes prize competition

Section 707 establishes a program to award prizes to stimulate the research, development, or commercialization of technologies to automatically detect machine-manipulated media.

DIVISION B

TITLE XXI—INTELLIGENCE ACTIVITIES

Section 2101—Authorization of appropriations

Section 2101 lists the United States Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for Fiscal Year 2019. The bill deems authorized the funds already appropriated for Fiscal Year 2018.

Section 2102—Classified schedule of authorizations

Section 2102 provides that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activi-

ties for Fiscal Year 2019 are contained in classified Schedule of Authorizations and that the classified Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

Section 2103—Intelligence Community Management Account

Section 104 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the ODNI for Fiscal Year 2019.

TITLE XXII—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 2201—Authorization of appropriations

Section 201 authorizes appropriations in the amount of $514,000,000 for the CIA Retirement and Disability Fund for Fiscal Year 2019.

Section 2202—Computation of annuities for employees of the Central Intelligence Agency

Section 2202 makes technical changes to the CIA Retirement Act to conform with various statutes governing the Civil Service Retirement System.

TITLE XXIII—GENERAL INTELLIGENCE COMMUNITY MATTERS

Section 2301—Restriction on conduct of intelligence activities

Section 2301 provides that the authorization of appropriations by the Act shall not be deemed to constitute authority for the conduct of any intelligence activity that is not otherwise authorized by the Constitution or laws of the United States.

Section 2302—Increase in employee compensation and benefits authorized by law

Section 2302 provides that funds authorized to be appropriated by the 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 compensation or benefits authorized by law.

Section 2303—Modification of special pay authority for science, technology, engineering, or mathematics positions and addition of special pay authority for cyber positions

Section 2303 provides an increased yearly cap for Science, Technology, Engineering, or Mathematics (STEM) employee positions in the IC that support critical cyber missions. Section 303 also permits the National Security Agency (NSA) to establish a special rate of pay for positions that perform functions that execute the agency's cyber mission.

Section 2304—Modification of appointment of chief information officer of the intelligence community

Section 2304 changes the position of IC Chief Information Officer from being subject to presidential appointment to being subject to appointment by the DNI.

Section 2305—Director of national intelligence review of placement of positions within the intelligence community on the executive schedule

Section 2305 requires the DNI, in coordination with the Office of Personnel Management, to conduct a review of the positions within the IC that may be appropriate for inclusion on the Executive Schedule, and the appropriate levels for inclusion.

Section 2306—Supply chain and counterintelligence risk management task force

Section 2306 requires the DNI to establish a task force to standardize information sharing between the IC and the United States Government acquisition community with respect to supply chain and counterintelligence risks. Section 2306 further provides requirements for membership, security clearances, and annual reports.

Section 2307—Consideration of adversarial telecommunications and cybersecurity infrastructure when sharing intelligence with foreign governments and entities

Section 2307 requires the IC, when entering into foreign intelligence sharing agreements, to consider the pervasiveness of telecommunications and cybersecurity infrastructure, equipment, and services provided by United States adversaries or entities thereof.

Section 2308—Cyber protection support for the personnel of the intelligence community in positions highly vulnerable to cyber attack

Section 2308 permits the DNI to provide cyber protection support for the personal technology devices and personal accounts of IC personnel whom the DNI determines to be highly vulnerable to cyber attacks and hostile information collection activities.

Section 2309—Elimination of sunset authority relating to management of supply-chain risk

Section 2309 eliminates the sunset of certain IC procurement authorities to manage and protect against supply chain risks.

Section 2310—Limitations on determinations regarding certain security classifications

Section 2310 prohibits an officer of the IC who is nominated to a Senate-confirmed position from making certain classification determinations posing potential conflicts of interest regarding that nominee.

Section 2311—Joint intelligence community council

Section 2311 amends Section 101A of the National Security Act of 1947 (50 U.S.C. 3022(d)) as to the Joint Intelligence Community Council meetings and to require a report on its activities.

Section 2312—Intelligence community information technology environment

Section 2312 defines the roles and responsibilities for the performance of the Intelligence Community Information Technology Environment (IC ITE). Section 2312 requires certain reporting and

briefing requirements to the congressional intelligence committees regarding the IC's ongoing implementation of IC ITE.

Section 2313—Report on development of secure mobile voice solution for intelligence community

Section 2313 requires the DNI, in coordination with the Directors of the CIA and NSA, provide the congressional intelligence committees with a classified report on the feasibility, desirability, cost, and required schedule associated with the implementation of a secure mobile voice solution for the intelligence community.

Section 2314—Policy on minimum insider threat standards

Section 2314 requires the DNI to develop minimum insider threat standards to be followed by each element of the IC, consistent with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

Section 2315—Submission of intelligence community policies

Section 2315 requires the DNI to make all ODNI policies and procedures available to the congressional intelligence committees. Section 2315 also requires ODNI to notify the congressional committees of any new or rescinded policies.

Section 2316—Expansion of intelligence community recruitment efforts

Section 2316 requires the DNI, in consultation with IC elements, to submit a plan to congressional intelligence committees as to each element's efforts in recruitment from rural and underrepresented regions.

TITLE XXIV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SUBTITLE A—OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Section 2401—Authority for protection of current and former employees of the Office of the Director of National Intelligence

Section 2401 amends Title 50, section 3506, to provide protection for current and former ODNI personnel and designated immediate family members, if there is a national security threat that warrants such protection.

Section 2402—Designation of the Program Manager-Information Sharing environment

Section 2402 amends the Intelligence Reform and Terrorism Protection Act of 2004 so that the Program Manager-Information Sharing Environment (PM–ISE) is subject to appointment by the DNI, not the President.

Section 2403—Technical modification to the Executive Schedule

Section 2403 amends the Executive Schedule to make the Director of the National Counterintelligence and Security Center a Level IV position on the Executive Schedule.

Section 2404—Chief Financial Officer of the Intelligence Community

Section 2404 amends the National Security Act of 1947 by requiring the Chief Financial Officer of the Intelligence Community to directly report to the DNI.

Section 2405—Chief Information Officer of the Intelligence Community

Section 2405 amends the National Security Act of 1947 by requiring the Chief Information Officer of the Intelligence Community to directly report to the DNI.

SUBTITLE B—CENTRAL INTELLIGENCE AGENCY

Section 2411—Central Intelligence Agency subsistence for personnel assigned to austere locations

Section 2411 authorizes the Director of the CIA to approve, with or without reimbursement, subsistence to personnel assigned to an austere overseas location.

Section 2412—Special rules for certain monthly workers' compensation payments and other payments for Central Intelligence Agency Personnel

Section 2412 authorizes the Director of the CIA to provide enhanced injury benefits to a covered employee or qualifying dependents who suffer an injury overseas due to war, insurgency, hostile act, or terrorist activities.

Section 2413—Expansion of security protective service jurisdiction of the Central Intelligence Agency

Section 2413 expands the security perimeter jurisdiction at CIA facilities from 500 feet to 500 yards.

Section 2414—Repeal of foreign language proficiency requirement for certain senior level positions in the Central Intelligence Agency

Section 2414 repeals Title 50, section 3036(g), with conforming amendments to section 611 of the Intelligence Authorization Act for Fiscal Year 2005 (Public Law 108–487).

SUBTITLE C—OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE OF DEPARTMENT OF ENERGY

Section 2421—Consolidation of Department of Energy Office of Intelligence and Counterintelligence

Section 2421 amends the Department of Energy Organization Act to consolidate the offices of intelligence and counterintelligence into the DOE Office of Intelligence and Counterintelligence.

Section 2422—Establishment of Energy Infrastructure Security Center

Section 2422 establishes the Energy Infrastructure Security Center under the Department of Energy Office of Intelligence and Counterintelligence that will be responsible for coordinating intel-

ligence regarding the to the protection of U.S. energy infrastructure.

Section 2423—Repeal of Department of Energy Intelligence Executive Committee and Budget Reporting Requirement

Section 2423 amends the Department of Energy Organization Act by repealing the Department of Energy Intelligence Executive Committee, as well as certain budgetary reporting requirements.

SUBTITLE D—OTHER ELEMENTS

Section 2431—Plan for designation of counterintelligence component of defense security service as an element of intelligence community

Section 2431 directs the DNI and the Under Secretary of Defense for Intelligence, in coordination with the Director of the National Counterintelligence and Security Center, to provide the congressional intelligence and defense committees with an implementation plan to make the Defense Security Service's (DSS's) Counterintelligence component an element of the IC as defined in paragraph (4) of section 3 of the National Security Act of 1947 (50 U.S.C. 3003(4)), by January 1, 2021. Section 2431 further provides that the plan shall not address the DSS's personnel security functions.

Section 2432—Notice not required for private entities

Section 2432 provides a Rule of Construction that the Secretary of the DHS is not required to provide notice to private entities before issuing directives on agency information security policies and practices.

Section 2433—Establishment of advisory board for National Reconnaissance Office

Section 2433 amends the National Security Act of 1947 to authorize the Director of the NRO to establish an advisory board to study matters related to space, overhead reconnaissance, acquisition, and other matters. Section 2433 provides that the board shall terminate three years after the Director declares the board's first meeting.

Section 2434—Collocation of certain Department of Homeland Security personnel at field locations

Section 2434 requires DHS I&A to identify opportunities for collocation of I&A field officers and to submit to the congressional intelligence committees a plan for deployment.

TITLE XXV—ELECTION MATTERS

Section 2501—Report on cyber attacks by foreign governments against United States election infrastructure

Section 2501 directs the DHS Under Secretary for I&A to submit a report on cyberattacks and attempted cyberattacks by foreign governments on United States election infrastructure, in connection with the 2016 presidential election. Section 2501 further requires this report to include identification of the States and localities affected and include efforts to attack voter registration databases,

voting machines, voting-related computer networks, and the networks of Secretaries of State and other election officials.

Section 2502—Review of Intelligence Community's posture to collect against and analyze Russian efforts to influence the presidential election

Section 2502 requires the DNI to submit to the congressional intelligence committees, within one year of enactment of the Act, a report on the Director's review of the IC's posture to collect against and analyze Russian efforts to interfere with the 2016 United States presidential election. Section 2502 further requires the review to include assessments of IC resources, information sharing, and legal authorities.

Section 2503—Assessment of foreign intelligence threats to Federal elections

Section 2503 requires the DNI, in coordination with the Director of the CIA, Director of the NSA, Director of the FBI, Secretary of DHS, and heads of other relevant IC elements, to commence assessments of security vulnerabilities of State election systems one year before regularly scheduled Federal elections. Section 2503 further requires the DNI to submit a report on such assessments 180 days before regularly scheduled Federal elections, and an updated assessment 90 days before regularly scheduled Federal elections.

Section 2504—Strategy for countering Russian cyber threats to United States elections

Section 2504 requires the DNI, in coordination with the Secretary of DHS, Director of the FBI, Director of the CIA, Secretary of State, Secretary of Defense, and Secretary of the Treasury, to develop a whole-of-government strategy for countering Russian cyber threats against United States electoral systems and processes. Section 2504 further requires this strategy to include input from solicited Secretaries of State and chief election officials.

Section 2505—Assessment of significant Russian influence campaigns directed at foreign elections and referenda

Section 2505 requires the DNI to provide a report assessing past and ongoing Russian influence campaigns against foreign elections and referenda, to include a summary of the means by which such influence campaigns have been or are likely to be conducted, a summary of defenses against or responses to such Russian influence campaigns, a summary of IC activities to assist foreign governments against such campaigns, and an assessment of the effectiveness of such foreign defenses and responses.

Section 2506—Information sharing with state election officials

Section 2506 requires the DNI, within 30 days of enactment of the Act, to support security clearances for each eligible chief election official of a State, territory, or the District of Columbia (and additional eligible designees), up to the Top Secret level. Section 2506 also requires the DNI to assist with sharing appropriate classified information about threats to election systems.

Section 2507—Notification of significant foreign cyber intrusions and active measures campaigns directed at elections for federal offices

Section 2507 requires the Director of the FBI, and the Secretary of Homeland Security to brief the congressional intelligence committees, congressional leadership, the armed services committees, the appropriations committees, and the homeland security committees (consistent with sources and methods) not later than 14 days after a determination has been made with moderate or high confidence that a significant foreign cyber intrusion or active measures campaign intended to influence an upcoming election for any Federal office has taken place by a foreign state or foreign nonstate person, group, or other entity. The briefing shall provide a description of the significant foreign cyber intrusion or active measures campaign, including an identification of the foreign state or foreign nonstate person or group.

Section 2508—Designation of Counterintelligence Officer to lead election security matters

Section 2508 requires the DNI to designate a national counterintelligence officer within the National Counterintelligence and Security Center to lead, manage, and coordinate election security-related counterintelligence matters, including certain risks from foreign power interference.

TITLE XXVI—ELECTION MATTERS

Section 2601—Definitions

Section 2601 provides definitions for terminology used throughout this Title.

Section 2602—Reports and plans relating to security clearances and background investigations

Section 2602 requires the interagency Performance Accountability Council (Council) to provide plans to reduce the background investigation inventory and best align the investigation function between the Department of Defense and the National Background Investigation Bureau. Section 2602 further requires the Council to report on the future of the clearance process and requires the DNI to notify the appropriate committees upon determining requests to change clearance standards, and the status of those requests' disposition.

Section 2603—Improving the process for security clearances

Section 2603 requires the DNI to review the Questionnaire for National Security positions (SF–86) and the Federal Investigative Standards to determine potential unnecessary information required and assess whether revisions are necessary to account for insider threats. Section 2603 further requires the DNI, in coordination with the Council, to establish policies on interim clearances and consistency between the clearance process for contract and government personnel.

Section 2604—Goals for promptness of determinations regarding security clearances

Section 2604 requires the Council to implement a plan to be able to process 90 percent of clearance requests at the Secret level in thirty days, and at the Top Secret level in 90 days. The plan shall also address how to recognize reciprocity in accepting clearances among agencies within two weeks, and to require that ninety percent of clearance holders not be subject to a time-based periodic investigation.

Section 2605—Security Executive Agent

Section 2605 establishes the DNI as the government's Security Executive Agent, consistent with Executive Order 13467, and sets forth relevant authorities.

Section 2606—Report on unified, simplified, governmentwide standards for positions of trust and security clearances

Section 2606 directs the DNI and the Director of the Office of Personnel Management to report on the advisability and implications of consolidating the tiers for positions of trust and security clearances from five to three tiers.

Section 2607—Report on clearance in person concept

Section 2607 requires the DNI to submit a report on a concept whereby an individual can maintain eligibility for access to classified information for up to three years after access may lapse.

Section 2608—Reports on reciprocity for security clearances inside of departments and agencies

Section 2608 requires each federal agency to submit a report to the DNI that identifies the number of clearances that take more than two weeks to reciprocally recognize and set forth the reason for any delays. Section 2608 further requires the DNI to submit an annual report summarizing reciprocity.

Section 2609—Intelligence Community reports on security clearances

Section 2609 requires the DNI to submit a report on each IC element's security clearance metrics, segregated by Federal employees and contractor employees.

Section 2610—Periodic report on positions in the Intelligence Community that can be conducted without access to classified information, networks, or facilities

Section 2610 requires the DNI to submit to the congressional intelligence committees a report on positions that can be conducted without access to classified information, networks, or facilities, or may require only a Secret-level clearance.

Section 2611—Information sharing program for positions of trust and security clearances

Section 2611 requires the Security Executive Agent and the Suitability/Credentialing Executive Agent to establish a program to share information between and among government agencies and in-

dustry partners to inform decisions about positions of trust and security clearances.

Section 2612—Report on protections for confidentiality of whistleblower-related communications

Section 2612 requires the Security Executive Agent, in coordination with the Inspector General of the Intelligence Community, to submit a report detailing the IC's controls used to ensure continuous evaluation programs protect the confidentiality of whistleblower-related communications.

TITLE XXVII—REPORTS AND OTHER MATTERS

SUBTITLE A—MATTERS RELATING TO RUSSIA AND OTHER FOREIGN POWERS

Section 2701—Limitation relating to establishment or support of cybersecurity unit with the Russian Federation

Section 2701 prohibits the Federal government from expending any funds to establish or support a cybersecurity unit or other cyber agreement that is jointly established or otherwise implemented by the United States Government and the Russian Federation, unless the DNI submits a report to the appropriate congressional committees at least 30 days prior to any such agreement. The report shall include the agreement's purpose, intended shared intelligence, value to national security, counterintelligence concerns, and any measures taken to mitigate such concerns.

Section 2702—Report on returning Russian compounds

Section 2702 requires the IC to submit to the congressional intelligence committees, within 180 days of enactment of the Act, both classified and unclassified reports on the intelligence risks of returning the diplomatic compounds—in New York, Maryland, and California—taken from Russia as a reprisal for Russian meddling in the 2016 United States presidential election. Section 2702 also establishes an ongoing requirement for producing similar assessments for future assignment of diplomatic compounds within the United States.

Section 2703—Assessment of threat finance relating to Russia

Section 2703 requires the DNI, in coordination with the Assistant Secretary of the Treasury for Intelligence and Analysis, to submit to the congressional intelligence committees, within 60 days of enactment of the Act, an assessment of Russian threat finance, based on all-source intelligence from both the IC and the Office of Terrorism and Financial Intelligence of the Treasury Department. Section 2703 further requires the assessment to include global nodes and entry points for Russian money laundering; United States vulnerabilities; connections between Russian individuals involved in money laundering and the Russian Government; counterintelligence threats to the United States posed by Russian money laundering and other forms of threat finance; and challenges to United States Government efforts to enforce sanctions and combat organized crime.

Section 2704—Notification of an active measures campaign

Section 2704 requires the DNI to notify congressional leadership, and the Chairman and Vice Chairman or Ranking Member of the appropriate congressional committees, each time the DNI has determined there is credible information that a foreign power has attempted, is attempting, or will attempt to employ a covert influence or active measures campaign with regard to the modernization, employment, doctrine, or force posture of the nuclear deterrent or missile defense. Section 2704 further requires that such notification must include information on any actions that the United States has taken to expose or halt such attempts.

Section 2705—Notification of travel by accredited diplomatic and consular personnel of the Russian Federation in the United States

Section 2705 requires the Secretary of State to ensure that the Russian Federation provides notification at least two business days in advance of all travel that is subject to such requirements by accredited diplomatic and consular personnel of the Russian Federation in the United States, and take necessary action to secure full compliance by Russian personnel and address any noncompliance.

Section 2706—Report on outreach strategy addressing threats from United States adversaries to the United States technology sector

Section 2706 requires the DNI to submit a report to appropriate committees on the IC's and the Defense Intelligence Enterprise's outreach to United States non-government entities (including private businesses and academia), regarding the United States' adversaries' efforts to acquire critical United States infrastructure technology, intellectual property, and research and development information.

Section 2707—Report on Iranian support of proxy forces in Syria and Lebanon

Section 2707 requires the DNI to submit a report to appropriate congressional committees on Iranian support of proxy forces in Syria and Lebanon and the threat posed to Israel and other United States regional allies and interests.

Section 2708—Annual report on Iranian expenditures supporting foreign military and terrorist activates

Section 2708 requires the DNI to submit a report to Congress describing Iranian expenditures on military and terrorist activities outside the country.

Section 2709—Expansion of scope of Committee to Counter Active Measures and report on establishment of Foreign Malign Influence Center

Section 2709 amends a provision in the *Intelligence Authorization Act for Fiscal Year 2017* to expand the scope of the Committee to Counter Active Measures to add China, Iran, North Korea, and other nation states. Section 2709 further requires DNI, in coordination with relevant intelligence community elements, to submit to congressional intelligence committees a report on establishing a

center to assess and disseminate foreign influence activities, including the desirability and barriers to such establishment.

SUBTITLE B—REPORTS

Section 2711—Technical correction to Inspector General study

Section 2711 amends Title 50, section 11001(d), by replacing the IC IG's "audit" requirement for Inspectors General with employees having classified material access, with a "review" requirement.

Section 2712—Reports on authorities of the Chief Intelligence Officer of the Department of Homeland Security

Section 2712 requires the Secretary of DHS, in consultation with the Under Secretary for I&A, to submit to the congressional intelligence committees a report on the adequacy of the Under Secretary's authorities required as the Chief Intelligence Officer to organize the Homeland Security Intelligence Enterprise, and the legal and policy changes necessary to coordinate, organize, and lead DHS intelligence activities.

Section 2713—Review of Intelligence Community whistleblower matters

Section 2713 directs the Inspector General of the IC (IC IG), in consultations with the IGs of other IC agencies, to conduct a review of practices and procedures relating to IC whistleblower matters.

Section 2714—Report on role of Director of National Intelligence with respect to certain foreign investments

Section 2714 directs the DNI to submit a report on ODNI's role in preparing analytic materials in connection with the United States Government's evaluation of national security risks associated with potential foreign investments.

Section 2715—Report on surveillance by foreign governments against United States telecommunications networks

Section 2715 requires the DNI, in coordination with the Director of the CIA, Director of the NSA, Director of the FBI, and Secretary of DHS, to submit to the congressional intelligence, judiciary, and homeland security committees, within 180 days of enactment of the Act, a report on known attempts by foreign governments to exploit cybersecurity vulnerabilities in United States telecommunications networks to surveil United States persons, and any actions that the IC has taken to protect United States Government agencies and personnel from such surveillance.

Section 2716—Biennial report on foreign investment risks

Section 2716 requires the DNI to establish an IC working group on foreign investment risks and prepare a biennial report that includes an identification, analysis, and explanation of national security vulnerabilities, foreign investment trends, foreign countries' strategies to exploit vulnerabilities through the acquisition of either critical technologies (including components or items essential to national defense), critical materials (including physical materials essential to national security), or critical infrastructure (including physical or virtual systems and assets whose destruction or inca-

pacity would have a debilitating impact on national security), and market distortions caused by foreign countries. Technologies, materials, and infrastructure are deemed to be "critical" under this provision if their exploitation by a foreign government could cause severe harm to the national security of the United States.

Section 2717—Modification of certain reporting requirement on travel of foreign diplomats

Section 2717 amends a provision in the *Intelligence Authorization Act for Fiscal Year 2017,* to require reporting of "a best estimate" of known or suspected violations of certain travel requirements by accredited diplomatic and consular personnel of the Russian Federation.

Section 2718—Semiannual reports on investigations of unauthorized disclosures of classified information

Section 2718 requires the Assistant Attorney General for National Security at the Department of Justice, in consultation with the Director of the FBI, to submit to the congressional intelligence and judiciary committees a semiannual report on the status of IC referrals to the Department regarding unauthorized disclosures of classified information. Section 2718 also directs IC elements to submit to the congressional intelligence committees a semiannual report on the number of investigations opened and completed by each agency regarding an unauthorized public disclosure of classified information to the media, and the number of completed investigations referred to the Attorney General.

Section 2719—Congressional notification of designation of covered intellgience officer as persona non grata

Section 2719 requires, not later than 72 hours after a covered intelligence officer is designated as *persona non grata*, that the DNI, in consultation with the Secretary of State, submit to the designated committees a notification of that designation, to include the basis for the designation and justification for the expulsion.

Section 2720—Reports on Intelligence Community participation in vulnerabilities equities process of Federal government

Section 2720 requires the DNI to submit, within 90 days of enactment of the Act, to the congressional intelligence committees a report describing the Vulnerabilities Equities Process (VEP) roles and responsibilities for each IC element. Section 2720 further requires each IC element to report to the congressional intelligence committees within 30 days of a significant change to that respective IC element's VEP process and criteria. Section 2720 also requires the DNI to submit an annual report to the congressional intelligence committees with specified information on certain VEP metrics.

Section 2721—Inspectors General reports on classification

Section 2721 requires each designated IG to submit to the congressional intelligence committees a report on the accuracy in the application of classification and handling markings on a representative sample of finished products, to include those with compartments. Section 2721 also directs analyses of compliance with de-

classification procedures and a review of the effectiveness of processes for identifying topics of public or historical importance that merit prioritization for declassification review.

Section 2722—Reports on global water insecurity and national security implications and briefing on emerging infectious disease and pandemics

Section 2722 requires the DNI to submit to the congressional intelligence committees a report every five years on the implications of global water insecurity on the United States' national security interests. Section 2722 further requires the DNI to provide a briefing to appropriate congressional committees on the geopolitical effects of emerging infectious disease and pandemics, and their implications on the United States' national security.

Section 2722—Reports on global water insecurity and national security implications and briefing on emerging infectious disease and pandemics

Section 2722 requires the DNI to submit to the congressional intelligence committees a report every five years on the implications of global water insecurity on the United States' national security interests. Section 2722 further requires the DNI to provide a briefing to appropriate congressional committees on the geopolitical effects of emerging infectious disease and pandemics, and their implications on the United States' national security.

Section 2723—Annual report on memoranda of understanding between elements of intelligence community and other entities of the United States government regarding significant operational activities or policy

Section 2723 amends a provision in the Intelligence Authorization Act for Fiscal Year 2017, instead requiring each IC element to submit an annual report to the congressional intelligence committees that lists each significant memorandum of understanding or other agreement entered into during the preceding fiscal year. Section 2723 further requires each IC element to provide such documents if an intelligence committee so requests.

Section 2724—Study on the feasibility of encrypting unclassified wireline and wireless telephone calls

Section 2724 requires the DNI to complete a study and report on the feasibility of encrypting unclassified wireline and wireless telephone calls between personnel in the IC.

Section 2725—Modification of requirement for annual report on hiring and retention of minority employees

Section 2725 expands and clarifies current IC reporting requirements on diversity of IC personnel to include five prior fiscal years and to disaggregate data by IC element.

Section 2726—Reports on Intelligence Community loan repayment and related programs

Section 2726 requires the DNI, in cooperation with the heads of the elements of the IC, to submit to the congressional intelligence

committees a report on potentially establishing an IC-wide program for student loan repayment and forgiveness.

Section 2727—Repeal of certain reporting requirements

Section 2727 repeals certain intelligence community reporting requirements.

Section 2728—Inspector General of the Intelligence Community report on senior executives of the Office of the Director of National Intelligence

Section 2728 directs the Inspector General of the Intelligence Community to submit a report to the congressional intelligence committees regarding senior executive service staffing at the ODNI.

Section 2729—Briefing on Federal Bureau of Investigation offering permanent residence to sources and cooperators

Section 2729 directs the FBI within 30 days of enactment of this Act to provide a briefing to the congressional intelligence committees regarding the FBI's ability to provide permanent U.S. residence to foreign individuals who serve as cooperators in national security-related investigations.

Section 2730—Intelligence assessment of North Korea revenue sources

Section 2730 requires the DNI, in coordination with other relevant IC elements, to produce to the congressional intelligence committees an intelligence assessment of the North Korean regime's revenue sources.

Section 2731—Report on possible exploitation of virtual currencies by terrorist actors

Section 2731 requires the DNI, in consultation with the Secretary of Treasury, to submit to Congress a report on the possible exploitation of virtual currencies by terrorist actors.

SUBTITLE C—OTHER MATTERS

Section 2741—Public Interest Declassification Board

Section 2741 reauthorizes the Public Interest Declassification Board administered by the National Archives for a term of ten years, expiring on December 31, 2028.

Section 2742—Technical and clerical amendments to the National Security Act of 1947

Section 2742 makes certain edits to the National Security Act of 1947 as amended for technical or clerical purposes.

Section 2743—Technical amendments related to the Department of Energy

Section 2743 provides technical corrections to certain provisions regarding the Department of Energy's Office of Intelligence and Counterintelligence.

Section 2744—Sense of Congress on notifications of certain disclosures of classified information

Section 2744 expresses the sense of Congress that, pursuant to the requirement for the IC to keep the congressional intelligence committees fully and currently informed" in Section 502 of the National Security Act of 1947, IC agencies must submit prompt written notification after becoming aware that an individual in the executive branch has disclosed certain classified information outside established intelligence channels to foreign adversaries—North Korea, Iran, China, Russia, or Cuba.

Section 2745—Sense of Congress on consideration of espionage activities when considering whether or not to provide visas to foreign individuals to be accredited to a United Nations Mission in the United States

Section 2745 provides a Sense of Congress that, as to foreign individuals to be accredited to a United Nations mission, the Secretary of State should consider known and suspected intelligence and espionage activities, including activities constituting precursors to espionage, carried out by such individuals against the United States, or against foreign allies or partners of the United States. Section 2745 further provides that the Secretary of State should consider an individual's status as a known or suspected intelligence officer for a foreign adversary.

OVERSIGHT FINDINGS AND RECOMMENDATIONS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held multiple hearings on the classified budgetary issues raised by H.R. 3494. The bill, as reported by the Committee, reflects conclusions reached by the Committee in light of this oversight activity.

GENERAL PERFORMANCE GOALS AND OBJECTIVES

The goals and objectives of H.R. 3494 are to authorize the intelligence and intelligence-related activities of the United States Government for Fiscal Years 2018, 2019, and 2020. These activities enhance the national security of the United States, support and assist the armed forces of the United States, and support the President in the execution of the foreign policy of the United States.

The classified annex that accompanies this report reflects in great detail the Committee's specific performance goals and objectives at the programmatic level with respect to classified programs.

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandates Reform Act, P.L. 104–4) requires a statement of whether the provisions of the reported bill include unfunded mandates. In compliance with this requirement, the Committee has received a letter from the Congressional Budget Office included herein.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 11, 2019.

Hon. ADAM SCHIFF,
Chairman, Permanent Select Committee on Intelligence,
House of Representatives, Washington, DC 20515.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3494, the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is William Ma.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

At a Glance

H.R. 3494, Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020

As ordered reported by the House Permanent Select Committee on Intelligence on June 27, 2019

By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	*	*
Revenues	0	0	0
Deficit Effect	0	*	*
Spending Subject to Appropriation (Outlays)	0	5,938	n.e.

		Mandate Effects	
Statutory pay-as-you-go procedures apply?	Yes	Contains intergovernmental mandate?	No
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains private-sector mandate?	No

n.e. = not estimated; * = between -$500,000 and $500,000.

The bill would

- Modify the process for granting security clearances to federal employees and contractors
- Authorize the appropriation of $566 million for fiscal year 2020 for the Intelligence Community Management Account (ICMA)
- Make several changes to pay and benefits for civilian employees of the intelligence community
- Require the Director of National Intelligence to award prizes to encourage research on detecting forged or manipulated digital content and on developing fifth-generation wireless technology

Estimated budgetary effects would primarily stem from

- Establishing timeliness goals for completing initial secret and top secret clearances
- Authorizing amounts to be appropriated for the ICMA
- Enhancing benefits for employees of the intelligence community

Areas of significant uncertainty include

- Anticipating the manner in which the Administration would implement changes to the security clearance process
- Estimating the number of employees of the intelligence community who would benefit from the expansion of personnel benefits

Detailed estimate begins on the next page.

Bill summary: H.R. 3494 would authorize appropriations for fiscal years 2019 and 2020 for intelligence activities of the U.S. government, including the Intelligence Community Management Account and the Central Intelligence Agency Retirement and Disability System (CIARDS). The bill also would modify the security clearance process for federal agencies, expand personnel benefits for employees of the intelligence community, and create or modify other intelligence programs.

CBO does not provide estimates for classified programs; therefore, this estimate addresses only the unclassified aspects of the bill. In addition, CBO cannot provide estimates for certain provisions in the unclassified portion of the bill because they concern classified programs. On that limited basis, CBO estimates that implementing the unclassified provisions of the bill would cost about $5.9 billion over the 2020–2024 period; that spending would be subject to the appropriation of the specified and estimated amounts.

In addition, several provisions of the bill also would increase and decrease direct spending; therefore, pay-as-you-go procedures apply. On net, however, CBO estimates that those effects would be insignificant over the 2020–2029 period. Enacting the bill would not affect revenues.

CBO estimates that enacting H.R. 3494 would not significantly increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2030.

H.R. 3494 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

Estimated Federal cost: The estimated budgetary effect of H.R. 3494 is shown in Table 1. The costs of the legislation fall within all budget functions that fund security and suitability investigations.

TABLE 1—ESTIMATED BUDGETARY EFFECTS OF H.R. 3494, AS ORDERED REPORTED BY THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE ON JUNE 27, 2019

	By fiscal year, millions of dollars[a]—						
	2019	2020	2021	2022	2023	2024	2019–2024
SPENDING SUBJECT TO APPROPRIATION							
Security Clearances:							
Estimated Authorization Level	0	411	840	1,310	1,350	1,400	5,311
Estimated Outlays	0	361	800	1,260	1,350	1,400	5,171
Intelligence Community Management Account:							
Authorization Level	0	566	0	0	0	0	566
Estimated Outlays	0	368	158	20	8	3	557
Pay and Benefits:							
Estimated Authorization Level	0	1	23	47	49	51	171
Estimated Outlays	0	1	23	47	49	51	171
Task Forces and Other Advisory Bodies:							
Estimated Authorization Level	0	5	5	5	4	3	22
Estimated Outlays	0	5	5	5	4	3	22
Prize Competitions:							
Estimated Authorization Level	0	11	*	0	0	0	11
Estimated Outlays	0	1	10	0	0	0	11
Assessments, and Briefings:							
Estimated Authorization Level	0	5	*	*	*	*	6
Estimated Outlays	0	5	*	*	*	*	6
Totals:.							

TABLE 1—ESTIMATED BUDGETARY EFFECTS OF H.R. 3494, AS ORDERED REPORTED BY THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE ON JUNE 27, 2019—Continued

	By fiscal year, millions of dollars[a]—						
	2019	2020	2021	2022	2023	2024	2019–2024
Estimated Authorization Level	0	999	868	1,362	1,403	1,454	6,087
Estimated Outlays	0	741	996	1,332	1,411	1,457	5,938

Components may not sum to totals because of rounding; * = between -$500,000 and $500,000.

a. In addition to the budgetary effects shown above, enacting H.R. 3494 would affect direct spending by between -$500,000 and $500,000 over the 2020–2029 period.

Basis of estimate: For this estimate, CBO assumes that H.R. 3494 will be enacted near the beginning of fiscal year 2020. Outlays are based on historical spending patterns for existing or similar programs.

Spending subject to appropriation

CBO estimates that implementing the bill would cost about $5.9 billion over the 2020–2024 period. Such spending would be subject to appropriation of the estimated and specified amounts.

Security Clearances. Title XXVI of the bill would require the Security, Suitability, and Credentialing Performance Accountability Council (the Council) to achieve the following performance goals by December 31, 2021:[1]

- Issue 90 percent of initial determinations for secret and top secret clearances within 30 and 90 days, respectively;
- Accept 90 percent of security clearances for employees moving between federal agencies within two weeks if the clearances are equivalent; and
- Reinvestigate not more than 10 percent of all clearance holders at set intervals.

Title XXVI also would require the Council, the Director of National Intelligence, and other federal entities to develop plans, policies, and strategies, to perform reviews, and to prepare reports on different aspects of the security clearance process. In total, CBO estimates that implementing title XXVI would cost about $5.2 billion over the 2020–2024 period.

Timeliness. Current law sets a goal of completing 90 percent of security-clearance determinations within an average of 60 days from the date that the completed application is received. The Administration only applies that timeliness standard to initial determinations for secret clearances and has adopted other standards for top secret clearances and periodic reinvestigations. The current timeliness goals for the fastest 90 percent of security-clearance determinations are:

- An average of 60 days for initial secret clearances (40 days to complete the investigative phase and 20 days to complete the adjudicative phase),

[1] The Security, Suitability, and Credentialing Performance Accountability Council was established by Executive Order 13467, as amended, to oversee reform of the federal government's system for determining the eligibility of individuals to access classified information, hold sensitive positions (positions in which an individual could affect national security or trust in the federal government regardless of whether the individual has access to classified information), and gain physical or logical access to federal facilities or information systems.

• An average of 100 days for initial top secret clearances (80 days to complete the investigative phase and 20 days to complete the adjudicative phase), and

• An average of 180 days for periodic reinvestigations regardless of clearance level (150 days to complete the investigative phase and 30 days to complete the adjudicative phase).

Those goals, whether determined by statute or policy, however, currently are not being met. At the end of May 2019, the backlog of pending cases totaled 433,000. CBO estimates that the Administration will spend about $1.5 billion on all investigative services and another $0.1 billion on adjudicative services in 2019. With that backlog, and under those resource levels, the average time it took to complete the investigative and adjudicative phases for the fastest 90 percent of clearances at the end of May 2019 was:

• 169 days for initial secret clearances (139 days to complete the investigative phase and 30 days to complete the adjudicative phase).

• 338 days for initial top secret clearances (296 days to complete the investigative phase and 42 days to complete the adjudicative phase).

• 425 days for periodic reinvestigations (325 days to complete the investigative phase and 100 days to complete the adjudicative phase).

In order to meet the 30 and 90-day requirements of title XXVI, the National Background Investigations Bureau (NBIB) must first reduce the backlog to a level that would allow the federal government to meet the existing investigative and adjudicative processing goals. The bureau has been steadily expanding its workforce and reports that it expects to reduce the backlog to a manageable level in a couple of years. Concurrently, as NBIB works to reduce the backlog, the bureau's background-investigation program is being transferred to the Department of Defense (DoD).[2]

CBO expects that the current and upcoming initiatives will continue to reduce the backlog as planned and allow the current timeliness goals to be met by 2022. We also assume that the transfer of NBIB's responsibilities to DoD will be completed as planned.

The difference between the current timeliness goals and those prescribed by the bill is significant. The current structure establishes goals for an average processing time for the fastest 90 percent of cases. By contrast, the bill would establish maximum processing times for the fastest 90 percent of cases. Those targets would be significantly shorter than the current average processing times. Taking that into consideration, we estimate that the capacity to investigate and adjudicate initial secret and top secret clearances would need to increase by about 200 percent and 67 percent, respectively, to meet the faster processing requirements of title XXVI. For 2019, CBO estimates that the executive branch will spend about $0.4 billion and $0.6 billion on investigating and adjudicating initial secret clearances and initial top secret clearances, respectively. Thus, spending on those activities would ultimately

[2] Section 925 of Public Law 115–91, the National Defense Authorization Act for Fiscal Year 2018, authorized DoD to conduct security, suitability, and credentialing background investigations for DoD personnel. The Administration has since decided to transfer NBIB's investigation program to DoD. Executive Order 13869, signed April 24, 2019, makes the newly formed Defense Counterintelligence and Security Agency of DoD responsible for conducting background investigations for the federal government.

need to increase by about $1.2 billion annually. Under title XXVI, DoD would have three years to hire and train the necessary number of investigators and adjudicators to meet the prescribed timeliness goals in fiscal year 2022. Accounting for that implementation phase, CBO estimates that it would cost about $0.4 billion in 2020 and about $5.2 billion over the 2020–2024 period.

Administrative Costs. Title XXVI would require federal entities to develop policies, perform assessments, and prepare reports on several aspects of the security-clearance process. For entities in the intelligence community, CBO expects that the administrative costs of those requirements would be covered by the amounts authorized to be appropriated in the classified annex and for the ICMA. For federal entities that are not part of the intelligence community, CBO estimates total costs of $1 million over the 2020–2024 period.

Periodic Reinvestigations. Title XXVI would encourage the Council to limit reinvestigations conducted on the schedules set by the Administration to not more than 10 percent of all clearance holders. In 2017, about 4 million individuals held clearances, and this provision would require the federal government to use methods other than periodic reinvestigations on about 3.6 million of them to ensure that they remain eligible to access classified information. CBO expects that the method used to replace periodic reinvestigations would include, but not be limited to, the use of automated records checks.

Any costs or savings realized by using automated records checks as part of a larger effort to replace periodic investigations would depend on the frequency (e.g. daily, weekly, monthly, annually) with which they are conducted and the methods used to obtain information they cannot provide. Because CBO does not know how the Council would implement this provision, we cannot estimate its effects on spending.

While most agencies are funded by annual appropriations, some agencies are authorized to spend monies collected from other sources, such as user fees. In addition to the increases in spending subject to appropriation described above, any increase in costs to process security clearances and satisfy the requirements of this title incurred by those agencies would be considered direct spending. Those effects are described below in the "Direct Spending" section of this estimate.

Intelligence Community Management Account. Section 103 would authorize the appropriation of $566 million for fiscal year 2020 for the ICMA. The ICMA is the principal source of funding for the Office of the Director of National Intelligence and for coordinating the intelligence activities of the federal government. CBO estimates that implementing section 103 would cost about $557 million over the 2020–2024 period, subject to appropriation of the authorized amount.

Pay and Benefits. Sections 303 and 2303 would expand pay and benefits offered to employees of the intelligence community. In total, CBO estimates that implementing those provisions would cost $171 million over the 2020–2024 period.

Paid Parental Leave. Section 303 would provide 12 weeks of paid leave to employees of the intelligence community following the birth or adoption of a child or the initial placement of a foster child. Such leave would be available during the 12-month period

beginning on the date of the child's birth or placement. DNI would have 18 months from the date of enactment of the bill to implement the new leave program. Employees of the intelligence community would become entitled to paid leave for the birth or placement of a child that occurs on or after the date of such implementation.

Under current law, federal employees are entitled to up to 12 weeks of leave without pay after the birth or adoption of a child or the initial placement of a foster child. Employees may get paid during that 12-week period by using any annual or sick leave that they have accrued. The leave provided by this bill would be in addition to any leave available to, or taken by, those employees during the 12-week period provided by the Family and Medical Leave Act (FMLA). CBO expects that employees entitled to paid leave provided under H.R. 3494 would substitute that leave for annual or sick leave they otherwise would have taken during the 12-week FMLA leave period.

CBO estimates that implementing section 303 would cost $163 million over the 2020–2024 period. Because the exact number of employees in each element of the intelligence community is classified, CBO relied on publicly available information about the amounts appropriated to DoD and the intelligence community, as well as the number of people employed by DoD as the basis of this estimate.

In addition to the increases in spending subject to appropriation described above, enacting section 303 also would affect direct spending. Those effects are described below in the "Direct Spending" section of this estimate.

National Security Agency (NSA) Pay Authority. Section 2303 would authorize the NSA to establish higher pay rates for employees in cybersecurity fields at the agency. In general, the rates of pay established under that authority could not exceed the rate of basic pay for level II of the Executive Schedule ($192,300, in 2019); however, in certain circumstances, up to 100 NSA employees at any given time could receive up to the rate of basic pay for the Vice President of the United States ($246,900, in 2019).

On the basis of information from DoD, CBO estimates that about two to three dozen employees would receive an average of $15,800 more in compensation in fiscal year 2020 under section 2303. That estimate is based on CBO's expectation that the new pay rates would take effect six months following enactment (halfway into the fiscal year) to allow NSA time to develop and apply those higher rates of pay. After accounting for annual pay increases and the expectation that NSA would expand its use of this authority over time, CBO estimates that by 2024 the average increase in annual compensation would be about $35,100 and the number of NSA employees receiving such increases would double. Thus, CBO estimates that increasing pay for those NSA employees would cost $8 million over the 2020–2024 period.

Task Forces and Other Advisory Bodies. Several sections of the bill would require elements of the intelligence community to establish task forces and other oversight and advisory bodies; a handful of those would disband after a few years while others would operate permanently. CBO estimates that salaries for about two dozen full-time equivalents plus other support costs to establish and carry

out the responsibilities of those groups would total $5 million in 2020 and $22 million over the 2020–2024 period.

Prize Competitions. Sections 706 and 707 would authorize the Director of National Intelligence to organize two competitions to encourage research. In each of those competitions, the Director could award prizes totaling up to $5 million. The competition authorized by section 706 would be used to promote research and development of fifth-generation wireless technology. The competition authorized by section 707 would be used to promote research and development of technologies to detect forged or manipulated digital content.

CBO expects that it would take the Director one year to organize those competitions and to publicly announce, advertise, and publish the terms in advance of each competition. Those efforts would cost $1 million in 2020 and as competitions occurred, an additional $10 million in 2021, for a total of $11 million over the 2020–2024 period, CBO estimates.

Reports, Briefings, and Assessments. Division B of the bill would require several agencies to complete more than 60 reports, briefings, and assessments and to deliver those products and findings to the Congress. On the basis of the costs of similar activities, satisfying those requirements would cost $6 million over the 2020–2024 period, CBO estimates.

Direct spending

H.R. 3494 would extend workers' compensation benefits to certain private-sector employees, enhance the benefits offered to certain annuitants of the Central Intelligence Agency Retirement and Disability System, and authorize appropriations for 2019 and 2020. The bill also would affect spending by agencies not funded through annual appropriations. On net, and excluding provisions related to classified programs, CBO estimates that enacting H.R. 3494 would have an insignificant effect on direct spending over the 2020–2029 period.

Public-Private Talent Exchange. Section 306 would establish a program for temporarily exchanging employees of elements of the intelligence community and employees of entities in the private sector. That exchange would increase direct spending for compensation for private-sector employees who are injured in the course of their work in the intelligence community. Those related medical expenses would be paid through the federal workers' compensation program; such payments are classified as direct spending. CBO expects that few private-sector employees would become injured while participating in the program established by section 306; thus, the additional liability would increase direct spending by less than $500,000 over the 2020–2029 period.

CIARDS Benefits Adjustments. Section 2202 would make a number of changes to CIARDS to align the benefits offered to employees, retirees, or survivors under CIARDS with the benefits currently offered to employees, retirees, or survivors under the Civil Service Retirement System. Those changes would both increase and decrease spending on retirement benefits. For example, the bill would increase retirement benefits for employees who worked for the Central Intelligence Agency (CIA) before April 7, 1986, and at some point during their career, worked on a part-time basis. The

bill also would allow married employees retiring under CIARDS after enactment to provide a survivor annuity to someone with an insurable interest. (An insurable interest exists when an individual derives financial benefit from the retiring employee continuing to be alive.) Total annuity payments for retirees who elect to provide a survivor annuity to someone with an insurable interest would be reduced or increased depending on how long they and the designated beneficiary live. On the basis of information from the CIA, CBO estimates that only a small number of individuals would benefit from the changes in section 2202. On net, CBO estimates that the difference in direct spending from enacting the section would be less than $500,000 over the 2020–2029 period.

Security Clearances. Implementing any actions necessary to comply with the requirements of title XXVI and preparing the required reports would increase the administrative expenses for agencies not funded through annual appropriations. Such spending is considered direct spending. Because those agencies are able to increase the fees that provide their funding as necessary to cover their costs, CBO estimates that the net difference in spending by those agencies would be insignificant over the 2020–2029 period. (More information about the requirements of title XXVI of the bill is provided above under the heading, "Spending Subject to Appropriation.")

Paid Parental Leave. Section 303 would provide up to 12 weeks of paid leave to employees of the intelligence community following the birth or adoption of a child or the initial placement of a foster child. Once implemented, CBO estimates that section 303 would increase balances of sick leave for those employees who now would defer the use of some sick leave they otherwise would have taken for child care under current law. Any additional sick leave carried through to retirement would be used in the computation of those employees' or survivors' annuities; increases in annuity payments are classified as direct spending. Because the effect on the payment of future retirement annuities would be small, CBO estimates that enacting section 303 would increase direct spending by less than $500,000 over the 2020–2029 period. (More information about Paid Parental Leave is provided above under the heading, "Spending Subject to Appropriation.")

CIARDS Fund Payment. Sections 201 and 2201 would authorize the appropriation of $514 million for CIARDS for fiscal years 2020 and 2019, respectively, to maintain the necessary funding level for operating that retirement and disability system. Appropriations to CIARDS are treated as direct spending in the budget and are projected to continue at the authorized levels in CBO's baseline pursuant to section 257 of the Balanced Budget and Emergency Deficit Control Act of 1985. Because the amount that would be authorized by the bill is included in CBO's baseline, that authorization would have no budgetary effect relative to the baseline.

Uncertainty

The most significant area of uncertainty arises from estimating the costs of changing the process for granting security clearances. The bill would give the Council broad latitude in reforming that process; thus, the steps taken by the Council to meet the processing goals of security clearance investigations and other matters could differ significantly from CBO's estimate.

Additionally, the actual number of personnel employed by the intelligence community is classified. The costs of additional personnel benefits are also uncertain because the number of personnel that would receive those benefits could differ significantly from CBO's estimate.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. Pay-as-you-go procedures apply to this legislation because enacting it would affect direct spending; however, CBO estimates that those effects would be insignificant.

Increase in long-term deficits: CBO estimates that enacting H.R. 3494 would not increase on-budget deficits by more than $5 billion in any of the four consecutive 10-year periods beginning in 2030.

Mandates: None.

Estimate prepared by: Federal Costs: William Ma, Dan Ready (federal pay), and Meredith Decker (workers' compensation); Mandates: Brandon Lever.

Estimate reviewed by: David Newman, Chief, Defense, International Affairs, and Veterans' Affairs Cost Estimates Unit; Susan Willie, Chief, Mandates Unit; Leo Lex, Deputy Assistant Director for Budget Analysis; Theresa Gullo, Assistant Director for Budget.

STATEMENT ON CONGRESSIONAL EARMARKS

Pursuant to clause 9 of rule XXI of the Rules of the House of Representatives, the Committee states that the bill as reported contains no congressional earmarks, limited tax benefits, or limited tariff benefits.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

NATIONAL SECURITY ACT OF 1947

SHORT TITLE

That this Act may be cited as the "National Security Act of 1947".

TABLE OF CONTENTS

* * * * * * *

Sec. 3. Definitions.

TITLE I—COORDINATION FOR NATIONAL SECURITY

* * * * * * *

[Sec. 107. National Security Resources Board.]

* * * * * * *

[Sec. 113B. Special pay authority for science, technology, engineering, or math positions.]

TITLE I—COORDINATION FOR NATIONAL SECURITY

* * * * * * *

JOINT INTELLIGENCE COMMUNITY COUNCIL

SEC. 101A. (a) JOINT INTELLIGENCE COMMUNITY COUNCIL.—There is a Joint Intelligence Community Council.

(b) MEMBERSHIP.—The Joint Intelligence Community Council shall consist of the following:

(1) The Director of National Intelligence, who shall chair the Council.

(2) The Secretary of State.

(3) The Secretary of the Treasury.

(4) The Secretary of Defense.

(5) The Attorney General.

(6) The Secretary of Energy.

(7) The Secretary of Homeland Security.

(8) Such other officers of the United States Government as the President may designate from time to time.

(c) FUNCTIONS.—The Joint Intelligence Community Council shall assist the Director of National Intelligence in developing and implementing a joint, unified national intelligence effort to protect national security by—

(1) advising the Director on establishing requirements, developing budgets, financial management, and monitoring and evaluating the performance of the intelligence community, and on such other matters as the Director may request; and

(2) ensuring the timely execution of programs, policies, and directives established or developed by the Director.

(d) MEETINGS.—The Director of National Intelligence shall convene [regular] meetings of the Joint Intelligence Community Council *as the Director considers appropriate*.

(e) ADVICE AND OPINIONS OF MEMBERS OTHER THAN CHAIRMAN.—(1) A member of the Joint Intelligence Community Council (other than the Chairman) may submit to the Chairman advice or an opinion in disagreement with, or advice or an opinion in addition to, the advice presented by the Director of National Intelligence to the President or the National Security Council, in the role of the Chairman as Chairman of the Joint Intelligence Community Council. If a member submits such advice or opinion, the Chairman shall present the advice or opinion of such member at the same time the Chairman presents the advice of the Chairman to the President or the National Security Council, as the case may be.

(2) The Chairman shall establish procedures to ensure that the presentation of the advice of the Chairman to the President or the National Security Council is not unduly delayed by reason of the submission of the individual advice or opinion of another member of the Council.

(f) RECOMMENDATIONS TO CONGRESS.—Any member of the Joint Intelligence Community Council may make such recommendations to Congress relating to the intelligence community as such member considers appropriate.

* * * * * * *

RESPONSIBILITIES AND AUTHORITIES OF THE DIRECTOR OF NATIONAL INTELLIGENCE

SEC. 102A. (a) PROVISION OF INTELLIGENCE.—(1) The Director of National Intelligence shall be responsible for ensuring that national intelligence is provided—

(A) to the President;

(B) to the heads of departments and agencies of the executive branch;

(C) to the Chairman of the Joint Chiefs of Staff and senior military commanders;

(D) to the Senate and House of Representatives and the committees thereof; and

(E) to such other persons as the Director of National Intelligence determines to be appropriate.

(2) Such national intelligence should be timely, objective, independent of political considerations, and based upon all sources available to the intelligence community and other appropriate entities.

(b) ACCESS TO INTELLIGENCE.—Unless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any Federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence.

(c) BUDGET AUTHORITIES.—(1) With respect to budget requests and appropriations for the National Intelligence Program, the Director of National Intelligence shall—

(A) based on intelligence priorities set by the President, provide to the heads of departments containing agencies or organizations within the intelligence community, and to the heads of such agencies and organizations, guidance for developing the National Intelligence Program budget pertaining to such agencies and organizations;

(B) based on budget proposals provided to the Director of National Intelligence by the heads of agencies and organizations within the intelligence community and the heads of their respective departments and, as appropriate, after obtaining the advice of the Joint Intelligence Community Council, develop and determine an annual consolidated National Intelligence Program budget; and

(C) present such consolidated National Intelligence Program budget, together with any comments from the heads of departments containing agencies or organizations within the intelligence community, to the President for approval.

(2) In addition to the information provided under paragraph (1)(B), the heads of agencies and organizations within the intelligence community shall provide the Director of National Intelligence such other information as the Director shall request for the purpose of determining the annual consolidated National Intelligence Program budget under that paragraph.

(3)(A) The Director of National Intelligence shall participate in the development by the Secretary of Defense of the annual budget for the Military Intelligence Program or any successor program or programs.

(B) The Director of National Intelligence shall provide guidance for the development of the annual budget for each element of the intelligence community that is not within the National Intelligence Program.

(4) The Director of National Intelligence shall ensure the effective execution of the annual budget for intelligence and intelligence-related activities.

(5)(A) The Director of National Intelligence shall be responsible for managing appropriations for the National Intelligence Program by directing the allotment or allocation of such appropriations through the heads of the departments containing agencies or organizations within the intelligence community and the Director of the Central Intelligence Agency, with prior notice (including the provision of appropriate supporting information) to the head of the department containing an agency or organization receiving any such allocation or allotment or the Director of the Central Intelligence Agency.

(B) Notwithstanding any other provision of law, pursuant to relevant appropriations Acts for the National Intelligence Program, the Director of the Office of Management and Budget shall exercise the authority of the Director of the Office of Management and Budget to apportion funds, at the exclusive direction of the Director of National Intelligence, for allocation to the elements of the intelligence community through the relevant host executive departments and the Central Intelligence Agency. Department comptrollers or appropriate budget execution officers shall allot, allocate, reprogram, or transfer funds appropriated for the National Intelligence Program in an expeditious manner.

(C) The Director of National Intelligence shall monitor the implementation and execution of the National Intelligence Program by the heads of the elements of the intelligence community that manage programs and activities that are part of the National Intelligence Program, which may include audits and evaluations.

(6) Apportionment and allotment of funds under this subsection shall be subject to chapter 13 and section 1517 of title 31, United States Code, and the Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. 621 et seq.).

(7)(A) The Director of National Intelligence shall provide a semiannual report, beginning April 1, 2005, and ending April 1, 2007, to the President and the Congress regarding implementation of this section.

(B) The Director of National Intelligence shall report to the President and the Congress not later than 15 days after learning of any instance in which a departmental comptroller acts in a manner inconsistent with the law (including permanent statutes, authorization Acts, and appropriations Acts), or the direction of the Director of National Intelligence, in carrying out the National Intelligence Program.

(d) ROLE OF DIRECTOR OF NATIONAL INTELLIGENCE IN TRANSFER AND REPROGRAMMING OF FUNDS.—(1)(A) No funds made available under the National Intelligence Program may be transferred or reprogrammed without the prior approval of the Director of National Intelligence, except in accordance with procedures prescribed by the Director of National Intelligence.

(B) The Secretary of Defense shall consult with the Director of National Intelligence before transferring or reprogramming funds made available under the Military Intelligence Program or any successor program or programs.

(2) Subject to the succeeding provisions of this subsection, the Director of National Intelligence may transfer or reprogram funds appropriated for a program within the National Intelligence Program—

(A) to another such program;

(B) to other departments or agencies of the United States Government for the development and fielding of systems of common concern related to the collection, processing, analysis, exploitation, and dissemination of intelligence information; or

(C) to a program funded by appropriations not within the National Intelligence Program to address critical gaps in intelligence information sharing or access capabilities.

(3) The Director of National Intelligence may only transfer or reprogram funds referred to in paragraph (1)(A)—

(A) with the approval of the Director of the Office of Management and Budget; and

(B) after consultation with the heads of departments containing agencies or organizations within the intelligence community to the extent such agencies or organizations are affected, and, in the case of the Central Intelligence Agency, after consultation with the Director of the Central Intelligence Agency.

(4) The amounts available for transfer or reprogramming in the National Intelligence Program in any given fiscal year, and the terms and conditions governing such transfers and reprogrammings, are subject to the provisions of annual appropriations Acts and this subsection.

(5)(A) A transfer or reprogramming of funds may be made under this subsection only if—

(i) the funds are being transferred to an activity that is a higher priority intelligence activity;

(ii) the transfer or reprogramming supports an emergent need, improves program effectiveness, or increases efficiency;

(iii) the transfer or reprogramming does not involve a transfer or reprogramming of funds to a Reserve for Contingencies of the Director of National Intelligence or the Reserve for Contingencies of the Central Intelligence Agency;

(iv) the transfer or reprogramming results in a cumulative transfer or reprogramming of funds out of any department or agency, as appropriate, funded in the National Intelligence Program in a single fiscal year—

(I) that is less than $150,000,000, and

(II) that is less than 5 percent of amounts available to a department or agency under the National Intelligence Program; and

(v) the transfer or reprogramming does not terminate an acquisition program.

(B) A transfer or reprogramming may be made without regard to a limitation set forth in clause (iv) or (v) of subparagraph (A) if the transfer has the concurrence of the head of the department involved or the Director of the Central Intelligence Agency (in the case of the Central Intelligence Agency). The authority to provide such concurrence may only be delegated by the head of the department involved or the Director of the Central Intelligence Agency (in the case of the Central Intelligence Agency) to the deputy of such officer.

(6) Funds transferred or reprogrammed under this subsection shall remain available for the same period as the appropriations account to which transferred or reprogrammed.

(7) Any transfer or reprogramming of funds under this subsection shall be carried out in accordance with existing procedures applicable to reprogramming notifications for the appropriate congressional committees. Any proposed transfer or reprogramming for which notice is given to the appropriate congressional committees shall be accompanied by a report explaining the nature of the proposed transfer or reprogramming and how it satisfies the requirements of this subsection. In addition, the congressional intelligence committees shall be promptly notified of any transfer or reprogramming of funds made pursuant to this subsection in any case in which the transfer or reprogramming would not have otherwise required reprogramming notification under procedures in effect as of the date of the enactment of this subsection.

(e) TRANSFER OF PERSONNEL.—(1)(A) In addition to any other authorities available under law for such purposes, in the first twelve months after establishment of a new national intelligence center, the Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in consultation with the congressional committees of jurisdiction referred to in subparagraph (B), may transfer not more than 100 personnel authorized for elements of the intelligence community to such center.

(B) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

(i) the congressional intelligence committees;

(ii) the Committees on Appropriations of the Senate and the House of Representatives;

(iii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and

(iv) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

(C) The Director shall include in any notice under subparagraph (B) an explanation of the nature of the transfer and how it satisfies the requirements of this subsection.

(2)(A) The Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in accordance with procedures to be developed by the Director of National Intelligence and the heads of the departments and agencies concerned, may transfer personnel authorized for an element of the intelligence community to another such element for a period of not more than 2 years.

(B) A transfer of personnel may be made under this paragraph only if—

(i) the personnel are being transferred to an activity that is a higher priority intelligence activity; and

(ii) the transfer supports an emergent need, improves program effectiveness, or increases efficiency.

(C) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

(i) the congressional intelligence committees;

(ii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and

(iii) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

(D) The Director shall include in any notice under subparagraph (C) an explanation of the nature of the transfer and how it satisfies the requirements of this paragraph.

(3)(A) In addition to the number of full-time equivalent positions authorized for the Office of the Director of National Intelligence for a fiscal year, there is authorized for such Office for each fiscal year an additional 100 full-time equivalent positions that may be used only for the purposes described in subparagraph (B).

(B) Except as provided in subparagraph (C), the Director of National Intelligence may use a full-time equivalent position authorized under subparagraph (A) only for the purpose of providing a temporary transfer of personnel made in accordance with paragraph (2) to an element of the intelligence community to enable such element to increase the total number of personnel authorized for such element, on a temporary basis—

(i) during a period in which a permanent employee of such element is absent to participate in critical language training; or

(ii) to accept a permanent employee of another element of the intelligence community to provide language-capable services.

(C) Paragraph (2)(B) shall not apply with respect to a transfer of personnel made under subparagraph (B).

(D) For each of the fiscal years 2010, 2011, and 2012, the Director of National Intelligence shall submit to the congressional intelligence committees an annual report on the use of authorities under this paragraph. Each such report shall include a description of—

(i) the number of transfers of personnel made by the Director pursuant to subparagraph (B), disaggregated by each element of the intelligence community;

(ii) the critical language needs that were fulfilled or partially fulfilled through the use of such transfers; and

(iii) the cost to carry out subparagraph (B).

(4) It is the sense of Congress that—

(A) the nature of the national security threats facing the United States will continue to challenge the intelligence community to respond rapidly and flexibly to bring analytic resources to bear against emerging and unforeseen requirements;

(B) both the Office of the Director of National Intelligence and any analytic centers determined to be necessary should be fully and properly supported with appropriate levels of personnel resources and that the President's yearly budget requests adequately support those needs; and

(C) the President should utilize all legal and administrative discretion to ensure that the Director of National Intelligence and all other elements of the intelligence community have the necessary resources and procedures to respond promptly and

effectively to emerging and unforeseen national security challenges.

(f) TASKING AND OTHER AUTHORITIES.—(1)(A) The Director of National Intelligence shall—

(i) establish objectives, priorities, and guidance for the intelligence community to ensure timely and effective collection, processing, analysis, and dissemination (including access by users to collected data consistent with applicable law and, as appropriate, the guidelines referred to in subsection (b) and analytic products generated by or within the intelligence community) of national intelligence;

(ii) determine requirements and priorities for, and manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community, including—

(I) approving requirements (including those requirements responding to needs provided by consumers) for collection and analysis; and

(II) resolving conflicts in collection requirements and in the tasking of national collection assets of the elements of the intelligence community; and

(iii) provide advisory tasking to intelligence elements of those agencies and departments not within the National Intelligence Program.

(B) The authority of the Director of National Intelligence under subparagraph (A) shall not apply—

(i) insofar as the President so directs;

(ii) with respect to clause (ii) of subparagraph (A), insofar as the Secretary of Defense exercises tasking authority under plans or arrangements agreed upon by the Secretary of Defense and the Director of National Intelligence; or

(iii) to the direct dissemination of information to State government and local government officials and private sector entities pursuant to sections 201 and 892 of the Homeland Security Act of 2002 (6 U.S.C. 121, 482).

(2) The Director of National Intelligence shall oversee the National Counterterrorism Center, the National Counterproliferation Center, and the National Counterintelligence and Security Center and may establish such other national intelligence centers as the Director determines necessary.

(3)(A) The Director of National Intelligence shall prescribe, in consultation with the heads of other agencies or elements of the intelligence community, and the heads of their respective departments, personnel policies and programs applicable to the intelligence community that—

(i) encourage and facilitate assignments and details of personnel to national intelligence centers, and between elements of the intelligence community;

(ii) set standards for education, training, and career development of personnel of the intelligence community;

(iii) encourage and facilitate the recruitment and retention by the intelligence community of highly qualified individuals for the effective conduct of intelligence activities;

(iv) ensure that the personnel of the intelligence community are sufficiently diverse for purposes of the collection and anal-

ysis of intelligence through the recruitment and training of women, minorities, and individuals with diverse ethnic, cultural, and linguistic backgrounds;

(v) make service in more than one element of the intelligence community a condition of promotion to such positions within the intelligence community as the Director shall specify; and

(vi) ensure the effective management of intelligence community personnel who are responsible for intelligence community-wide matters.

(B) Policies prescribed under subparagraph (A) shall not be inconsistent with the personnel policies otherwise applicable to members of the uniformed services.

(4) The Director of National Intelligence shall ensure compliance with the Constitution and laws of the United States by the Central Intelligence Agency and shall ensure such compliance by other elements of the intelligence community through the host executive departments that manage the programs and activities that are part of the National Intelligence Program.

(5) The Director of National Intelligence shall ensure the elimination of waste and unnecessary duplication within the intelligence community.

(6) The Director of National Intelligence shall establish requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for national intelligence purposes, except that the Director shall have no authority to direct or undertake electronic surveillance or physical search operations pursuant to that Act unless authorized by statute or Executive order.

(7)(A) The Director of National Intelligence shall, if the Director determines it is necessary, or may, if requested by a congressional intelligence committee, conduct an accountability review of an element of the intelligence community or the personnel of such element in relation to a failure or deficiency within the intelligence community.

(B) The Director of National Intelligence, in consultation with the Attorney General, shall establish guidelines and procedures for conducting an accountability review under subparagraph (A).

(C)(i) The Director of National Intelligence shall provide the findings of an accountability review conducted under subparagraph (A) and the Director's recommendations for corrective or punitive action, if any, to the head of the applicable element of the intelligence community. Such recommendations may include a recommendation for dismissal of personnel.

(ii) If the head of such element does not implement a recommendation made by the Director under clause (i), the head of such element shall submit to the congressional intelligence committees a notice of the determination not to implement the recommendation, including the reasons for the determination.

(D) The requirements of this paragraph shall not be construed to limit any authority of the Director of National Intelligence under subsection (m) or with respect to supervision of the Central Intelligence Agency.

(8) The Director of National Intelligence shall perform such other functions as the President may direct.

(9) Nothing in this title shall be construed as affecting the role of the Department of Justice or the Attorney General under the Foreign Intelligence Surveillance Act of 1978.

(g) INTELLIGENCE INFORMATION SHARING.—(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

(A) establish uniform security standards and procedures;

(B) establish common information technology standards, protocols, and interfaces;

(C) ensure development of information technology systems that include multi-level security and intelligence integration capabilities;

(D) establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;

(E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture;

(F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program; and

(G) in accordance with Executive Order No. 13526 (75 Fed. Reg. 707; relating to classified national security information) (or any subsequent corresponding executive order), and part 2001 of title 32, Code of Federal Regulations (or any subsequent corresponding regulation), establish—

(i) guidance to standardize, in appropriate cases, the formats for classified and unclassified intelligence products created by elements of the intelligence community for purposes of promoting the sharing of intelligence products; and

(ii) policies and procedures requiring the increased use, in appropriate cases, and including portion markings, of the classification of portions of information within one intelligence product.

(2) The President shall ensure that the Director of National Intelligence has all necessary support and authorities to fully and effectively implement paragraph (1).

(3) Except as otherwise directed by the President or with the specific written agreement of the head of the department or agency in question, a Federal agency or official shall not be considered to have met any obligation to provide any information, report, assessment, or other material (including unevaluated intelligence information) to that department or agency solely by virtue of having provided that information, report, assessment, or other material to the Director of National Intelligence or the National Counterterrorism Center.

(4) The Director of National Intelligence shall, in a timely manner, report to Congress any statute, regulation, policy, or practice that the Director believes impedes the ability of the Director to fully and effectively ensure maximum availability of access to intel-

ligence information within the intelligence community consistent with the protection of the national security of the United States.

(h) ANALYSIS.—To ensure the most accurate analysis of intelligence is derived from all sources to support national security needs, the Director of National Intelligence shall—

(1) implement policies and procedures—

(A) to encourage sound analytic methods and tradecraft throughout the elements of the intelligence community;

(B) to ensure that analysis is based upon all sources available; and

(C) to ensure that the elements of the intelligence community regularly conduct competitive analysis of analytic products, whether such products are produced by or disseminated to such elements;

(2) ensure that resource allocation for intelligence analysis is appropriately proportional to resource allocation for intelligence collection systems and operations in order to maximize analysis of all collected data;

(3) ensure that differences in analytic judgment are fully considered and brought to the attention of policymakers; and

(4) ensure that sufficient relationships are established between intelligence collectors and analysts to facilitate greater understanding of the needs of analysts.

(i) PROTECTION OF INTELLIGENCE SOURCES AND METHODS.—(1) The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.

(2) Consistent with paragraph (1), in order to maximize the dissemination of intelligence, the Director of National Intelligence shall establish and implement guidelines for the intelligence community for the following purposes:

(A) Classification of information under applicable law, Executive orders, or other Presidential directives.

(B) Access to and dissemination of intelligence, both in final form and in the form when initially gathered.

(C) Preparation of intelligence products in such a way that source information is removed to allow for dissemination at the lowest level of classification possible or in unclassified form to the extent practicable.

(3) The Director may only delegate a duty or authority given the Director under this subsection to the Principal Deputy Director of National Intelligence.

(j) UNIFORM PROCEDURES FOR CLASSIFIED INFORMATION.—The Director of National Intelligence, subject to the direction of the President, shall—

(1) establish uniform standards and procedures for the grant of access to sensitive compartmented information to any officer or employee of any agency or department of the United States and to employees of contractors of those agencies or departments;

(2) ensure the consistent implementation of those standards and procedures throughout such agencies and departments;

(3) ensure that security clearances granted by individual elements of the intelligence community are recognized by all elements of the intelligence community, and under contracts entered into by those agencies;

(4) ensure that the process for investigation and adjudication of an application for access to sensitive compartmented infor-

mation is performed in the most expeditious manner possible consistent with applicable standards for national security;

(5) ensure that the background of each employee or officer of an element of the intelligence community, each contractor to an element of the intelligence community, and each individual employee of such a contractor who has been determined to be eligible for access to classified information is monitored on a continual basis under standards developed by the Director, including with respect to the frequency of evaluation, during the period of eligibility of such employee or officer of an element of the intelligence community, such contractor, or such individual employee to such a contractor to determine whether such employee or officer of an element of the intelligence community, such contractor, and such individual employee of such a contractor continues to meet the requirements for eligibility for access to classified information; and

(6) develop procedures to require information sharing between elements of the intelligence community concerning potentially derogatory security information regarding an employee or officer of an element of the intelligence community, a contractor to an element of the intelligence community, or an individual employee of such a contractor that may impact the eligibility of such employee or officer of an element of the intelligence community, such contractor, or such individual employee of such a contractor for a security clearance.

(k) COORDINATION WITH FOREIGN GOVERNMENTS.—Under the direction of the President and in a manner consistent with section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), the Director of National Intelligence shall oversee the coordination of the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

(l) ENHANCED PERSONNEL MANAGEMENT.—(1)(A) The Director of National Intelligence shall, under regulations prescribed by the Director, provide incentives for personnel of elements of the intelligence community to serve—

(i) on the staff of the Director of National Intelligence;

(ii) on the staff of the national intelligence centers;

(iii) on the staff of the National Counterterrorism Center; and

(iv) in other positions in support of the intelligence community management functions of the Director.

(B) Incentives under subparagraph (A) may include financial incentives, bonuses, and such other awards and incentives as the Director considers appropriate.

(2)(A) Notwithstanding any other provision of law, the personnel of an element of the intelligence community who are assigned or detailed under paragraph (1)(A) to service under the Director of National Intelligence shall be promoted at rates equivalent to or better than personnel of such element who are not so assigned or detailed.

(B) The Director may prescribe regulations to carry out this paragraph.

(3)(A) The Director of National Intelligence shall prescribe mechanisms to facilitate the rotation of personnel of the intelligence community through various elements of the intelligence community in the course of their careers in order to facilitate the widest possible understanding by such personnel of the variety of intelligence requirements, methods, users, and capabilities.

(B) The mechanisms prescribed under subparagraph (A) may include the following:

(i) The establishment of special occupational categories involving service, over the course of a career, in more than one element of the intelligence community.

(ii) The provision of rewards for service in positions undertaking analysis and planning of operations involving two or more elements of the intelligence community.

(iii) The establishment of requirements for education, training, service, and evaluation for service involving more than one element of the intelligence community.

(C) It is the sense of Congress that the mechanisms prescribed under this subsection should, to the extent practical, seek to duplicate for civilian personnel within the intelligence community the joint officer management policies established by chapter 38 of title 10, United States Code, and the other amendments made by title IV of the Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99–433).

(D) The mechanisms prescribed under subparagraph (A) and any other policies of the Director—

(i) may not require an employee of an office of inspector general for an element of the intelligence community, including the Office of the Inspector General of the Intelligence Community, to rotate to a position in an office or organization of such an element over which such office of inspector general exercises jurisdiction; and

(ii) shall be implemented in a manner that exempts employees of an office of inspector general from a rotation that may impact the independence of such office.

(4)(A) Except as provided in subparagraph (B) and subparagraph (D), this subsection shall not apply with respect to personnel of the elements of the intelligence community who are members of the uniformed services.

(B) Mechanisms that establish requirements for education and training pursuant to paragraph (3)(B)(iii) may apply with respect to members of the uniformed services who are assigned to an element of the intelligence community funded through the National Intelligence Program, but such mechanisms shall not be inconsistent with personnel policies and education and training requirements otherwise applicable to members of the uniformed services.

(C) The personnel policies and programs developed and implemented under this subsection with respect to law enforcement officers (as that term is defined in section 5541(3) of title 5, United States Code) shall not affect the ability of law enforcement entities to conduct operations or, through the applicable chain of command, to control the activities of such law enforcement officers.

(D) Assignment to the Office of the Director of National Intelligence of commissioned officers of the Armed Forces shall be considered a joint-duty assignment for purposes of the joint officer

management policies prescribed by chapter 38 of title 10, United States Code, and other provisions of that title.

(m) ADDITIONAL AUTHORITY WITH RESPECT TO PERSONNEL.—(1) In addition to the authorities under subsection (f)(3), the Director of National Intelligence may exercise with respect to the personnel of the Office of the Director of National Intelligence any authority of the Director of the Central Intelligence Agency with respect to the personnel of the Central Intelligence Agency under the Central Intelligence Agency Act of 1949 (50 U.S.C. 403a et seq.), and other applicable provisions of law, as of the date of the enactment of this subsection to the same extent, and subject to the same conditions and limitations, that the Director of the Central Intelligence Agency may exercise such authority with respect to personnel of the Central Intelligence Agency.

(2) Employees and applicants for employment of the Office of the Director of National Intelligence shall have the same rights and protections under the Office of the Director of National Intelligence as employees of the Central Intelligence Agency have under the Central Intelligence Agency Act of 1949, and other applicable provisions of law, as of the date of the enactment of this subsection.

(n) ACQUISITION AND OTHER AUTHORITIES.—(1) In carrying out the responsibilities and authorities under this section, the Director of National Intelligence may exercise the acquisition and appropriations authorities referred to in the Central Intelligence Agency Act of 1949 (50 U.S.C. 403a et seq.) other than the authorities referred to in section 8(b) of that Act (50 U.S.C. 403j(b)).

(2) For the purpose of the exercise of any authority referred to in paragraph (1), a reference to the head of an agency shall be deemed to be a reference to the Director of National Intelligence or the Principal Deputy Director of National Intelligence.

(3)(A) Any determination or decision to be made under an authority referred to in paragraph (1) by the head of an agency may be made with respect to individual purchases and contracts or with respect to classes of purchases or contracts, and shall be final.

(B) Except as provided in subparagraph (C), the Director of National Intelligence or the Principal Deputy Director of National Intelligence may, in such official's discretion, delegate to any officer or other official of the Office of the Director of National Intelligence any authority to make a determination or decision as the head of the agency under an authority referred to in paragraph (1).

(C) The limitations and conditions set forth in section 3(d) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403c(d)) shall apply to the exercise by the Director of National Intelligence of an authority referred to in paragraph (1).

(D) Each determination or decision required by an authority referred to in the second sentence of section 3(d) of the Central Intelligence Agency Act of 1949 shall be based upon written findings made by the official making such determination or decision, which findings shall be final and shall be available within the Office of the Director of National Intelligence for a period of at least six years following the date of such determination or decision.

(4)(A) In addition to the authority referred to in paragraph (1), the Director of National Intelligence may authorize the head of an element of the intelligence community to exercise an acquisition authority referred to in section 3 or 8(a) of the Central Intelligence

Agency Act of 1949 (50 U.S.C. 403c and 403j(a)) for an acquisition by such element that is more than 50 percent funded under the National Intelligence Program.

(B) The head of an element of the intelligence community may not exercise an authority referred to in subparagraph (A) until—

(i) the head of such element (without delegation) submits to the Director of National Intelligence a written request that includes—

(I) a description of such authority requested to be exercised;

(II) an explanation of the need for such authority, including an explanation of the reasons that other authorities are insufficient; and

(III) a certification that the mission of such element would be—

(aa) impaired if such authority is not exercised; or

(bb) significantly and measurably enhanced if such authority is exercised; and

(ii) the Director of National Intelligence issues a written authorization that includes—

(I) a description of the authority referred to in subparagraph (A) that is authorized to be exercised; and

(II) a justification to support the exercise of such authority.

(C) A request and authorization to exercise an authority referred to in subparagraph (A) may be made with respect to an individual acquisition or with respect to a specific class of acquisitions described in the request and authorization referred to in subparagraph (B).

(D)(i) A request from a head of an element of the intelligence community located within one of the departments described in clause (ii) to exercise an authority referred to in subparagraph (A) shall be submitted to the Director of National Intelligence in accordance with any procedures established by the head of such department.

(ii) The departments described in this clause are the Department of Defense, the Department of Energy, the Department of Homeland Security, the Department of Justice, the Department of State, and the Department of the Treasury.

(E)(i) The head of an element of the intelligence community may not be authorized to utilize an authority referred to in subparagraph (A) for a class of acquisitions for a period of more than 3 years, except that the Director of National Intelligence (without delegation) may authorize the use of such an authority for not more than 6 years.

(ii) Each authorization to utilize an authority referred to in subparagraph (A) may be extended in accordance with the requirements of subparagraph (B) for successive periods of not more than 3 years, except that the Director of National Intelligence (without delegation) may authorize an extension period of not more than 6 years.

(F) Subject to clauses (i) and (ii) of subparagraph (E), the Director of National Intelligence may only delegate the authority of the Director under subparagraphs (A) through (E) to the Principal Dep-

uty Director of National Intelligence or a Deputy Director of National Intelligence.

(G) The Director of National Intelligence shall submit—

(i) to the congressional intelligence committees a notification of an authorization to exercise an authority referred to in subparagraph (A) or an extension of such authorization that includes the written authorization referred to in subparagraph (B)(ii); and

(ii) to the Director of the Office of Management and Budget a notification of an authorization to exercise an authority referred to in subparagraph (A) for an acquisition or class of acquisitions that will exceed $50,000,000 annually.

(H) Requests and authorizations to exercise an authority referred to in subparagraph (A) shall remain available within the Office of the Director of National Intelligence for a period of at least 6 years following the date of such request or authorization.

(I) Nothing in this paragraph may be construed to alter or otherwise limit the authority of the Central Intelligence Agency to independently exercise an authority under section 3 or 8(a) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403c and 403j(a)).

(o) CONSIDERATION OF VIEWS OF ELEMENTS OF INTELLIGENCE COMMUNITY.—In carrying out the duties and responsibilities under this section, the Director of National Intelligence shall take into account the views of a head of a department containing an element of the intelligence community and of the Director of the Central Intelligence Agency.

(p) RESPONSIBILITY OF DIRECTOR OF NATIONAL INTELLIGENCE REGARDING NATIONAL INTELLIGENCE PROGRAM BUDGET CONCERNING THE DEPARTMENT OF DEFENSE.—Subject to the direction of the President, the Director of National Intelligence shall, after consultation with the Secretary of Defense, ensure that the National Intelligence Program budgets for the elements of the intelligence community that are within the Department of Defense are adequate to satisfy the national intelligence needs of the Department of Defense, including the needs of the Chairman of the Joint Chiefs of Staff and the commanders of the unified and specified commands, and wherever such elements are performing Government-wide functions, the needs of other Federal departments and agencies.

(q) ACQUISITIONS OF MAJOR SYSTEMS.—(1) For each intelligence program within the National Intelligence Program for the acquisition of a major system, the Director of National Intelligence shall—

(A) require the development and implementation of a program management plan that includes cost, schedule, and performance goals and program milestone criteria, except that with respect to Department of Defense programs the Director shall consult with the Secretary of Defense;

(B) serve as exclusive milestone decision authority, except that with respect to Department of Defense programs the Director shall serve as milestone decision authority jointly with the Secretary of Defense or the designee of the Secretary; and

(C) periodically—

(i) review and assess the progress made toward the achievement of the goals and milestones established in such plan; and

(ii) submit to Congress a report on the results of such review and assessment.

(2) If the Director of National Intelligence and the Secretary of Defense are unable to reach an agreement on a milestone decision under paragraph (1)(B), the President shall resolve the conflict.

(3) Nothing in this subsection may be construed to limit the authority of the Director of National Intelligence to delegate to any other official any authority to perform the responsibilities of the Director under this subsection.

(4) In this subsection:

(A) The term "intelligence program", with respect to the acquisition of a major system, means a program that—

(i) is carried out to acquire such major system for an element of the intelligence community; and

(ii) is funded in whole out of amounts available for the National Intelligence Program.

(B) The term "major system" has the meaning given such term in section 4(9) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 403(9)).

(r) PERFORMANCE OF COMMON SERVICES.—The Director of National Intelligence shall, in consultation with the heads of departments and agencies of the United States Government containing elements within the intelligence community and with the Director of the Central Intelligence Agency, coordinate the performance by the elements of the intelligence community within the National Intelligence Program of such services as are of common concern to the intelligence community, which services the Director of National Intelligence determines can be more efficiently accomplished in a consolidated manner.

(s) PAY AUTHORITY FOR CRITICAL POSITIONS.—(1) Notwithstanding any pay limitation established under any other provision of law applicable to employees in elements of the intelligence community, the Director of National Intelligence may, in coordination with the Director of the Office of Personnel Management and the Director of the Office of Management and Budget, grant authority to the head of a department or agency to fix the rate of basic pay for one or more positions within the intelligence community at a rate in excess of any applicable limitation, subject to the provisions of this subsection. The exercise of authority so granted is at the discretion of the head of the department or agency employing the individual in a position covered by such authority, subject to the provisions of this subsection and any conditions established by the Director of National Intelligence when granting such authority.

(2) Authority under this subsection may be granted or exercised only—

(A) with respect to a position that requires an extremely high level of expertise and is critical to successful accomplishment of an important mission; and

(B) to the extent necessary to recruit or retain an individual exceptionally well qualified for the position.

(3) The head of a department or agency may not fix a rate of basic pay under this subsection at a rate greater than the rate payable for level II of the Executive Schedule under section 5313 of title 5, United States Code, except upon written approval of the Director of National Intelligence or as otherwise authorized by law.

(4) The head of a department or agency may not fix a rate of basic pay under this subsection at a rate greater than the rate payable for level I of the Executive Schedule under section 5312 of title 5, United States Code, except upon written approval of the President in response to a request by the Director of National Intelligence or as otherwise authorized by law.

(5) Any grant of authority under this subsection for a position shall terminate at the discretion of the Director of National Intelligence.

(6)(A) The Director of National Intelligence shall notify the congressional intelligence committees not later than 30 days after the date on which the Director grants authority to the head of a department or agency under this subsection.

(B) The head of a department or agency to which the Director of National Intelligence grants authority under this subsection shall notify the congressional intelligence committees and the Director of the exercise of such authority not later than 30 days after the date on which such head exercises such authority.

(t) AWARD OF RANK TO MEMBERS OF THE SENIOR NATIONAL INTELLIGENCE SERVICE.—(1) The President, based on the recommendation of the Director of National Intelligence, may award a rank to a member of the Senior National Intelligence Service or other intelligence community senior civilian officer not already covered by such a rank award program in the same manner in which a career appointee of an agency may be awarded a rank under section 4507 of title 5, United States Code.

(2) The President may establish procedures to award a rank under paragraph (1) to a member of the Senior National Intelligence Service or a senior civilian officer of the intelligence community whose identity as such a member or officer is classified information (as defined in section 606(1)).

(u) CONFLICT OF INTEREST REGULATIONS.—The Director of National Intelligence, in consultation with the Director of the Office of Government Ethics, shall issue regulations prohibiting an officer or employee of an element of the intelligence community from engaging in outside employment if such employment creates a conflict of interest or appearance thereof.

(v) AUTHORITY TO ESTABLISH POSITIONS IN EXCEPTED SERVICE.—(1) The Director of National Intelligence, with the concurrence of the head of the covered department concerned and in consultation with the Director of the Office of Personnel Management, may—

(A) convert competitive service positions, and the incumbents of such positions, within an element of the intelligence community in such department, to excepted service positions as the Director of National Intelligence determines necessary to carry out the intelligence functions of such element; and

(B) establish new positions in the excepted service within an element of the intelligence community in such department, if the Director of National Intelligence determines such positions are necessary to carry out the intelligence functions of such element.

(2) An incumbent occupying a position on the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2012 selected to be converted to the excepted service under this section shall have the right to refuse such conversion. Once such indi-

vidual no longer occupies the position, the position may be converted to the excepted service.

(3) A covered department may appoint an individual to a position converted or established pursuant to this subsection without regard to the civil-service laws, including parts II and III of title 5, United States Code.

(4) In this subsection, the term "covered department" means the Department of Energy, the Department of Homeland Security, the Department of State, or the Department of the Treasury.

(w) NUCLEAR PROLIFERATION ASSESSMENT STATEMENTS INTELLIGENCE COMMUNITY ADDENDUM.—The Director of National Intelligence, in consultation with the heads of the appropriate elements of the intelligence community and the Secretary of State, shall provide to the President, the congressional intelligence committees, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate an addendum to each Nuclear Proliferation Assessment Statement accompanying a civilian nuclear cooperation agreement, containing a comprehensive analysis of the country's export control system with respect to nuclear-related matters, including interactions with other countries of proliferation concern and the actual or suspected nuclear, dual-use, or missile-related transfers to such countries.

(x) REQUIREMENTS FOR INTELLIGENCE COMMUNITY CONTRACTORS.—The Director of National Intelligence, in consultation with the head of each department of the Federal Government that contains an element of the intelligence community and the Director of the Central Intelligence Agency, shall—

(1) ensure that—

(A) any contractor to an element of the intelligence community with access to a classified network or classified information develops and operates a security plan that is consistent with standards established by the Director of National Intelligence for intelligence community networks; and

(B) each contract awarded by an element of the intelligence community includes provisions requiring the contractor comply with such plan and such standards;

(2) conduct periodic assessments of each security plan required under paragraph (1)(A) to ensure such security plan complies with the requirements of such paragraph; and

(3) ensure that the insider threat detection capabilities and insider threat policies of the intelligence community apply to facilities of contractors with access to a classified network.

(y) FUNDRAISING.—(1) The Director of National Intelligence may engage in fundraising in an official capacity for the benefit of nonprofit organizations that—

(A) provide support to surviving family members of a deceased employee of an element of the intelligence community; or

(B) otherwise provide support for the welfare, education, or recreation of employees of an element of the intelligence community, former employees of an element of the intelligence community, or family members of such employees.

(2) In this subsection, the term "fundraising" means the raising of funds through the active participation in the promotion, produc-

tion, or presentation of an event designed to raise funds and does not include the direct solicitation of money by any other means.

(3) Not later than 7 days after the date the Director engages in fundraising authorized by this subsection or at the time the decision is made to participate in such fundraising, the Director shall notify the congressional intelligence committees of such fundraising.

(4) The Director, in consultation with the Director of the Office of Government Ethics, shall issue regulations to carry out the authority provided in this subsection. Such regulations shall ensure that such authority is exercised in a manner that is consistent with all relevant ethical constraints and principles, including the avoidance of any prohibited conflict of interest or appearance of impropriety.

(z) ANALYSES AND IMPACT STATEMENTS REGARDING PROPOSED INVESTMENT INTO THE UNITED STATES.—(1) Not later than 20 days after the completion of a review or an investigation of any proposed investment into the United States for which the Director has prepared analytic materials, the Director shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representative copies of such analytic materials, including any supplements or amendments to such analysis made by the Director.

(2) Not later than 60 days after the completion of consideration by the United States Government of any investment described in paragraph (1), the Director shall determine whether such investment will have an operational impact on the intelligence community, and, if so, shall submit a report on such impact to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives. Each such report shall—

(A) describe the operational impact of the investment on the intelligence community; and

(B) describe any actions that have been or will be taken to mitigate such impact.

* * * * * * *

CHIEF INFORMATION OFFICER

SEC. 103G. (a) CHIEF INFORMATION OFFICER.—To assist the Director of National Intelligence in carrying out the responsibilities of the Director under this Act and other applicable provisions of law, there shall be within the Office of the Director of National Intelligence a Chief Information Officer of the Intelligence Community who shall be appointed by the [President] *Director*. *The Chief Information Officer shall report directly to the Director of National Intelligence.*

(b) DUTIES AND RESPONSIBILITIES.—Subject to the direction of the Director of National Intelligence, the Chief Information Officer of the Intelligence Community shall—

(1) manage activities relating to the information technology infrastructure and enterprise architecture requirements of the intelligence community;

(2) have procurement approval authority over all information technology items related to the enterprise architectures of all intelligence community components;

(3) direct and manage all information technology-related procurement for the intelligence community; and

(4) ensure that all expenditures for information technology and research and development activities are consistent with the intelligence community enterprise architecture and the strategy of the Director for such architecture.

(c) PROHIBITION ON SIMULTANEOUS SERVICE AS OTHER CHIEF INFORMATION OFFICER.—An individual serving in the position of Chief Information Officer of the Intelligence Community may not, while so serving, serve as the chief information officer of any other department or agency, or component thereof, of the United States Government.

INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

SEC. 103H. (a) OFFICE OF INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—There is within the Office of the Director of National Intelligence an Office of the Inspector General of the Intelligence Community.

(b) PURPOSE.—The purpose of the Office of the Inspector General of the Intelligence Community is—

(1) to create an objective and effective office, appropriately accountable to Congress, to initiate and conduct independent investigations, inspections, audits, and reviews on programs and activities within the responsibility and authority of the Director of National Intelligence;

(2) to provide leadership and coordination and recommend policies for activities designed—

(A) to promote economy, efficiency, and effectiveness in the administration and implementation of such programs and activities; and

(B) to prevent and detect fraud and abuse in such programs and activities;

(3) to provide a means for keeping the Director of National Intelligence fully and currently informed about—

(A) problems and deficiencies relating to the administration of programs and activities within the responsibility and authority of the Director of National Intelligence; and

(B) the necessity for, and the progress of, corrective actions; and

(4) in the manner prescribed by this section, to ensure that the congressional intelligence committees are kept similarly informed of—

(A) significant problems and deficiencies relating to programs and activities within the responsibility and authority of the Director of National Intelligence; and

(B) the necessity for, and the progress of, corrective actions.

(c) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—(1) There is an Inspector General of the Intelligence Community, who shall be the head of the Office of the Inspector General of the Intelligence Community, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) The nomination of an individual for appointment as Inspector General shall be made—

(A) without regard to political affiliation;

(B) on the basis of integrity, compliance with security standards of the intelligence community, and prior experience in the field of intelligence or national security; and

(C) on the basis of demonstrated ability in accounting, financial analysis, law, management analysis, public administration, or investigations.

(3) The Inspector General shall report directly to and be under the general supervision of the Director of National Intelligence.

(4) The Inspector General may be removed from office only by the President. The President shall communicate in writing to the congressional intelligence committees the reasons for the removal not later than 30 days prior to the effective date of such removal. Nothing in this paragraph shall be construed to prohibit a personnel action otherwise authorized by law, other than transfer or removal.

(d) ASSISTANT INSPECTORS GENERAL.—Subject to the policies of the Director of National Intelligence, the Inspector General of the Intelligence Community shall—

(1) appoint an Assistant Inspector General for Audit who shall have the responsibility for supervising the performance of auditing activities relating to programs and activities within the responsibility and authority of the Director;

(2) appoint an Assistant Inspector General for Investigations who shall have the responsibility for supervising the performance of investigative activities relating to such programs and activities; and

(3) appoint other Assistant Inspectors General that, in the judgment of the Inspector General, are necessary to carry out the duties of the Inspector General.

(e) DUTIES AND RESPONSIBILITIES.—It shall be the duty and responsibility of the Inspector General of the Intelligence Community—

(1) to provide policy direction for, and to plan, conduct, supervise, and coordinate independently, the investigations, inspections, audits, and reviews relating to programs and activities within the responsibility and authority of the Director of National Intelligence;

(2) to keep the Director of National Intelligence fully and currently informed concerning violations of law and regulations, fraud, and other serious problems, abuses, and deficiencies relating to the programs and activities within the responsibility and authority of the Director, to recommend corrective action concerning such problems, and to report on the progress made in implementing such corrective action;

(3) to take due regard for the protection of intelligence sources and methods in the preparation of all reports issued by the Inspector General, and, to the extent consistent with the purpose and objective of such reports, take such measures as may be appropriate to minimize the disclosure of intelligence sources and methods described in such reports; and

(4) in the execution of the duties and responsibilities under this section, to comply with generally accepted government auditing.

(f) LIMITATIONS ON ACTIVITIES.—(1) The Director of National Intelligence may prohibit the Inspector General of the Intelligence Community from initiating, carrying out, or completing any investigation, inspection, audit, or review if the Director determines that such prohibition is necessary to protect vital national security interests of the United States.

(2) Not later than seven days after the date on which the Director exercises the authority under paragraph (1), the Director shall submit to the congressional intelligence committees an appropriately classified statement of the reasons for the exercise of such authority.

(3) The Director shall advise the Inspector General at the time a statement under paragraph (2) is submitted, and, to the extent consistent with the protection of intelligence sources and methods, provide the Inspector General with a copy of such statement.

(4) The Inspector General may submit to the congressional intelligence committees any comments on the statement of which the Inspector General has notice under paragraph (3) that the Inspector General considers appropriate.

(g) AUTHORITIES.—(1) The Inspector General of the Intelligence Community shall have direct and prompt access to the Director of National Intelligence when necessary for any purpose pertaining to the performance of the duties of the Inspector General.

(2)(A) The Inspector General shall, subject to the limitations in subsection (f), make such investigations and reports relating to the administration of the programs and activities within the authorities and responsibilities of the Director as are, in the judgment of the Inspector General, necessary or desirable.

(B) The Inspector General shall have access to any employee, or any employee of a contractor, of any element of the intelligence community needed for the performance of the duties of the Inspector General.

(C) The Inspector General shall have direct access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials that relate to the programs and activities with respect to which the Inspector General has responsibilities under this section.

(D) The level of classification or compartmentation of information shall not, in and of itself, provide a sufficient rationale for denying the Inspector General access to any materials under subparagraph (C).

(E) The Director, or on the recommendation of the Director, another appropriate official of the intelligence community, shall take appropriate administrative actions against an employee, or an employee of a contractor, of an element of the intelligence community that fails to cooperate with the Inspector General. Such administrative action may include loss of employment or the termination of an existing contractual relationship.

(3) The Inspector General is authorized to receive and investigate, pursuant to subsection (h), complaints or information from any person concerning the existence of an activity within the authorities and responsibilities of the Director of National Intelligence constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety. Once

such complaint or information has been received from an employee of the intelligence community—

(A) the Inspector General shall not disclose the identity of the employee without the consent of the employee, unless the Inspector General determines that such disclosure is unavoidable during the course of the investigation or the disclosure is made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken, and this provision shall qualify as a withholding statute pursuant to subsection (b)(3) of section 552 of title 5, United States Code (commonly known as the "Freedom of Information Act"); and

(B) no action constituting a reprisal, or threat of reprisal, for making such complaint or disclosing such information to the Inspector General may be taken by any employee in a position to take such actions, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

(4) The Inspector General shall have the authority to administer to or take from any person an oath, affirmation, or affidavit, whenever necessary in the performance of the duties of the Inspector General, which oath, affirmation, or affidavit when administered or taken by or before an employee of the Office of the Inspector General of the Intelligence Community designated by the Inspector General shall have the same force and effect as if administered or taken by, or before, an officer having a seal.

(5)(A) Except as provided in subparagraph (B), the Inspector General is authorized to require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data in any medium (including electronically stored information, as well as any tangible thing) and documentary evidence necessary in the performance of the duties and responsibilities of the Inspector General.

(B) In the case of departments, agencies, and other elements of the United States Government, the Inspector General shall obtain information, documents, reports, answers, records, accounts, papers, and other data and evidence for the purpose specified in subparagraph (A) using procedures other than by subpoenas.

(C) The Inspector General may not issue a subpoena for, or on behalf of, any component of the Office of the Director of National Intelligence or any element of the intelligence community, including the Office of the Director of National Intelligence.

(D) In the case of contumacy or refusal to obey a subpoena issued under this paragraph, the subpoena shall be enforceable by order of any appropriate district court of the United States.

(6) The Inspector General may obtain services as authorized by section 3109 of title 5, United States Code, at rates for individuals not to exceed the daily equivalent of the maximum annual rate of basic pay payable for grade GS–15 of the General Schedule under section 5332 of title 5, United States Code.

(7) The Inspector General may, to the extent and in such amounts as may be provided in appropriations, enter into contracts and other arrangements for audits, studies, analyses, and other services with public agencies and with private persons, and to make such payments as may be necessary to carry out the provisions of this section.

(h) COORDINATION AMONG INSPECTORS GENERAL.—(1)(A) In the event of a matter within the jurisdiction of the Inspector General of the Intelligence Community that may be subject to an investigation, inspection, audit, or review by both the Inspector General of the Intelligence Community and an inspector general with oversight responsibility for an element of the intelligence community, the Inspector General of the Intelligence Community and such other inspector general shall expeditiously resolve the question of which inspector general shall conduct such investigation, inspection, audit, or review to avoid unnecessary duplication of the activities of the inspectors general.

(B) In attempting to resolve a question under subparagraph (A), the inspectors general concerned may request the assistance of the Intelligence Community Inspectors General Forum established under paragraph (2). In the event of a dispute between an inspector general within a department or agency of the United States Government and the Inspector General of the Intelligence Community that has not been resolved with the assistance of such Forum, the inspectors general shall submit the question to the Director of National Intelligence and the head of the affected department or agency for resolution.

(2)(A) There is established the Intelligence Community Inspectors General Forum, which shall consist of all statutory or administrative inspectors general with oversight responsibility for an element of the intelligence community.

(B) The Inspector General of the Intelligence Community shall serve as the Chair of the Forum established under subparagraph (A). The Forum shall have no administrative authority over any inspector general, but shall serve as a mechanism for informing its members of the work of individual members of the Forum that may be of common interest and discussing questions about jurisdiction or access to employees, employees of contract personnel, records, audits, reviews, documents, recommendations, or other materials that may involve or be of assistance to more than one of its members.

(3) The inspector general conducting an investigation, inspection, audit, or review covered by paragraph (1) shall submit the results of such investigation, inspection, audit, or review to any other inspector general, including the Inspector General of the Intelligence Community, with jurisdiction to conduct such investigation, inspection, audit, or review who did not conduct such investigation, inspection, audit, or review.

(i) COUNSEL TO THE INSPECTOR GENERAL.—(1) The Inspector General of the Intelligence Community shall—

(A) appoint a Counsel to the Inspector General who shall report to the Inspector General; or

(B) obtain the services of a counsel appointed by and directly reporting to another inspector general or the Council of the Inspectors General on Integrity and Efficiency on a reimbursable basis.

(2) The counsel appointed or obtained under paragraph (1) shall perform such functions as the Inspector General may prescribe.

(j) STAFF AND OTHER SUPPORT.—(1) The Director of National Intelligence shall provide the Inspector General of the Intelligence Community with appropriate and adequate office space at central

and field office locations, together with such equipment, office supplies, maintenance services, and communications facilities and services as may be necessary for the operation of such offices.

(2)(A) Subject to applicable law and the policies of the Director of National Intelligence, the Inspector General shall select, appoint, and employ such officers and employees as may be necessary to carry out the functions, powers, and duties of the Inspector General. The Inspector General shall ensure that any officer or employee so selected, appointed, or employed has security clearances appropriate for the assigned duties of such officer or employee.

(B) In making selections under subparagraph (A), the Inspector General shall ensure that such officers and employees have the requisite training and experience to enable the Inspector General to carry out the duties of the Inspector General effectively.

(C) In meeting the requirements of this paragraph, the Inspector General shall create within the Office of the Inspector General of the Intelligence Community a career cadre of sufficient size to provide appropriate continuity and objectivity needed for the effective performance of the duties of the Inspector General.

(3) Consistent with budgetary and personnel resources allocated by the Director of National Intelligence, the Inspector General has final approval of—

(A) the selection of internal and external candidates for employment with the Office of the Inspector General; and

(B) all other personnel decisions concerning personnel permanently assigned to the Office of the Inspector General, including selection and appointment to the Senior Intelligence Service, but excluding all security-based determinations that are not within the authority of a head of a component of the Office of the Director of National Intelligence.

(4)(A) Subject to the concurrence of the Director of National Intelligence, the Inspector General may request such information or assistance as may be necessary for carrying out the duties and responsibilities of the Inspector General from any Federal, State (as defined ⟦in section 804⟧ *in section 805*), or local governmental agency or unit thereof.

(B) Upon request of the Inspector General for information or assistance from a department, agency, or element of the Federal Government under subparagraph (A), the head of the department, agency, or element concerned shall, insofar as is practicable and not in contravention of any existing statutory restriction or regulation of the department, agency, or element, furnish to the Inspector General, such information or assistance.

(C) The Inspector General of the Intelligence Community may, upon reasonable notice to the head of any element of the intelligence community and in coordination with that element's inspector general pursuant to subsection (h), conduct, as authorized by this section, an investigation, inspection, audit, or review of such element and may enter into any place occupied by such element for purposes of the performance of the duties of the Inspector General.

(k) REPORTS.—(1)(A) The Inspector General of the Intelligence Community shall, not later than October 31 and April 30 of each year, prepare and submit to the Director of National Intelligence a classified, and, as appropriate, unclassified semiannual report summarizing the activities of the Office of the Inspector General of

the Intelligence Community during the immediately preceding 6-month period ending September 30 and March 31, respectively. The Inspector General of the Intelligence Community shall provide any portion of the report involving a component of a department of the United States Government to the head of that department simultaneously with submission of the report to the Director of National Intelligence.

(B) Each report under this paragraph shall include, at a minimum, the following:

(i) A list of the title or subject of each investigation, inspection, audit, or review conducted during the period covered by such report.

(ii) A description of significant problems, abuses, and deficiencies relating to the administration of programs and activities of the intelligence community within the responsibility and authority of the Director of National Intelligence, and in the relationships between elements of the intelligence community, identified by the Inspector General during the period covered by such report.

(iii) A description of the recommendations for corrective action made by the Inspector General during the period covered by such report with respect to significant problems, abuses, or deficiencies identified in clause (ii).

(iv) A statement of whether or not corrective action has been completed on each significant recommendation described in previous semiannual reports, and, in a case where corrective action has been completed, a description of such corrective action.

(v) A certification of whether or not the Inspector General has had full and direct access to all information relevant to the performance of the functions of the Inspector General.

(vi) A description of the exercise of the subpoena authority under subsection (g)(5) by the Inspector General during the period covered by such report.

(vii) Such recommendations as the Inspector General considers appropriate for legislation to promote economy, efficiency, and effectiveness in the administration and implementation of programs and activities within the responsibility and authority of the Director of National Intelligence, and to detect and eliminate fraud and abuse in such programs and activities.

(C) Not later than 30 days after the date of receipt of a report under subparagraph (A), the Director shall transmit the report to the congressional intelligence committees together with any comments the Director considers appropriate. The Director shall transmit to the committees of the Senate and of the House of Representatives with jurisdiction over a department of the United States Government any portion of the report involving a component of such department simultaneously with submission of the report to the congressional intelligence committees.

(2)(A) The Inspector General shall report immediately to the Director whenever the Inspector General becomes aware of particularly serious or flagrant problems, abuses, or deficiencies relating to programs and activities within the responsibility and authority of the Director of National Intelligence.

(B) The Director shall transmit to the congressional intelligence committees each report under subparagraph (A) within 7 calendar days of receipt of such report, together with such comments as the Director considers appropriate. The Director shall transmit to the committees of the Senate and of the House of Representatives with jurisdiction over a department of the United States Government any portion of each report under subparagraph (A) that involves a problem, abuse, or deficiency related to a component of such department simultaneously with transmission of the report to the congressional intelligence committees.

(3)(A) In the event that—

(i) the Inspector General is unable to resolve any differences with the Director affecting the execution of the duties or responsibilities of the Inspector General;

(ii) an investigation, inspection, audit, or review carried out by the Inspector General focuses on any current or former intelligence community official who—

(I) holds or held a position in an element of the intelligence community that is subject to appointment by the President, whether or not by and with the advice and consent of the Senate, including such a position held on an acting basis;

(II) holds or held a position in an element of the intelligence community, including a position held on an acting basis, that is appointed by the Director of National Intelligence; or

(III) holds or held a position as head of an element of the intelligence community or a position covered by subsection (b) or (c) of section 106;

(iii) a matter requires a report by the Inspector General to the Department of Justice on possible criminal conduct by a current or former official described in clause (ii);

(iv) the Inspector General receives notice from the Department of Justice declining or approving prosecution of possible criminal conduct of any current or former official described in clause (ii); or

(v) the Inspector General, after exhausting all possible alternatives, is unable to obtain significant documentary information in the course of an investigation, inspection, audit, or review,

the Inspector General shall immediately notify, and submit a report to, the congressional intelligence committees on such matter.

(B) The Inspector General shall submit to the committees of the Senate and of the House of Representatives with jurisdiction over a department of the United States Government any portion of each report under subparagraph (A) that involves an investigation, inspection, audit, or review carried out by the Inspector General focused on any current or former official of a component of such department simultaneously with submission of the report to the congressional intelligence committees.

(4) The Director shall submit to the congressional intelligence committees any report or findings and recommendations of an investigation, inspection, audit, or review conducted by the office which has been requested by the Chairman or Vice Chairman or ranking minority member of either committee.

(5)(A) An employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community who intends to report to Congress a complaint or information with respect to an urgent concern may report such complaint or information to the Inspector General.

(B) Not later than the end of the 14-calendar-day period beginning on the date of receipt from an employee of a complaint or information under subparagraph (A), the Inspector General shall determine whether the complaint or information appears credible. Upon making such a determination, the Inspector General shall transmit to the Director a notice of that determination, together with the complaint or information.

(C) Upon receipt of a transmittal from the Inspector General under subparagraph (B), the Director shall, within 7 calendar days of such receipt, forward such transmittal to the congressional intelligence committees, together with any comments the Director considers appropriate.

(D)(i) If the Inspector General does not find credible under subparagraph (B) a complaint or information submitted under subparagraph (A), or does not transmit the complaint or information to the Director in accurate form under subparagraph (B), the employee (subject to clause (ii)) may submit the complaint or information to Congress by contacting either or both of the congressional intelligence committees directly.

(ii) An employee may contact the congressional intelligence committees directly as described in clause (i) only if the employee—

(I) before making such a contact, furnishes to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

(II) obtains and follows from the Director, through the Inspector General, direction on how to contact the congressional intelligence committees in accordance with appropriate security practices.

(iii) A member or employee of one of the congressional intelligence committees who receives a complaint or information under this subparagraph does so in that member or employee's official capacity as a member or employee of such committee.

(E) The Inspector General shall notify an employee who reports a complaint or information to the Inspector General under this paragraph of each action taken under this paragraph with respect to the complaint or information. Such notice shall be provided not later than 3 days after any such action is taken.

(F) An action taken by the Director or the Inspector General under this paragraph shall not be subject to judicial review.

(G) In this paragraph, the term "urgent concern" means any of the following:

(i) A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operation of an intelligence activity within the responsibility and authority of the Director of National Intelligence involving classified information, but does not include differences of opinions concerning public policy matters.

(ii) A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity.

(iii) An action, including a personnel action described in section 2302(a)(2)(A) of title 5, United States Code, constituting reprisal or threat of reprisal prohibited under subsection (g)(3)(B) of this section in response to an employee's reporting an urgent concern in accordance with this paragraph.

(H) Nothing in this section shall be construed to limit the protections afforded to an employee under section 17(d) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403q(d)) or section 8H of the Inspector General Act of 1978 (5 U.S.C. App.).

(I) An individual who has submitted a complaint or information to the Inspector General under this section may notify any member of either of the congressional intelligence committees, or a staff member of either of such committees, of the fact that such individual has made a submission to the Inspector General, and of the date on which such submission was made.

(6) In accordance with section 535 of title 28, United States Code, the Inspector General shall expeditiously report to the Attorney General any information, allegation, or complaint received by the Inspector General relating to violations of Federal criminal law that involves a program or operation of an element of the intelligence community, or in the relationships between the elements of the intelligence community, consistent with such guidelines as may be issued by the Attorney General pursuant to subsection (b)(2) of such section. A copy of each such report shall be furnished to the Director.

(l) CONSTRUCTION OF DUTIES REGARDING ELEMENTS OF INTELLIGENCE COMMUNITY.—Except as resolved pursuant to subsection (h), the performance by the Inspector General of the Intelligence Community of any duty, responsibility, or function regarding an element of the intelligence community shall not be construed to modify or affect the duties and responsibilities of any other inspector general having duties and responsibilities relating to such element.

(m) SEPARATE BUDGET ACCOUNT.—The Director of National Intelligence shall, in accordance with procedures issued by the Director in consultation with the congressional intelligence committees, include in the National Intelligence Program budget a separate account for the Office of the Inspector General of the Intelligence Community.

(n) BUDGET.—(1) For each fiscal year, the Inspector General of the Intelligence Community shall transmit a budget estimate and request to the Director of National Intelligence that specifies for such fiscal year—

(A) the aggregate amount requested for the operations of the Inspector General;

(B) the amount requested for all training requirements of the Inspector General, including a certification from the Inspector General that the amount requested is sufficient to fund all training requirements for the Office of the Inspector General; and

(C) the amount requested to support the Council of the Inspectors General on Integrity and Efficiency, including a justification for such amount.

(2) In transmitting a proposed budget to the President for a fiscal year, the Director of National Intelligence shall include for such fiscal year—

(A) the aggregate amount requested for the Inspector General of the Intelligence Community;

(B) the amount requested for Inspector General training;

(C) the amount requested to support the Council of the Inspectors General on Integrity and Efficiency; and

(D) the comments of the Inspector General, if any, with respect to such proposed budget.

(3) The Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives for each fiscal year—

(A) a separate statement of the budget estimate transmitted pursuant to paragraph (1);

(B) the amount requested by the Director for the Inspector General pursuant to paragraph (2)(A);

(C) the amount requested by the Director for the training of personnel of the Office of the Inspector General pursuant to paragraph (2)(B);

(D) the amount requested by the Director for support for the Council of the Inspectors General on Integrity and Efficiency pursuant to paragraph (2)(C); and

(E) the comments of the Inspector General under paragraph (2)(D), if any, on the amounts requested pursuant to paragraph (2), including whether such amounts would substantially inhibit the Inspector General from performing the duties of the Office of the Inspector General.

(o) INFORMATION ON WEBSITE.—(1) The Director of National Intelligence shall establish and maintain on the homepage of the publicly accessible website of the Office of the Director of National Intelligence information relating to the Office of the Inspector General of the Intelligence Community including methods to contact the Inspector General.

(2) The information referred to in paragraph (1) shall be obvious and facilitate accessibility to the information related to the Office of the Inspector General of the Intelligence Community.

CHIEF FINANCIAL OFFICER OF THE INTELLIGENCE COMMUNITY

SEC. 103I. (a) CHIEF FINANCIAL OFFICER OF THE INTELLIGENCE COMMUNITY.—To assist the Director of National Intelligence in carrying out the responsibilities of the Director under this Act and other applicable provisions of law, there is within the Office of the Director of National Intelligence a Chief Financial Officer of the Intelligence Community who shall be appointed by the Director. *The Chief Financial Officer shall report directly to the Director of National Intelligence.*

(b) DUTIES AND RESPONSIBILITIES.—Subject to the direction of the Director of National Intelligence, the Chief Financial Officer of the Intelligence Community shall—

(1) serve as the principal advisor to the Director of National Intelligence and the Principal Deputy Director of National Intelligence on the management and allocation of intelligence community budgetary resources;

(2) participate in overseeing a comprehensive and integrated strategic process for resource management within the intelligence community;

(3) ensure that the strategic plan of the Director of National Intelligence—

(A) is based on budgetary constraints as specified in the Future Year Intelligence Plans and Long-term Budget Projections required under section 506G; and

(B) contains specific goals and objectives to support a performance-based budget;

(4) prior to the obligation or expenditure of funds for the acquisition of any major system pursuant to a Milestone A or Milestone B decision, receive verification from appropriate authorities that the national requirements for meeting the strategic plan of the Director have been established, and that such requirements are prioritized based on budgetary constraints as specified in the Future Year Intelligence Plans and the Long-term Budget Projections for such major system required under section 506G;

(5) ensure that the collection architectures of the Director are based on budgetary constraints as specified in the Future Year Intelligence Plans and the Long-term Budget Projections required under section 506G;

(6) coordinate or approve representations made to Congress by the intelligence community regarding National Intelligence Program budgetary resources;

(7) participate in key mission requirements, acquisitions, or architectural boards formed within or by the Office of the Director of National Intelligence; and

(8) perform such other duties as may be prescribed by the Director of National Intelligence.

(c) OTHER LAW.—The Chief Financial Officer of the Intelligence Community shall serve as the Chief Financial Officer of the intelligence community and, to the extent applicable, shall have the duties, responsibilities, and authorities specified in chapter 9 of title 31, United States Code.

(d) PROHIBITION ON SIMULTANEOUS SERVICE AS OTHER CHIEF FINANCIAL OFFICER.—An individual serving in the position of Chief Financial Officer of the Intelligence Community may not, while so serving, serve as the chief financial officer of any other department or agency, or component thereof, of the United States Government.

(e) DEFINITIONS.—In this section:

(1) The term "major system" has the meaning given that term in section 506A(e).

(2) The term "Milestone A" has the meaning given that term in section 506G(f).

(3) The term "Milestone B" has the meaning given that term in section 506C(e).

* * * * * * *

DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY

SEC. 104A. (a) DIRECTOR OF CENTRAL INTELLIGENCE AGENCY.—There is a Director of the Central Intelligence Agency who shall be appointed by the President, by and with the advice and consent of the Senate.

(b) SUPERVISION.—The Director of the Central Intelligence Agency shall report to the Director of National Intelligence regarding the activities of the Central Intelligence Agency.

(c) DUTIES.—The Director of the Central Intelligence Agency shall—

(1) serve as the head of the Central Intelligence Agency; and

(2) carry out the responsibilities specified in subsection (d).

(d) RESPONSIBILITIES.—The Director of the Central Intelligence Agency shall—

(1) collect intelligence through human sources and by other appropriate means, except that the Director of the Central Intelligence Agency shall have no police, subpoena, or law enforcement powers or internal security functions;

(2) correlate and evaluate intelligence related to the national security and provide appropriate dissemination of such intelligence;

(3) provide overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the intelligence community authorized to undertake such collection and, in coordination with other departments, agencies, or elements of the United States Government which are authorized to undertake such collection, ensure that the most effective use is made of resources and that appropriate account is taken of the risks to the United States and those involved in such collection; and

(4) perform such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct.

(e) TERMINATION OF EMPLOYMENT OF CIA EMPLOYEES.—(1) Notwithstanding the provisions of any other law, the Director of the Central Intelligence Agency may, in the discretion of the Director, terminate the employment of any officer or employee of the Central Intelligence Agency whenever the Director deems the termination of employment of such officer or employee necessary or advisable in the interests of the United States.

(2) Any termination of employment of an officer or employee under paragraph (1) shall not affect the right of the officer or employee to seek or accept employment in any other department, agency, or element of the United States Government if declared eligible for such employment by the Office of Personnel Management.

(f) COORDINATION WITH FOREIGN GOVERNMENTS.—Under the direction of the Director of National Intelligence and in a manner consistent with section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), the Director of the Central Intelligence Agency shall coordinate the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

[(g) FOREIGN LANGUAGE PROFICIENCY FOR CERTAIN SENIOR LEVEL POSITIONS IN CENTRAL INTELLIGENCE AGENCY.—(1) Except as provided pursuant to paragraph (2), an individual in the Directorate of Intelligence career service or the National Clandestine Service career service may not be appointed or promoted to a position in the Senior Intelligence Service in the Directorate of Intelligence or the National Clandestine Service of the Central Intelligence Agency unless the Director of the Central Intelligence Agency determines that the individual has been certified as having a professional speaking and reading proficiency in a foreign language, such proficiency being at least level 3 on the Interagency Language Roundtable Language Skills Level or commensurate proficiency level using such other indicator of proficiency as the Director of the Central Intelligence Agency considers appropriate.

[(2) The Director of the Central Intelligence Agency may, in the discretion of the Director, waive the application of paragraph (1) to any position, category of positions, or occupation otherwise covered by that paragraph if the Director determines that foreign language proficiency is not necessary for the successful performance of the duties and responsibilities of such position, category of positions, or occupation.]

* * * * * * *

APPOINTMENT OF OFFICIALS RESPONSIBLE FOR INTELLIGENCE-RELATED ACTIVITIES

SEC. 106. (a) RECOMMENDATION OF DNI IN CERTAIN APPOINTMENTS.—(1) In the event of a vacancy in a position referred to in paragraph (2), the Director of National Intelligence shall recommend to the President an individual for nomination to fill the vacancy.

(2) Paragraph (1) applies to the following positions:

(A) The Principal Deputy Director of National Intelligence.

(B) The Director of the Central Intelligence Agency.

(b) CONCURRENCE OF DNI IN APPOINTMENTS TO POSITIONS IN THE INTELLIGENCE COMMUNITY.—(1) In the event of a vacancy in a position referred to in paragraph (2), the head of the department or agency having jurisdiction over the position shall obtain the concurrence of the Director of National Intelligence before appointing an individual to fill the vacancy or recommending to the President an individual to be nominated to fill the vacancy. If the Director does not concur in the recommendation, the head of the department or agency concerned may not fill the vacancy or make the recommendation to the President (as the case may be). In the case in which the Director does not concur in such a recommendation, the Director and the head of the department or agency concerned may advise the President directly of the intention to withhold concurrence or to make a recommendation, as the case may be.

(2) Paragraph (1) applies to the following positions:

(A) The Director of the National Security Agency.

(B) The Director of the National Reconnaissance Office.

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

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

(E) The Director of the Office of Intelligence *and Counterintelligence* of the Department of Energy.

[(F) The Director of the Office of Counterintelligence of the Department of Energy.]

[(G)] *(F)* The Assistant Secretary for Intelligence and Analysis of the Department of the Treasury.

[(H)] *(G)* The Executive Assistant Director for Intelligence of the Federal Bureau of Investigation or any successor to that position.

[(I)] *(H)* The Under Secretary of Homeland Security for Intelligence and Analysis.

(c) CONSULTATION WITH DNI IN CERTAIN POSITIONS.—(1) In the event of a vacancy in a position referred to in paragraph (2), the head of the department or agency having jurisdiction over the position shall consult with the Director of National Intelligence before appointing an individual to fill the vacancy or recommending to the President an individual to be nominated to fill the vacancy.

(2) Paragraph (1) applies to the following positions:

(A) The Director of the Defense Intelligence Agency.

(B) The Assistant Commandant of the Coast Guard for Intelligence.

(C) The Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code.

SEC. 106A. DIRECTOR OF THE NATIONAL RECONNAISSANCE OFFICE.

(a) IN GENERAL.—There is a Director of the National Reconnaissance Office.

(b) APPOINTMENT.—The Director of the National Reconnaissance Office shall be appointed by the President, by and with the advice and consent of the Senate.

(c) FUNCTIONS AND DUTIES.—The Director of the National Reconnaissance Office shall be the head of the National Reconnaissance Office and shall discharge such functions and duties as are provided by this Act or otherwise by law or executive order.

(d) ADVISORY BOARD.—

(1) ESTABLISHMENT.—There is established in the National Reconnaissance Office an advisory board (in this section referred to as the "Board").

(2) DUTIES.—The Board shall—

(A) study matters relating to the mission of the National Reconnaissance Office, including with respect to promoting innovation, competition, and resilience in space, overhead reconnaissance, acquisition, and other matters; and

(B) advise and report directly to the Director with respect to such matters.

(3) MEMBERS.—

(A) NUMBER AND APPOINTMENT.—

(i) IN GENERAL.—The Board shall be composed of 5 members appointed by the Director from among individuals with demonstrated academic, government, business, or other expertise relevant to the mission and functions of the National Reconnaissance Office.

(ii) NOTIFICATION.—Not later than 30 days after the date on which the Director appoints a member to the Board, the Director shall notify the congressional intel-

ligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) of such appointment.

(B) TERMS.—Each member shall be appointed for a term of 2 years. Except as provided by subparagraph (C), a member may not serve more than 3 terms.

(C) VACANCY.—Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has taken office.

(D) CHAIR.—The Board shall have a Chair, who shall be appointed by the Director from among the members.

(E) TRAVEL EXPENSES.—Each member shall 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.

(F) EXECUTIVE SECRETARY.—The Director may appoint an executive secretary, who shall be an employee of the National Reconnaissance Office, to support the Board.

(4) MEETINGS.—The Board shall meet not less than quarterly, but may meet more frequently at the call of the Director.

(5) REPORTS.—Not later than March 31 of each year, the Board shall submit to the Director and to the congressional intelligence committees a report on the activities and significant findings of the Board during the preceding year.

(6) NONAPPLICABILITY OF CERTAIN REQUIREMENTS.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Board.

(7) TERMINATION.—The Board shall terminate on the date that is 3 years after the date of the first meeting of the Board.

[NATIONAL SECURITY RESOURCES BOARD

[SEC. 107. (a) The Director of the Office of Defense Mobilization, subject to the direction of the President, is authorized, subject to the civil-service laws and the Classification Act of 1949, to appoint and fix the compensation of such personnel as may be necessary to assist the Director in carrying out his functions.

[(b) It shall be the function of the Director of the Office of Defense Mobilization to advise the President concerning the coordination of military, industrial, and civilian mobilization, including—

[(1) policies concerning industrial and civilian mobilization in order to assure the most effective mobilization and maximum utilization of the Nation's manpower in the event of war.

[(2) programs for the effective use in time of war of the Nation's natural and industrial resources for military and civilian needs, for the maintenance and stabilization of the civilian economy in time of war, and for the adjustment of such economy to war needs and conditions;

[(3) policies for unifying, in time of war, the activities of Federal agencies and departments engaged in or concerned with production, procurement, distribution, or transportation of military or civilian supplies, materials, and products;

[(4) the relationship between potential supplies of, and potential requirements for, manpower, resources, and productive facilities in time of war;

[(5) policies for establishing adequate reserves of strategic and critical material, and for the conservation of these reserves;

[(6) the strategic relocation of industries, services, government, and economic activities, the continuous operation of which is essential to the Nation's security.

[(c) In performing his functions, the Director of the Office of Defense Mobilization shall utilize to the maximum extent the facilities and resources of the departments and agencies of the Government.]

ANNUAL NATIONAL SECURITY STRATEGY REPORT

SEC. 108. (a)(1) The President shall transmit to Congress each year a comprehensive report on the national security strategy of the United States (hereinafter in this section referred to as a national security strategy report").

(2) The national security strategy report for any year shall be transmitted on the date on which the President submits to Congress the budget for the next fiscal year under section 1105 of title 31, United States Code.

(3) Not later than 150 days after the date on which a new President takes office, the President shall transmit to Congress a national security strategy report under this section. That report shall be in addition to the report for that year transmitted at the time specified in paragraph (2).

(b) Each national security strategy report shall set forth the national security strategy of the United States and shall include a comprehensive description and discussion of the following:

(1) The worldwide interests, goals, and objectives of the United States that are vital to the national security of the United States.

(2) The foreign policy, worldwide commitments, and national defense capabilities of the United States necessary to deter aggression and to implement the national security strategy of the United States.

(3) The proposed short-term and long-term uses of the political, economic, military, and other elements of the national power of the United States to protect or promote the interests and achieve the goals and objectives referred to in paragraph (1).

(4) The adequacy of the capabilities of the United States to carry out the national security strategy of the United States, including an evaluation of the balance among the capabilities of all elements of the national power of the United States to support the implementation of the national security strategy.

(5) Such other information as may be necessary to help inform Congress on matters relating to the national security strategy of the United States.

(c) Each national security strategy report shall be transmitted [in both a classified and an unclassified form] *to Congress in classified form, but may include an unclassified summary*.

* * * * * * *

RESTRICTIONS ON INTELLIGENCE SHARING WITH THE UNITED NATIONS

SEC. 112. (a) PROVISION OF INTELLIGENCE INFORMATION TO THE UNITED NATIONS.—(1) No United States intelligence information may be provided to the United Nations or any organization affiliated with the United Nations, or to any officials or employees thereof, unless the President certifies to the appropriate committees of Congress that the Director of National Intelligence, in consultation with the Secretary of State and the Secretary of Defense, has established and implemented procedures, and has worked with the United Nations to ensure implementation of procedures, for protecting from unauthorized disclosure United States intelligence sources and methods connected to such information.

(2) Paragraph (1) may be waived upon written certification by the President to the appropriate committees of Congress that providing such information to the United Nations or an organization affiliated with the United Nations, or to any officials or employees thereof, is in the national security interests of the United States.

(b) DELEGATION OF DUTIES.—The President may not delegate or assign the duties of the President under this section.

(c) RELATIONSHIP TO EXISTING LAW.—Nothing in this section shall be construed to—

(1) impair or otherwise affect the authority of the Director of National Intelligence to protect intelligence sources and methods from unauthorized disclosure pursuant to [section 103(c)(7)] *section 102A(i)* of this Act; or

(2) supersede or otherwise affect the provisions of title V of this Act.

(d) DEFINITION.—As used in this section, the term "appropriate committees of Congress" means the Committee on Foreign Relations and the Select Committee on Intelligence of the Senate and the Committee on Foreign Relations and the Permanent Select Committee on Intelligence of the House of Representatives.

* * * * * * *

SEC. 113B. SPECIAL PAY AUTHORITY FOR SCIENCE, TECHNOLOGY, ENGINEERING, OR MATHEMATICS POSITIONS.

[(a) AUTHORITY TO SET SPECIAL RATES OF PAY.—Notwithstanding part III of title 5, United States Code, the head of each element of the intelligence community may establish higher minimum rates of pay for 1 or more categories of positions in such element that require expertise in science, technology, engineering, or mathematics (STEM).]

(a) SPECIAL RATES OF PAY FOR POSITIONS REQUIRING EXPERTISE IN SCIENCE, TECHNOLOGY, ENGINEERING, OR MATHEMATICS.—

(1) IN GENERAL.—Notwithstanding part III of title 5, United States Code, the head of each element of the intelligence community may, for 1 or more categories of positions in such element that require expertise in science, technology, engineering, or mathematics—

(A) establish higher minimum rates of pay; and

(B) make corresponding increases in all rates of pay of the pay range for each grade or level, subject to subsection (b) or (c), as applicable.

(2) TREATMENT.—The special rate supplements resulting from the establishment of higher rates under paragraph (1) shall be basic pay for the same or similar purposes as those specified in section 5305(j) of title 5, United States Code.

(b) SPECIAL RATES OF PAY FOR CYBER POSITIONS.—

(1) IN GENERAL.—Notwithstanding subsection (c), the Director of the National Security Agency may establish a special rate of pay—

(A) not to exceed the rate of basic pay payable for level II of the Executive Schedule under section 5313 of title 5, United States Code, if the Director certifies to the Under Secretary of Defense for Intelligence, in consultation with the Under Secretary of Defense for Personnel and Readiness, that the rate of pay is for positions that perform functions that execute the cyber mission of the Agency; or

(B) not to exceed the rate of basic pay payable for the Vice President of the United States under section 104 of title 3, United States Code, if the Director certifies to the Secretary of Defense, by name, individuals that have advanced skills and competencies and that perform critical functions that execute the cyber mission of the Agency.

(2) PAY LIMITATION.—Employees receiving a special rate under paragraph (1) shall be subject to an aggregate pay limitation that parallels the limitation established in section 5307 of title 5, United States Code, except that—

(A) any allowance, differential, bonus, award, or other similar cash payment in addition to basic pay that is authorized under title 10, United States Code, (or any other applicable law in addition to title 5 of such Code, excluding the Fair Labor Standards Act of 1938 (29 U.S.C. 201 et seq.)) shall also be counted as part of aggregate compensation; and

(B) aggregate compensation may not exceed the rate established for the Vice President of the United States under section 104 of title 3, United States Code.

(3) LIMITATION ON NUMBER OF RECIPIENTS.—The number of individuals who receive basic pay established under paragraph (1)(B) may not exceed 100 at any time.

(4) LIMITATION ON USE AS COMPARATIVE REFERENCE.—Notwithstanding any other provision of law, special rates of pay and the limitation established under paragraph (1)(B) may not be used as comparative references for the purpose of fixing the rates of basic pay or maximum pay limitations of qualified positions under section 1599f of title 10, United States Code, or section 226 of the Homeland Security Act of 2002 (6 U.S.C. 147).

[(b)**]** *(c)* MAXIMUM SPECIAL RATE OF PAY.—**[**A minimum**]** *Except as provided in subsection (b), a minimum* rate of pay established for a category of positions under subsection (a) may not exceed the maximum rate of basic pay (excluding any locality-based comparability payment under section 5304 of title 5, United States

Code, or similar provision of law) for the position in that category of positions without the authority of subsection (a) by more than 30 percent, and no rate may be established under this section in excess of the rate of basic pay payable for level IV of the Executive Schedule under section 5315 of title 5, United States Code.

[(c)] *(d)* NOTIFICATION OF REMOVAL FROM SPECIAL RATE OF PAY.—If the head of an element of the intelligence community removes a category of positions from coverage under a rate of pay authorized by subsection (a) *or (b)* after that rate of pay takes effect—

(1) the head of such element shall provide notice of the loss of coverage of the special rate of pay to each individual in such category; and

(2) the loss of coverage will take effect on the first day of the first pay period after the date of the notice.

[(d)] *(e)* REVISION OF SPECIAL RATES OF PAY.—Subject to the limitations in this section, rates of pay established under this section by the head of the element of the intelligence community may be revised from time to time by the head of such element and the revisions have the force and effect of statute.

[(e)] *(f)* REGULATIONS.—The head of each element of the intelligence community shall promulgate regulations to carry out this section with respect to such element, which shall, to the extent practicable, be comparable to the regulations promulgated to carry out section 5305 of title 5, United States Code.

[(f)] *(g)* REPORTS.—

(1) REQUIREMENT FOR REPORTS.—[Not later than 90 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2017] *Not later than 90 days after the date of the enactment of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019*, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report on any rates of pay established for such element under this section.

(2) CONTENTS.—Each report required by paragraph (1) shall contain for each element of the intelligence community—

(A) a description of any rates of pay established under subsection (a) *or (b)*; and

(B) the number of positions in such element that will be subject to such rates of pay.

ANNUAL REPORT ON HIRING AND RETENTION OF MINORITY EMPLOYEES

SEC. 114.

(a) The Director of National Intelligence shall, on an annual basis, submit to Congress a report on the employment of covered persons within each element of the intelligence community for the preceding fiscal year *and the preceding 5 fiscal years*.

(b) Each such report shall include [disaggregated data by category of covered person from each element of the intelligence community] *data, disaggregated by category of covered person and by element of the intelligence community,* on the following:

(1) Of all individuals employed in the element during the fiscal year involved, the aggregate percentage of such individuals who are covered persons.

(2) Of all individuals employed in the element during the fiscal year involved at the levels referred to in subparagraphs (A) and (B), the percentage of covered persons employed at such levels:

(A) Positions at levels 1 through 15 of the General Schedule.

(B) Positions at levels above GS–15.

(3) Of all individuals hired by the element involved during the fiscal year involved, the percentage of such individuals who are covered persons.

(c) Each such report shall be submitted in unclassified form, but may contain a classified annex.

(d) Nothing in this section shall be construed as providing for the substitution of any similar report required under another provision of law.

(e) In this section the term "covered persons" means—

(1) racial and ethnic minorities;

(2) women; and

(3) individuals with disabilities.

* * * * * * *

SEC. 120. CLIMATE SECURITY ADVISORY COUNCIL.

(a) ESTABLISHMENT.—The Director of National Intelligence shall establish a Climate Security Advisory Council for the purpose of—

(1) assisting intelligence analysts of various elements of the intelligence community with respect to analysis of climate security and its impact on the areas of focus of such analysts;

(2) facilitating coordination between the elements of the intelligence community and elements of the Federal Government that are not elements of the intelligence community in collecting data on, and conducting analysis of, climate change and climate security; and

(3) ensuring that the intelligence community is adequately prioritizing climate change in carrying out its activities.

(b) COMPOSITION OF COUNCIL.—

(1) MEMBERS.—The Council shall be composed of the following individuals appointed by the Director of National Intelligence:

(A) An appropriate official from the National Intelligence Council, who shall chair the Council.

(B) The lead official with respect to climate and environmental security analysis from—

(i) the Central Intelligence Agency;

(ii) the Bureau of Intelligence and Research of the Department of State;

(iii) the National Geospacial-Intelligence Agency;

(iv) the Office of Intelligence and Counterintelligence of the Department of Energy;

(v) the Office of the Under Secretary of Defense for Intelligence; and

(vi) the Defense Intelligence Agency.

(C) Three appropriate officials from elements of the Federal Government that are not elements of the intelligence community that are responsible for—

(i) providing decision-makers with a predictive understanding of the climate;

(ii) making observations of our Earth system that can be used by the public, policymakers, and to support strategic decisions; or

(iii) coordinating Federal research and investments in understanding the forces shaping the global environment, both human and natural, and their impacts on society.

(D) Any other officials as the Director of National Intelligence or the chair of the Council may determine appropriate.

(2) RESPONSIBILITIES OF CHAIR.—The chair of the Council shall have responsibility for—

(A) identifying agencies to supply individuals from elements of the Federal Government that are not elements of the intelligence community;

(B) securing the permission of the relevant agency heads for the participation of such individuals on the Council; and

(C) any other duties that the Director of National Intelligence may direct.

(c) DUTIES AND RESPONSIBILITIES OF COUNCIL.—The Council shall carry out the following duties and responsibilities:

(1) To meet at least quarterly to—

(A) exchange appropriate data between elements of the intelligence community and elements of the Federal Government that are not elements of the intelligence community;

(B) discuss processes for the routine exchange of such data and implementation of such processes; and

(C) prepare summaries of the business conducted at each meeting.

(2) To assess and determine best practices with respect to the analysis of climate security, including identifying publicly available information and intelligence acquired through clandestine means that enables such analysis.

(3) To assess and identify best practices with respect to prior efforts of the intelligence community to analyze climate security.

(4) To assess and describe best practices for identifying and disseminating climate security indicators and warnings;

(5) To recommend methods of incorporating analysis of climate security and the best practices identified under paragraphs (2) through (4) into existing analytic training programs.

(6) To consult, as appropriate, with other elements of the intelligence community that conduct analysis of climate change or climate security and elements of the Federal Government that are not elements of the intelligence community that conduct analysis of climate change or climate security, for the purpose of sharing information about ongoing efforts and avoiding duplication of existing efforts.

(7) To work with elements of the intelligence community that conduct analysis of climate change or climate security and elements of the Federal Government that are not elements of the intelligence community that conduct analysis of climate change or climate security—

(A) to exchange appropriate data between such elements, establish processes, procedures and practices for the routine exchange of such data, discuss the implementation of such processes; and

(B) to enable and facilitate the sharing of findings and analysis between such elements.

(8) To assess whether the elements of the intelligence community that conduct analysis of climate change or climate security may inform the research direction of academic work and the sponsored work of the United States Government.

(9) At the discretion of the chair of the Council, to convene conferences of analysts and non-intelligence community personnel working on climate change or climate security on subjects that the chair shall direct.

(d) SUNSET.—The Council shall terminate on the date that is 4 years after the date of the enactment of this section.

(e) DEFINITIONS.—In this section:

(1) CLIMATE SECURITY.—The term "climate security" means the effects of climate change on the following:

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

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

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

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

(2) CLIMATE INTELLIGENCE INDICATIONS AND WARNINGS.—The term "climate intelligence indications and warnings" means developments relating to climate security with the potential to—

(A) imminently and substantially alter the political stability or degree of human security in a country or region; or

(B) imminently and substantially threaten—

(i) the national security of the United States;

(ii) the military, political, or economic interests of allies and partners of the United States; or

(iii) citizens of the United States abroad.

* * * * * * *

TITLE II—THE DEPARTMENT OF DEFENSE

[SEC. 201.

[(d) Except to the extent inconsistent with the provisions of this Act, the provisions of title IV of the Revised Statutes as now of hereafter amended shall be applicable to the Department of Defense.]

SEC. 201. DEPARTMENT OF DEFENSE.

Except to the extent inconsistent with the provisions of this Act or other provisions of law, the provisions of title 5, United States Code, shall be applicable to the Department of Defense.

DEPARTMENT OF THE ARMY

SEC. 205.

[(b)] *(a)* All laws, orders, regulations, and other actions relating to the Department of War or to any officer or activity whose title is changed under this section shall, insofar as they are not inconsistent with the provisions of this Act, be deemed to relate to the Department of the Army within the Department of Defense or to such officer or activity designated by his or its new title.

[(c)] *(b)* the term "Department of the Army" as used in this Act shall be construed to mean the Department of the Army at the seat of government and all field headquarters, forces, reserve components, installations, activities, and functions under the control or supervision of the Department of the Army.

DEPARTMENT OF THE NAVY

SEC. 206. [(a)] The term "Department of the Navy" as used in this Act shall be construed to mean the Department of the Navy at the seat of government; the headquarters, United States Marine Corps; the entire operating forces of the United States Navy, including naval aviation, and of the United States Marine Corps, including the reserve components of such forces; all field activities, headquarters, forces, bases, installations, activities and functions under the control or supervision of the Department of the Navy; and the United States Coast Guard when operating as a part of the Navy pursuant to law.

DEPARTMENT OF THE AIR FORCE

SEC. 207.

[(c)] The term "Department of the Air Force" as used in this Act shall be construed to mean the Department of the Air Force at the seat of government and all field headquarters, forces, reserve components, installations, activities, and functions under the control or supervision of the Department of the Air Force.

TITLE III—MISCELLANEOUS

* * * * * * *

SEC. 305. PAID PARENTAL LEAVE.

(a) PAID PARENTAL LEAVE.—Notwithstanding any other provision of law, a civilian employee of an element of the intelligence community shall have available a total of 12 administrative workweeks of paid parental leave in the event of the birth of a son or daughter of the employee, or placement of a son or daughter with the employee for adoption or foster care in order to care for such son or daughter. Such paid parental leave shall be used during the 12-month period beginning on the date of the birth or placement. Nothing in this section shall be construed to modify or otherwise affect the eligibility of an employee of an element of the intelligence community for benefits relating to leave under any other provision of law.

(b) TREATMENT OF PARENTAL LEAVE REQUEST.—Notwithstanding any other provision of law—

(1) an element of the intelligence community shall accommodate an employee's leave request under subsection (a), including

a request to use such leave intermittently or to create a reduced work schedule, to the extent that the requested leave schedule does not unduly disrupt operations; and

(2) to the extent that an employee's requested leave described in paragraph (1) arises out of medical necessity related to a serious health condition connected to the birth of a son or daughter, the employing element shall handle the scheduling consistent with the treatment of employees who are using leave under subparagraph (C) or (D) of section 6382(a)(1) of title 5, United States Code.

(c) RULES RELATING TO PAID LEAVE.—Notwithstanding any other provision of law—

(1) an employee may not be required to first use all or any portion of any unpaid leave available to the employee before being allowed to use the paid parental leave described in subsection (a); and

(2) paid parental leave under subsection (a)—

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

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

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

(D) may be granted only to the extent that the employee does not receive a total of more than 12 weeks of paid parental leave in any 12-month period beginning on the date of a birth or placement;

(E) may not be granted—

(i) in excess of a lifetime aggregate total of 30 administrative workweeks based on placements of a foster child for any individual employee; or

(ii) in connection with temporary foster care placements expected to last less than 1 year;

(F) may not be granted for a child being placed for foster care or adoption if such leave was previously granted to the same employee when the same child was placed with the employee for foster care in the past;

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

(H) may not be used during off-season (nonpay status) periods for employees with seasonal work schedules.

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

(1) processes and procedures for implementing the paid parental leave policies under subsections (a) through (c);

(2) an explanation of how the implementation of subsections (a) through (c) will be reconciled with policies of other elements of the Federal Government, including the impact on elements funded by the National Intelligence Program that are housed within agencies outside the intelligence community; and

(3) all costs or operational expenses associated with the implementation of subsections (a) through (c).

(e) DIRECTIVE.—Not later than 180 days after the Director of National Intelligence submits the implementation plan under subsection (d), the Director of National Intelligence shall issue a written directive to implement this section, which directive shall take effect on the date of issuance.

(f) ANNUAL REPORT.—The Director of National Intelligence shall submit to the congressional intelligence committees an annual report that—

(1) details the number of employees of each element of the intelligence community who applied for and took paid parental leave under subsection (a) during the year covered by the report;

(2) details the number of—

(A) employees of each element of the intelligence community stationed abroad who applied for and took paid parental leave under subsection (a) during the year covered by the report; and

(B) employees of each element of the intelligence community stationed abroad who applied for paid parental leave but such application was not granted because of an undue impact on operations as specified in subsection (b)(1); and

(3) includes updates on major implementation challenges or costs associated with paid parental leave.

(g) DEFINITION OF SON OR DAUGHTER.—For purposes of this section, the term "son or daughter" has the meaning given the term in section 6381 of title 5, United States Code.

* * * * * * *

DEFINITIONS

SEC. 308. (a) As used in [this Act] *sections 2, 101, 102, 103, and 303 of this Act*, the term "function" includes functions, powers, and duties.

(b) As used in this Act, the term, "Department of Defense" shall be deemed to include the military departments of the Army, the Navy, and the Air Force, and all agencies created under title II of this Act.

* * * * * * *

REPEALING AND SAVING PROVISIONS

SEC. [411.] *312.* All laws, orders, and regulations inconsistent with the provisions of this title are repealed insofar as they are inconsistent with the powers, duties, and responsibilities enacted hereby: *Provided,* That the powers, duties, and responsibilities of the Secretary of Defense under this title shall be administered in conformance with the policy and requirements for administration of budgetary and fiscal matters in the Government generally, including accounting and financial reporting, and that nothing in this

title shall be construed as eliminating or modifying the powers, duties, and responsibilities of any other department, agency, or officer of the Government in connection with such matters, but no such department, agency, or officer shall exercise any such powers, duties, or responsibilities in a manner that will render ineffective the provisions of this title.

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

* * * * * * *

PRESIDENTIAL APPROVAL AND REPORTING OF COVERT ACTIONS

SEC. 503. (a) The President may not authorize the conduct of a covert action by departments, agencies, or entities of the United States Government unless the President determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States, which determination shall be set forth in a finding that shall meet each of the following conditions:

(1) Each finding shall be in writing, unless immediate action by the United States is required and time does not permit the preparation of a written finding, in which case a written record of the President's decision shall be contemporaneously made and shall be reduced to a written finding as soon as possible but in no event more than 48 hours after the decision is made.

(2) Except as permitted by paragraph (1), a finding may not authorize or sanction a covert action, or any aspect of any such action, which already has occurred.

(3) Each finding shall specify each department, agency, or entity of the United States Government authorized to fund or otherwise participate in any significant way in such action. Any employee, contractor, or contract agent of a department, agency, or entity of the United States Government other than the Central Intelligence Agency directed to participate in any way in a covert action shall be subject either to the policies and regulations of the Central Intelligence Agency, or to written policies or regulations adopted by such department, agency, or entity, to govern such participation.

(4) Each finding shall specify whether it is contemplated that any third party which is not an element of, or a contractor or contract agent of, the United States Government, or is not otherwise subject to United States Government policies and regulations, will be used to fund or otherwise participate in any significant way in the covert action concerned, or be used to undertake the covert action concerned on behalf of the United States.

(5) A finding may not authorize any action that would violate the Constitution or any statute of the United States.

(b) To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of National Intelligence and the heads of all departments, agencies, and entities of the United States Government involved in a covert action—

(1) shall keep the congressional intelligence committees fully and currently informed of all covert actions which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including significant failures; and

(2) shall furnish to the congressional intelligence committees any information or material concerning covert actions (including the legal basis under which the covert action is being or was conducted) which is in the possession, custody, or control of any department, agency, or entity of the United States Government and which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.

(c)(1) The President shall ensure that any finding approved pursuant to subsection (a) shall be reported in writing to the congressional intelligence committees as soon as possible after such approval and before the initiation of the covert action authorized by the finding, except as otherwise provided in paragraph (2) and paragraph (3).

(2) If the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States, the finding may be reported to the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President.

(3) Whenever a finding is not reported pursuant to paragraph (1) or (2) of this section, the President shall fully inform the congressional intelligence committees in a timely fashion and shall provide a statement of the reasons for not giving prior notice.

(4) In a case under paragraph (1), (2), or (3), a copy of the finding, signed by the President, shall be provided to the chairman of each congressional intelligence committee.

(5)(A) When access to a finding, or a notification provided under subsection (d)(1), is limited to the Members of Congress specified in paragraph (2), a written statement of the reasons for limiting such access shall also be provided.

(B) Not later than 180 days after a statement of reasons is submitted in accordance with subparagraph (A) or this subparagraph, the President shall ensure that—

(i) all members of the congressional intelligence committees are provided access to the finding or notification; or

(ii) a statement of reasons that it is essential to continue to limit access to such finding or such notification to meet extraordinary circumstances affecting vital interests of the United States is submitted to the Members of Congress specified in paragraph (2).

(d)(1) The President shall ensure that the congressional intelligence committees, or, if applicable, the Members of Congress specified in subsection (c)(2), are notified in writing of any significant change in a previously approved covert action, or any significant undertaking pursuant to a previously approved finding, in the same manner as findings are reported pursuant to subsection (c).

(2) In determining whether an activity constitutes a significant undertaking for purposes of paragraph (1), the President shall consider whether the activity—

(A) involves significant risk of loss of life;

(B) requires an expansion of existing authorities, including authorities relating to research, development, or operations;

(C) results in the expenditure of significant funds or other resources;

(D) requires notification under section 504;

(E) gives rise to a significant risk of disclosing intelligence sources or methods; or

(F) presents a reasonably foreseeable risk of serious damage to the diplomatic relations of the United States if such activity were disclosed without authorization.

(e) As used in this title, the term "covert action" means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include—

(1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) traditional diplomatic or military activities or routine support to such activities;

(3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(f) No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

(g)(1) In any case where access to a finding reported under subsection (c) or notification provided under subsection (d)(1) is not made available to all members of a congressional intelligence committee in accordance with subsection (c)(2), the President shall notify all members of such committee that such finding or such notification has been provided only to the members specified in subsection (c)(2).

(2) In any case where access to a finding reported under subsection (c) or notification provided under subsection (d)(1) is not made available to all members of a congressional intelligence committee in accordance with subsection (c)(2), the President shall provide to all members of such committee a general description regarding the finding or notification, as applicable, consistent with the reasons for not yet fully informing all members of such committee.

(3) The President shall maintain—

(A) a record of the members of Congress to whom a finding is reported under subsection (c) or notification is provided under subsection (d)(1) and the date on which each member of Congress receives such finding or notification; and

(B) each written statement provided under subsection (c)(5).

(h) For each type of activity undertaken as part of a covert action, the President shall establish in writing a plan to respond to the unauthorized public disclosure of that type of activity.

FUNDING OF INTELLIGENCE ACTIVITIES

SEC. 504. (a) Appropriated funds available to an intelligence agency may be obligated or expended for an intelligence or intelligence-related activity only if—

(1) those funds were specifically authorized by the Congress for use for such activities; or

(2) in the case of funds from the Reserve for Contingencies of the Central Intelligence Agency and consistent with the provisions of section 503 of this Act concerning any significant anticipated intelligence activity, the Director of the Central Intelligence Agency has notified the appropriate congressional committees of the intent to make such funds available for such activity; or

(3) in the case of funds specifically authorized by the Congress for a different activity—

(A) the activity to be funded is a higher priority intelligence or intelligence-related activity;

(B) the use of such funds for such activity supports an emergent need, improves program effectiveness, or increases efficiency; and

(C) the Director of National Intelligence, the Secretary of Defense, or the Attorney General, as appropriate, has notified the appropriate congressional committees of the intent to make such funds available for such activity;

(4) nothing in this subsection prohibits obligation or expenditure of funds available to an intelligence agency in accordance with sections 1535 and 1536 of title 31, United States Code.

(b) Funds available to an intelligence agency may not be made available for any intelligence or intelligence-related activity for which funds were denied by the Congress.

(c) No funds appropriated for, or otherwise available to, any department, agency, or entity of the United States Government may be expended, or may be directed to be expended, for any covert action, as defined in section 503(e), unless and until a Presidential finding required by subsection (a) of section 503 has been signed or otherwise issued in accordance with that subsection.

(d)(1) Except as otherwise specifically provided by law, funds available to an intelligence agency that are not appropriated funds may be obligated or expended for an intelligence or intelligence-related activity only if those funds are used for activities reported to the appropriate congressional committees pursuant to procedures which identify—

(A) the types of activities for which nonappropriated funds may be expended; and

(B) the circumstances under which an activity must be reported as a significant anticipated intelligence activity before such funds can be expended.

(2) Procedures for purposes of paragraph (1) shall be jointly agreed upon by the congressional intelligence committees and, as

appropriate, the Director of National Intelligence or the Secretary of Defense.

(e) As used in this section—

(1) the term "intelligence agency" means any department, agency, or other entity of the United States involved in intelligence or intelligence-related activities;

(2) the term "appropriate congressional committees" means the Permanent Select Committee on Intelligence and the Committee on Appropriations of the House of Representatives and the Select Committee on Intelligence and the Committee on Appropriations of the Senate; and

(3) the term "specifically authorized by the Congress" means that—

(A) the activity and the amount of funds proposed to be used for that activity were identified in a formal budget request to the Congress, but funds shall be deemed to be specifically authorized for that activity only to the extent that the Congress both authorized the funds to be appropriated for that activity and appropriated the funds for that activity; or

(B) although the funds were not formally requested, the Congress both specifically authorized the appropriation of the funds for the activity and appropriated the funds for the activity.

* * * * * * *

REPORTS ON SECURITY CLEARANCES

SEC. 506H. (a) REPORT ON SECURITY CLEARANCE DETERMINATIONS.—(1) Not later than February 1 of each year, the President shall submit to Congress a report on the security clearance process. Such report shall include, for each security clearance level—

(A) the number of employees of the United States Government who—

(i) held a security clearance at such level as of October 1 of the preceding year; and

(ii) were approved for a security clearance at such level during the preceding fiscal year; *and*

(B) the number of contractors to the United States Government who—

(i) held a security clearance at such level as of October 1 of the preceding year; and

(ii) were approved for a security clearance at such level during the preceding fiscal year**[**; and**]**.

[(C) for each element of the intelligence community—

[(i) the total amount of time it took to process the security clearance determination for such level that—

[(I) was among the 80 percent of security clearance determinations made during the preceding fiscal year that took the shortest amount of time to complete; and

[(II) took the longest amount of time to complete;

[(ii) the total amount of time it took to process the security clearance determination for such level that—

[(I) was among the 90 percent of security clearance determinations made during the preceding fiscal year that took the shortest amount of time to complete; and

[(II) took the longest amount of time to complete;

[(iii) the number of pending security clearance investigations for such level as of October 1 of the preceding year that have remained pending for—

[(I) 4 months or less;

[(II) between 4 months and 8 months;

[(III) between 8 months and one year; and

[(IV) more than one year;

[(iv) the percentage of reviews during the preceding fiscal year that resulted in a denial or revocation of a security clearance;

[(v) the percentage of investigations during the preceding fiscal year that resulted in incomplete information;

[(vi) the percentage of investigations during the preceding fiscal year that did not result in enough information to make a decision on potentially adverse information; and

[(vii) for security clearance determinations completed or pending during the preceding fiscal year that have taken longer than one year to complete—

[(I) the number of security clearance determinations for positions as employees of the United States Government that required more than one year to complete;

[(II) the number of security clearance determinations for contractors that required more than one year to complete;

[(III) the agencies that investigated and adjudicated such determinations; and

[(IV) the cause of significant delays in such determinations.]

(2) For purposes of paragraph (1), the President may consider—

(A) security clearances at the level of confidential and secret as one security clearance level; and

(B) security clearances at the level of top secret or higher as one security clearance level.

(b) INTELLIGENCE COMMUNITY REPORTS.—(1) Not later than March 1 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on the security clearances processed by each element of the intelligence community during the preceding fiscal year. Each such report shall separately identify security clearances processed for Federal employees and contractor employees sponsored by each such element.

(2) Each report submitted under paragraph (1) shall include each of the following for each element of the intelligence community for the fiscal year covered by the report:

(A) The total number of initial security clearance background investigations sponsored for new applicants.

(B) The total number of security clearance periodic reinvestigations sponsored for existing employees.

(C) The total number of initial security clearance background investigations for new applicants that were adjudicated with notice of a determination provided to the prospective applicant, including—

(i) the total number that were adjudicated favorably and granted access to classified information; and

(ii) the total number that were adjudicated unfavorably and resulted in a denial or revocation of a security clearance.

(D) The total number of security clearance periodic background investigations that were adjudicated with notice of a determination provided to the existing employee, including—

(i) the total number that were adjudicated favorably; and

(ii) the total number that were adjudicated unfavorably and resulted in a denial or revocation of a security clearance.

(E) The total number of pending security clearance background investigations, including initial applicant investigations and periodic reinvestigations, that were not adjudicated as of the last day of such year and that remained pending as follows:

(i) For 180 days or less.

(ii) For 180 days or longer, but less than 12 months.

(iii) For 12 months or longer, but less than 18 months.

(iv) For 18 months or longer, but less than 24 months.

(v) For 24 months or longer.

(F) In the case of security clearance determinations completed or pending during the year preceding the year for which the report is submitted that have taken longer than 12 months to complete—

(i) an explanation of the causes for the delays incurred during the period covered by the report; and

(ii) the number of such delays involving a polygraph requirement.

(G) The percentage of security clearance investigations, including initial and periodic reinvestigations, that resulted in a denial or revocation of a security clearance.

(H) The percentage of security clearance investigations that resulted in incomplete information.

(I) The percentage of security clearance investigations that did not result in enough information to make a decision on potentially adverse information.

(3) The report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

[(b)**]** *(c)* FORM.—The reports required under **[**subsection (a)(1)**]** *subsections (a)(1) and (b)* shall be submitted in unclassified form, but may include a classified annex.

SUMMARY OF INTELLIGENCE RELATING TO TERRORIST RECIDIVISM OF DETAINEES HELD AT UNITED STATES NAVAL STATION, GUANTANAMO BAY, CUBA

SEC. 506I. (a) IN GENERAL.—The Director of National Intelligence, in consultation with the Director of the Central Intelligence Agency and the Director of the Defense Intelligence Agency, shall make publicly available an unclassified summary of—

(1) intelligence relating to recidivism of detainees currently or formerly held at the Naval Detention Facility at Guantanamo Bay, Cuba, by the Department of Defense; and

(2) an assessment of the likelihood that such detainees will engage in terrorism or communicate with persons in terrorist organizations.

(b) UPDATES.—Not less frequently than [once every 6 months] *annually*, the Director of National Intelligence, in consultation with the Director of the Central Intelligence Agency and the Secretary of Defense, shall update and make publicly available an unclassified summary consisting of the information required by subsection (a) and the number of individuals formerly detained at Naval Station, Guantanamo Bay, Cuba, who are confirmed or suspected of returning to terrorist activities after release or transfer from such Naval Station.

[SEC. 506J. ANNUAL ASSESSMENT OF INTELLIGENCE COMMUNITY PERFORMANCE BY FUNCTION.

[(a) IN GENERAL.—Not later than April 1, 2016, and each year thereafter, the Director of National Intelligence shall, in consultation with the Functional Managers, submit to the congressional intelligence committees a report on covered intelligence functions during the preceding year.

[(b) ELEMENTS.—Each report under subsection (a) shall include for each covered intelligence function for the year covered by such report the following:

[(1) An identification of the capabilities, programs, and activities of such intelligence function, regardless of the element of the intelligence community that carried out such capabilities, programs, and activities.

[(2) A description of the investment and allocation of resources for such intelligence function, including an analysis of the allocation of resources within the context of the National Intelligence Strategy, priorities for recipients of resources, and areas of risk.

[(3) A description and assessment of the performance of such intelligence function.

[(4) An identification of any issues related to the application of technical interoperability standards in the capabilities, programs, and activities of such intelligence function.

[(5) An identification of the operational overlap or need for de-confliction, if any, within such intelligence function.

[(6) A description of any efforts to integrate such intelligence function with other intelligence disciplines as part of an integrated intelligence enterprise.

[(7) A description of any efforts to establish consistency in tradecraft and training within such intelligence function.

[(8) A description and assessment of developments in technology that bear on the future of such intelligence function.

[(9) Such other matters relating to such intelligence function as the Director may specify for purposes of this section.

[(c) DEFINITIONS.—In this section:

[(1) The term "covered intelligence functions" means each intelligence function for which a Functional Manager has been established under section 103J during the year covered by a report under this section.

[(2) The term "Functional Manager" means the manager of an intelligence function established under section 103J.]

* * * * * * *

SEC. 511. ANNUAL REPORT ON VIOLATIONS OF LAW OR EXECUTIVE ORDER.

(a) ANNUAL REPORTS REQUIRED.—[The Director of National Intelligence] *The head of each element of the intelligence community* shall annually submit to the congressional intelligence committees a report on violations of law or executive order relating to intelligence activities by personnel of [an element] *the element* of the intelligence community that were identified during the previous calendar year.

(b) ELEMENTS.—Each report submitted under subsection (a) shall, consistent with the need to preserve ongoing criminal investigations, include a description of, and any action taken in response to, any violation of law or executive order (including Executive Order No. 12333 (50 U.S.C. 3001 note)) relating to intelligence activities committed by personnel of an element of the intelligence community in the course of the employment of such personnel that, during the previous calendar year, was—

(1) determined by the director, head, or general counsel of any element of the intelligence community to have occurred;

(2) referred to the Department of Justice for possible criminal prosecution; or

(3) substantiated by the inspector general of any element of the intelligence community.

SEC. 512. UNFUNDED PRIORITIES OF THE INTELLIGENCE COMMUNITY.

(a) BRIEFINGS.—Upon the request of an appropriate congressional committee, the Director of National Intelligence shall provide to the committee a briefing on the unfunded priorities of an element of the intelligence community.

(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 Appropriations of the House of Representatives and the Senate.

(2) UNFUNDED PRIORITY.—The term "unfunded priority", in the case of a fiscal year, means a program, activity, or other initiative of an element of the intelligence community that—

(A) was submitted by the head of the element to the Director of National Intelligence in the budget proposal for the element for that fiscal year, but was not included by the Director in the consolidated budget proposal submitted to the President for that fiscal year; or

(B) was submitted by the Director in the consolidated budget proposal submitted to the President for that fiscal year, but was not included in the budget of the President submitted to Congress for that fiscal year pursuant to section 1105 of title 31, United States Code.

SEC. 513. BRIEFINGS AND NOTIFICATIONS ON COUNTERINTELLIGENCE ACTIVITIES OF THE FEDERAL BUREAU OF INVESTIGATION.

(a) QUARTERLY BRIEFINGS.—In addition to, and without any derogation of, the requirement under section 501 to keep the congressional intelligence committees fully and currently informed of the intelligence and counterintelligence activities of the United States, not less frequently than once each quarter, the Director of the Federal Bureau of Investigation shall provide to the congressional intelligence committees a briefing on the counterintelligence activities of the Federal Bureau of Investigation. Such briefings shall include, at a minimum, an overview and update of—

(1) the counterintelligence posture of the Bureau;

(2) counterintelligence investigations; and

(3) any other information relating to the counterintelligence activities of the Bureau that the Director determines necessary.

(b) NOTIFICATIONS.—In addition to the quarterly briefings under subsection (a), the Director of the Federal Bureau of Investigation shall promptly notify the congressional intelligence committees of any counterintelligence investigation carried out by the Bureau with respect to any counterintelligence risk or threat that is related to an election or campaign for Federal office.

(c) GUIDELINES.—

(1) DEVELOPMENT AND CONSULTATION.—The Director shall develop guidelines governing the scope of the briefings provided under subsection (a), the notifications provided under subsection (b), and the information required by section 308(a)(2) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020. The Director shall consult the congressional intelligence committees during such development.

(2) SUBMISSION.—The Director shall submit to the congressional intelligence committees—

(A) the guidelines under paragraph (1) upon issuance; and

(B) any updates to such guidelines by not later than 15 days after making such update.

TITLE VI—PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION

* * * * * * *

DEFINITIONS

SEC. 605. For the purposes of this title:

(1) The term "classified information" means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

(2) The term "authorized", when used with respect to access to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities,

order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.

(3) The term "disclose" means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

(4) The term "covert agent" means—

(A) a present or retired officer or employee of an intelligence agency or a present or retired member of the Armed Forces assigned to duty with an intelligence [agency—]

[(i) whose identity] *agency whose identity* as such an officer, employee, or member is classified information[, and]*;*

[(ii) who is serving outside the United States or has within the last five years served outside the United States; or]

(B) a United States citizen whose intelligence relationship to the United States is classified information, and—

(i) who [resides and acts outside the United States] *acts* as an agent of, or informant or source of operational assistance to, an intelligence agency, or

(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

(5) The term "intelligence agency" means the elements of the intelligence community, as that term is defined in section 3(4).

(6) The term "informant" means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

(7) The terms "officer" and "employee" have the meanings given such terms by section 2104 and 2105, respectively, of title 5, United States Code.

(8) The term "Armed Forces" means the Army, Navy, Air Force, Marine Corps, and Coast Guard.

(9) The term "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(10) The term "pattern of activities" requires a series of acts with a common purpose or objective.

* * * * * * *

TITLE VIII—ACCESS TO CLASSIFIED INFORMATION

* * * * * * *

SEC. 803. SECURITY EXECUTIVE AGENT.

(a) IN GENERAL.—The Director of National Intelligence, or such other officer of the United States as the President may designate, shall serve as the Security Executive Agent for all departments and agencies of the United States.

(b) DUTIES.—The duties of the Security Executive Agent are as follows:

(1) To direct the oversight of investigations, reinvestigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information or eligibility to hold a sensitive position made by any Federal agency.

(2) To review the national security background investigation and adjudication programs of Federal agencies to determine whether such programs are being implemented in accordance with this section.

(3) To develop and issue uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations, polygraphs, and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position.

(4) Unless otherwise designated by law, to serve as the final authority to designate a Federal agency or agencies to conduct investigations of persons who are proposed for access to classified information or for eligibility to hold a sensitive position to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position, as applicable.

(5) Unless otherwise designated by law, to serve as the final authority to designate a Federal agency or agencies to determine eligibility for access to classified information or eligibility to hold a sensitive position in accordance with Executive Order 12968 (50 U.S.C. 3161 note; relating to access to classified information).

(6) To ensure reciprocal recognition of eligibility for access to classified information or eligibility to hold a sensitive position among Federal agencies, including acting as the final authority to arbitrate and resolve disputes among such agencies involving the reciprocity of investigations and adjudications of eligibility.

(7) To execute all other duties assigned to the Security Executive Agent by law.

(c) AUTHORITIES.—The Security Executive Agent shall—

(1) issue guidelines and instructions to the heads of Federal agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and security in processes relating to determinations by such agencies of eligibility for access to classified information or eligibility to hold a sensitive position, including such matters as investigations, polygraphs, adjudications, and reciprocity;

(2) have the authority to grant exceptions to, or waivers of, national security investigative requirements, including issuing implementing or clarifying guidance, as necessary;

(3) have the authority to assign, in whole or in part, to the head of any Federal agency (solely or jointly) any of the duties of the Security Executive Agent described in subsection (b) or the authorities described in paragraphs (1) and (2), provided

that the exercise of such assigned duties or authorities is subject to the oversight of the Security Executive Agent, including such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate; and

(4) define and set standards for continuous evaluation for continued access to classified information and for eligibility to hold a sensitive position.

EXCEPTIONS

SEC. [803.] *804.* Except as otherwise specifically provided, the provisions of this title shall not apply to the President and Vice President, Members of the Congress, Justices of the Supreme Court, and Federal judges appointed by the President.

DEFINITIONS

SEC. [804.] *805.* For purposes of this title—

(1) the term "authorized investigative agency" means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigations of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information;

(2) the term "classified information" means any information that has been determined pursuant to Executive Order No. 12356 of April 2, 1982, or successor orders, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and that is so designated;

(3) the term "consumer reporting agency" has the meaning given such term in section 603 of the Consumer Credit Protection Act (15 U.S.C. 1681a);

(4) the term "employee" includes any person who receives a salary or compensation of any kind from the United States Government, is a contractor of the United States Government or an employee thereof, is an unpaid consultant of the United States Government, or otherwise acts for or on behalf of the United States Government, except as otherwise determined by the President;

(5) the terms "financial agency" and "financial institution" have the meanings given to such terms in section 5312(a) of title 31, United States Code, and the term "holding company" has the meaning given to such term in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

(6) the terms "foreign power" and "agent of a foreign power" have the same meanings as set forth in sections 101 (a) and (b), respectively, of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

(7) the term "State" means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, the Republic of the Marshall Islands, the Federated States of Micronesia, and the Republic of Palau, and any other possession of the United States; and

(8) the term "computer" means any electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device and any data or other information stored or contained in such device.

* * * * * * *

TITLE XI—ADDITIONAL MISCELLANEOUS PROVISIONS

* * * * * * *

SEC. 1105. SEMIANNUAL REPORTS ON INVESTIGATIONS OF UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION.

(a) DEFINITIONS.—In this section:

(1) COVERED OFFICIAL.—The term "covered official" means—

(A) the heads of each element of the intelligence community; and

(B) the inspectors general with oversight responsibility for an element of the intelligence community.

(2) INVESTIGATION.—The term "investigation" means any inquiry, whether formal or informal, into the existence of an unauthorized public disclosure of classified information.

(3) UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION.—The term "unauthorized disclosure of classified information" means any unauthorized disclosure of classified information to any recipient.

(4) UNAUTHORIZED PUBLIC DISCLOSURE OF CLASSIFIED INFORMATION.—The term "unauthorized public disclosure of classified information" means the unauthorized disclosure of classified information to a journalist or media organization.

(b) INTELLIGENCE COMMUNITY REPORTING.—

(1) IN GENERAL.—Not less frequently than once every 6 months, each covered official shall submit to the congressional intelligence committees a report on investigations of unauthorized public disclosures of classified information.

(2) ELEMENTS.—Each report submitted under paragraph (1) shall include, with respect to the preceding 6-month period, the following:

(A) The number of investigations opened by the covered official regarding an unauthorized public disclosure of classified information.

(B) The number of investigations completed by the covered official regarding an unauthorized public disclosure of classified information.

(C) Of the number of such completed investigations identified under subparagraph (B), the number referred to the Attorney General for criminal investigation.

(c) DEPARTMENT OF JUSTICE REPORTING.—

(1) IN GENERAL.—Not less frequently than once every 6 months, the Assistant Attorney General for National Security of the Department of Justice, in consultation with the Director of the Federal Bureau of Investigation, shall submit to the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the

House of Representatives a report on the status of each referral made to the Department of Justice from any element of the intelligence community regarding an unauthorized disclosure of classified information made during the most recent 365-day period or any referral that has not yet been closed, regardless of the date the referral was made.

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

(A) The date the referral was received.

(B) A statement indicating whether the alleged unauthorized disclosure described in the referral was substantiated by the Department of Justice.

(C) A statement indicating the highest level of classification of the information that was revealed in the unauthorized disclosure.

(D) A statement indicating whether an open criminal investigation related to the referral is active.

(E) A statement indicating whether any criminal charges have been filed related to the referral.

(F) A statement indicating whether the Department of Justice has been able to attribute the unauthorized disclosure to a particular entity or individual.

(d) FORM OF REPORTS.—Each report submitted under this section shall be submitted in unclassified form, but may have a classified annex.

SEC. 1106. ANNUAL REPORTS ON INFLUENCE OPERATIONS AND CAMPAIGNS IN THE UNITED STATES BY THE COMMUNIST PARTY OF CHINA.

(a) REQUIREMENT.—On an annual basis, the Director of the National Counterintelligence and Security Center shall submit to the congressional intelligence committees a report on the influence operations and campaigns in the United States conducted by the Communist Party of China.

(b) CONTENTS.—Each report under subsection (a) shall include the following:

(1) A description of the organization of the United Front Work Department of the People's Republic of China, or the successors of the United Front Work Department, and the links between the United Front Work Department and the Central Committee of the Communist Party of China.

(2) An assessment of the degree to which organizations that are associated with or receive funding from the United Front Work Department, particularly such entities operating in the United States, are formally tasked by the Chinese Communist Party or the Government of China.

(3) A description of the efforts by the United Front Work Department and subsidiary organizations of the United Front Work Department to target, coerce, and influence foreign populations, particularly those of ethnic Chinese descent.

(4) An assessment of attempts by the Chinese Embassy, consulates, and organizations affiliated with the Chinese Communist Party (including, at a minimum, the United Front Work Department) to influence the United States-based Chinese Student Scholar Associations.

(5) A description of the evolution of the role of the United Front Work Department under the leadership of the President of China.

(6) An assessment of the activities of the United Front Work Department designed to influence the opinions of elected leaders of the United States, or candidates for elections in the United States, with respect to issues of importance to the Chinese Communist Party.

(7) A listing of all known organizations affiliated with the United Front Work Department that are operating in the United States as of the date of the report.

(8) With respect to reports submitted after the first report, an assessment of the change in goals, tactics, techniques, and procedures of the influence operations and campaigns conducted by the Chinese Communist Party.

(c) COORDINATION.—In carrying out subsection (a), the Director shall coordinate with the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, the Director of the National Security Agency, and any other relevant head of an element of the intelligence community.

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

TITLE 10, UNITED STATES CODE

* * * * * * *

SUBTITLE A—GENERAL MILITARY LAW

* * * * * * *

PART III—TRAINING AND EDUCATION

* * * * * * *

CHAPTER 108—DEPARTMENT OF DEFENSE SCHOOLS

Sec.
[2161. Degree granting authority for National Intelligence University.]

* * * * * * *

[§ 2161. Degree granting authority for National Intelligence University

[(a) AUTHORITY.—Under regulations prescribed by the Secretary of Defense, the President of the National Intelligence University may, upon the recommendation of the faculty of the National Intelligence University, confer appropriate degrees upon graduates who meet the degree requirements.

[(b) LIMITATION.—A degree may not be conferred under this section unless—

[(1) the Secretary of Education has recommended approval of the degree in accordance with the Federal Policy Governing Granting of Academic Degrees by Federal Agencies; and

[(2) the National Intelligence University is accredited by the appropriate civilian academic accrediting agency or organiza-

tion to award the degree, as determined by the Secretary of Education.

[(c) CONGRESSIONAL NOTIFICATION REQUIREMENTS.—(1) When seeking to establish degree granting authority under this section, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and House of Representatives—

[(A) a copy of the self assessment questionnaire required by the Federal Policy Governing Granting of Academic Degrees by Federal Agencies, at the time the assessment is submitted to the Department of Education's National Advisory Committee on Institutional Quality and Integrity; and

[(B) the subsequent recommendations and rationale of the Secretary of Education regarding the establishment of the degree granting authority.

[(2) Upon any modification or redesignation of existing degree granting authority, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and House of Representatives a report containing the rationale for the proposed modification or redesignation and any subsequent recommendation of the Secretary of Education on the proposed modification or redesignation.

[(3) The Secretary of Defense shall submit to the Committees on Armed Services of the Senate and House of Representatives a report containing an explanation of any action by the appropriate academic accrediting agency or organization not to accredit the National Intelligence University to award any new or existing degree.]

* * * * * * *

SUPPLEMENTAL APPROPRIATIONS ACT, 2009

* * * * * * *

TITLE III

DEPARTMENT OF DEFENSE

* * * * * * *

(INCLUDING TRANSFER OF FUNDS)

* * * * * * *

SEC. 319. (a) REPORTS REQUIRED.—Not later than 60 days after the date of the enactment of this Act and [every 90 days] *annually* thereafter, the President shall submit to the members and committees of Congress specified in subsection (b) a report on the prisoner population at the detention facility at Naval Station Guantanamo Bay, Cuba.

(b) SPECIFIED MEMBERS AND COMMITTEES OF CONGRESS.—The members and committees of Congress specified in this subsection are the following:

(1) The majority leader and minority leader of the Senate.

(2) The Chairman and Ranking Member on the Committee on Armed Services of the Senate.

(3) The Chairman and Vice Chairman of the Select Committee on Intelligence of the Senate.

(4) The Chairman and Vice Chairman of the Committee on Appropriations of the Senate.

(5) The Speaker of the House of Representatives.

(6) The minority leader of the House of Representatives.

(7) The Chairman and Ranking Member on the Committee on Armed Services of the House of Representatives.

(8) The Chairman and Vice Chairman of the Permanent Select Committee on Intelligence of the House of Representatives.

(9) The Chairman and Ranking Member of the Committee on Appropriations of the House of Representatives.

(c) MATTERS TO BE INCLUDED.—Each report submitted under subsection (a) shall include the following:

(1) The name and country of origin of each detainee at the detention facility at Naval Station Guantanamo Bay, Cuba, as of the date of such report.

(2) A current summary of the evidence, intelligence, and information used to justify the detention of each detainee listed under paragraph (1) at Naval Station Guantanamo Bay.

(3) A current accounting of all the measures taken to transfer each detainee listed under paragraph (1) to the individual's country of citizenship or another country.

(4) A current description of the number of individuals released or transferred from detention at Naval Station Guantanamo Bay who are confirmed or suspected of returning to terrorist activities after release or transfer from Naval Station Guantanamo Bay.

(5) An assessment of any efforts by al Qaeda to recruit detainees released from detention at Naval Station Guantanamo Bay.

(6) A summary of all known contact between any individual formerly detained at Naval Station Guantanamo Bay and any individual known or suspected to be associated with a foreign terrorist group, which contact included information or discussion about planning for or conduct of hostilities against the United States or its allies or the organizational, logistical, or resource needs or activities of any terrorist group or activity.

(7) For each individual described in paragraph (4), the date on which such individual was released or transferred from Naval Station Guantanamo Bay and the date on which it is confirmed that such individual is suspected or confirmed of reengaging in terrorist activities.

(8) The average period of time described in paragraph (7) for all the individuals described in paragraph (4).

(d) ADDITIONAL MATTERS TO BE INCLUDED IN INITIAL REPORT.—The first report submitted under subsection (a) shall also include the following:

(1) A description of the process that was previously used for screening the detainees described by subsection (c)(4) prior to their release or transfer from detention at Naval Station Guantanamo Bay, Cuba.

(2) An assessment of the adequacy of that screening process for reducing the risk that detainees previously released or transferred from Naval Station Guantanamo Bay would return to terrorist activities after release or transfer from Naval Station Guantanamo Bay.

(3) An assessment of lessons learned from previous releases and transfers of individuals who returned to terrorist activities for reducing the risk that detainees released or transferred from Naval Station Guantanamo Bay will return to terrorist activities after their release or transfer.

* * * * * * *

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2017

* * * * * * *

DIVISION N—INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2017

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This division may be cited as the "Intelligence Authorization Act for Fiscal Year 2017".

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

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

* * * * * * *

SEC. 308. GUIDANCE AND REPORTING REQUIREMENT REGARDING THE INTERACTIONS BETWEEN THE INTELLIGENCE COMMUNITY AND ENTERTAINMENT INDUSTRY.

(a) DEFINITIONS.—In this section:

(1) ENGAGEMENT.—The term "engagement"—

(A) means any significant interaction between an element of the intelligence community and an entertainment industry entity for the purposes of contributing to an entertainment product intended to be heard, read, viewed, or otherwise experienced by the public; and

(B) does not include routine inquiries made by the press or news media to the public affairs office of an intelligence community.

(2) ENTERTAINMENT INDUSTRY ENTITY.—The term "entertainment industry entity" means an entity that creates, produces, promotes, or distributes a work of entertainment intended to

be heard, read, viewed, or otherwise experienced by an audience, including—

(A) theater productions, motion pictures, radio broadcasts, television broadcasts, podcasts, webcasts, other sound or visual recording, music, or dance;

(B) books and other published material; and

(C) such other entertainment activity, as determined by the Director of National Intelligence.

(b) DIRECTOR OF NATIONAL INTELLIGENCE GUIDANCE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall issue, and release to the public, guidance regarding engagements by elements of the intelligence community with entertainment industry entities.

(2) CRITERIA.—The guidance required by paragraph (1) shall—

(A) permit an element of the intelligence community to conduct engagements, if the head of the element, or a designee of such head, provides prior approval; and

(B) require an unclassified annual report to the congressional intelligence committees regarding engagements.

[(c) ANNUAL REPORT.—Each report required by subsection (b)(2)(B) shall include the following:

[(1) A description of the nature and duration of each engagement included in the review.

[(2) The cost incurred by the United States Government for each such engagement.

[(3) A description of the benefits to the United States Government for each such engagement.

[(4) A determination of whether any information was declassified, and whether any classified information was improperly disclosed, or each such engagement.

[(5) A description of the work produced through each such engagement.]

* * * * * * *

SEC. 311. NOTIFICATION OF MEMORANDA OF UNDERSTANDING.

[(a) IN GENERAL.—The head of each element of the intelligence community shall submit to the congressional intelligence committees a copy of each memorandum of understanding or other agreement regarding significant operational activities or policy between or among such element and any other entity or entities of the United States Government—

[(1) for such a memorandum or agreement that is in effect on the date of the enactment of this Act, not later than 60 days after such date; and

[(2) for such a memorandum or agreement entered into after such date, in a timely manner and not more than 60 days after the date such memorandum or other agreement is entered into.]

(a) IN GENERAL.—Each year, concurrent with the annual budget request submitted by the President to Congress under section 1105 of title 31, United States Code, each head of an element of the intelligence community shall submit to the congressional intelligence committees a report that lists each memorandum of understanding

or other agreement regarding significant operational activities or policy entered into during the most recently completed fiscal year between or among such element and any other entity of the United States Government.

(b) PROVISION OF DOCUMENTS.—Each head of an element of an intelligence community who receives a request from the Select Committee on Intelligence of the Senate or the Permanent Select Committee on Intelligence of the House of Representatives for a copy of a memorandum of understanding or other document listed in a report submitted by the head under subsection (a) shall submit to such committee the requested copy as soon as practicable after receiving such request.

[(b)**]** *(c)* ADMINISTRATIVE MEMORANDUM OR AGREEMENT.—Nothing in this section may be construed to require an element of the intelligence community to submit to the congressional intelligence committees any memorandum or agreement that is solely administrative in nature, including a memorandum or agreement regarding joint duty or other routine personnel assignments.

* * * * * * *

TITLE V—MATTERS RELATING TO FOREIGN COUNTRIES

SEC. 501. COMMITTEE TO COUNTER ACTIVE MEASURES BY THE RUSSIAN FEDERATION, *THE PEOPLE'S REPUBLIC OF CHINA, THE ISLAMIC REPUBLIC OF IRAN, THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA, OR OTHER NATION STATE* TO EXERT COVERT INFLUENCE OVER PEOPLES AND GOVERNMENTS.

(a) DEFINITIONS.—In this section:

(1) ACTIVE MEASURES BY RUSSIA TO EXERT COVERT INFLUENCE.—The term "active measures by Russia*, China, Iran, North Korea, or other nation state* to exert covert influence" means activities intended to influence a person or government that are carried out in coordination with, or at the behest of, political leaders or the security services of the Russian Federation*, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state* and the role of the Russian Federation*, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state* has been hidden or not acknowledged publicly, including the following:

(A) Establishment or funding of a front group.
(B) Covert broadcasting.
(C) Media manipulation.
(D) Disinformation and forgeries.
(E) Funding agents of influence.
(F) Incitement and offensive counterintelligence.
(G) Assassinations.
(H) Terrorist acts.

(2) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means—

(A) the congressional intelligence committees;

(B) the Committee on Armed Services and the Committee on Foreign Relations of the Senate; and

(C) the Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives.

(b) ESTABLISHMENT.—There is established within the executive branch an interagency committee to counter active measures by the Russian Federation*, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state* to exert covert influence.

(c) MEMBERSHIP.—

(1) IN GENERAL.—

(A) APPOINTMENT.—Each head of an agency or department of the Government set out under subparagraph (B) shall appoint one member of the committee established by subsection (b) from among officials of such agency or department who occupy a position that is required to be appointed by the President, with the advice and consent of the Senate.

(B) HEAD OF AN AGENCY OR DEPARTMENT.—The head of an agency or department of the Government set out under this subparagraph are the following:

(i) The Director of National Intelligence.

(ii) The Secretary of State.

(iii) The Secretary of Defense.

(iv) The Secretary of the Treasury.

(v) The Attorney General.

(vi) The Secretary of Energy.

(vii) The Director of the Federal Bureau of Investigation.

(viii) The head of any other agency or department of the United States Government designated by the President for purposes of this section.

(d) MEETINGS.—The committee shall meet on a regular basis.

(e) DUTIES.—The duties of the committee established by subsection (b) shall be as follows:

(1) To counter active measures by Russia*, China, Iran, North Korea, or other nation state* to exert covert influence, including by exposing falsehoods, agents of influence, corruption, human rights abuses, terrorism, and assassinations carried out by the security services or political elites of the Russian Federation*, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state* or their proxies.

(2) Such other duties as the President may designate for purposes of this section.

(f) STAFF.—The committee established by subsection (b) may employ such staff as the members of such committee consider appropriate.

(g) BUDGET REQUEST.—A request for funds required for the functioning of the committee established by subsection (b) may be included in each budget for a fiscal year submitted by the President pursuant to section 1105(a) of title 31, United States Code.

(h) ANNUAL REPORT.—

(1) REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, and con-

sistent with the protection of intelligence sources and methods, the committee established by subsection (b) shall submit to the appropriate committees of Congress a report describing steps being taken by the committee to counter active measures by Russia*, China, Iran, North Korea, or other nation state* to exert covert influence.

(2) CONTENT.—Each report required by paragraph (1) shall include the following:

(A) A summary of the active measures by the Russian Federation*, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state* to exert covert influence during the previous year, including significant incidents and notable trends.

(B) A description of the key initiatives of the committee.

(C) A description of the implementation of the committee's initiatives by the head of an agency or department of the Government set out under subsection (c)(1)(B).

(D) An analysis of the impact of the committee's initiatives.

(E) Recommendations for changes to the committee's initiatives from the previous year.

(3) SEPARATE REPORTING REQUIREMENT.—The requirement to submit an annual report under paragraph (1) is in addition to any other reporting requirements with respect to Russia*, China, Iran, North Korea, or other nation state*.

SEC. 502. STRICT ENFORCEMENT OF TRAVEL PROTOCOLS AND PROCEDURES OF ACCREDITED DIPLOMATIC AND CONSULAR PERSONNEL OF THE RUSSIAN FEDERATION IN THE UNITED STATES.

(a) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term "appropriate committees of Congress" means—

(1) the congressional intelligence committees;

(2) the Committee on Foreign Relations and the Committee on the Judiciary of the Senate; and

(3) the Committee on Foreign Affairs and the Committee on the Judiciary of the House of Representatives.

(b) ADVANCE NOTIFICATION REQUIREMENT.—The Secretary of State shall, in coordination with the Director of the Federal Bureau of Investigation and the Director of National Intelligence, establish a mandatory advance notification regime governing all travel by accredited diplomatic and consular personnel of the Russian Federation in the United States and take necessary action to secure full compliance by Russian personnel and address any noncompliance.

(c) INTERAGENCY COOPERATION.—The Secretary of State, the Director of the Federal Bureau of Investigation, and the Director of National Intelligence shall develop written mechanisms to share information—

(1) on travel by accredited diplomatic and consular personnel of the Russian Federation who are in the United States; and

(2) on any known or suspected noncompliance by such personnel with the regime required by subsection (b).

(d) QUARTERLY REPORTS.—Not later than 90 days after the date of the enactment of this Act, and quarterly thereafter, and consistent with the protection of intelligence sources and methods—

(1) the Secretary of State shall submit to the appropriate committees of Congress a written report detailing the number of notifications submitted under the regime required by subsection (b); and

(2) the Secretary of State and the Director of the Federal Bureau of Investigation shall jointly submit to the appropriate committees of Congress a written report detailing [the number] *a best estimate* of known or suspected violations of such requirements by any accredited diplomatic and consular personnel of the Russian Federation.

* * * * * * *

TITLE VI—REPORTS AND OTHER MATTERS

[SEC. 601. DECLASSIFICATION REVIEW WITH RESPECT TO DETAINEES TRANSFERRED FROM UNITED STATES NAVAL STATION, GUANTANAMO BAY, CUBA.

[(a) IN GENERAL.—For each individual detained at United States Naval Station, Guantanamo Bay, Cuba, who was transferred or released from United States Naval Station, Guantanamo Bay, Cuba, the Director of National Intelligence shall—

[(1)(A) complete a declassification review of intelligence reports regarding past terrorist activities of that individual prepared by the National Counterterrorism Center for the individual's Periodic Review Board sessions, transfer, or release; or

[(B) if the individual's transfer or release occurred prior to the date on which the National Counterterrorism Center first began to prepare such reports regarding detainees, such other intelligence report or reports that contain the same or similar information regarding the individual's past terrorist activities;

[(2) make available to the public—

[(A) any intelligence reports declassified as a result of the declassification review; and

[(B) with respect to each individual transferred or released, for whom intelligence reports are declassified as a result of the declassification review, an unclassified summary which shall be prepared by the President of measures being taken by the country to which the individual was transferred or released to monitor the individual and to prevent the individual from carrying out future terrorist activities; and

[(3) submit to the congressional intelligence committees a report setting out the results of the declassification review, including a description of intelligence reports covered by the review that were not declassified.

[(b) SCHEDULE.—

[(1) TRANSFER OR RELEASE PRIOR TO ENACTMENT.—Not later than 210 days after the date of the enactment of this Act, the Director of National Intelligence shall submit the report required by subsection (a)(3), which shall include the results of the declassification review completed for each individual detained at United States Naval Station, Guantanamo Bay, Cuba, who was transferred or released from United States

Naval Station, Guantanamo Bay, prior to the date of the enactment of this Act.

[(2) TRANSFER OR RELEASE AFTER ENACTMENT.—Not later than 120 days after the date an individual detained at United States Naval Station, Guantanamo Bay, on or after the date of the enactment of this Act is transferred or released from United States Naval Station, Guantanamo Bay, the Director shall submit the report required by subsection (a)(3) for such individual.

[(c) PAST TERRORIST ACTIVITIES.—For purposes of this section, the past terrorist activities of an individual shall include all terrorist activities conducted by the individual before the individual's transfer to the detention facility at United States Naval Station, Guantanamo Bay, including, at a minimum, the following:

[(1) The terrorist organization, if any, with which affiliated.

[(2) The terrorist training, if any, received.

[(3) The role in past terrorist attacks against United States interests or allies.

[(4) The direct responsibility, if any, for the death of United States citizens or members of the Armed Forces.

[(5) Any admission of any matter specified in paragraphs (1) through (4).

[(6) A description of the intelligence supporting any matter specified in paragraphs (1) through (5), including the extent to which such intelligence was corroborated, the level of confidence held by the intelligence community, and any dissent or reassessment by an element of the intelligence community.]

* * * * * * *

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

* * * * * * *

TITLE I—REFORM OF THE INTELLIGENCE COMMUNITY

* * * * * * *

SEC. 1016. INFORMATION SHARING.

(a) DEFINITIONS.—In this section:

(1) HOMELAND SECURITY INFORMATION.—The term "homeland security information" has the meaning given that term in section 892(f) of the Homeland Security Act of 2002 (6 U.S.C. 482(f)).

(2) INFORMATION SHARING COUNCIL.—The term "Information Sharing Council" means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).

(3) INFORMATION SHARING ENVIRONMENT.—The terms "information sharing environment" and "ISE" mean an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.

(4) PROGRAM MANAGER.—The term "program manager" means the program manager designated under subsection (f).

(5) TERRORISM INFORMATION.—The term "terrorism information"—

(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

(ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(iii) communications of or by such groups or individuals; or

(iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(B) includes weapons of mass destruction information.

(6) WEAPONS OF MASS DESTRUCTION INFORMATION.—The term "weapons of mass destruction information" means information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

(b) INFORMATION SHARING ENVIRONMENT.—

(1) ESTABLISHMENT.—The [President] *Director of National Intelligence* shall—

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) ATTRIBUTES.—The [President] *Director of National Intelligence* shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The [President] *Director of National Intelligence* shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that—

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties;

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;

(J) integrates the information within the scope of the information sharing environment, including any such information in legacy technologies;

(K) integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the Federal, State, and local levels;

(L) allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;

(M) permits analysts to collaborate both independently and in a group (commonly known as "collective and non-collective collaboration"), and across multiple levels of national security information and controlled unclassified information;

(N) provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and

(O) incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.

(c) PRELIMINARY REPORT.—Not later than 180 days after the date of the enactment of this Act, the program manager shall, in consultation with the Information Sharing Council—

(1) submit to the President and Congress a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed;

(2) establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism informa-

tion and people with relevant knowledge about intelligence and terrorism information; and

(3) conduct a review of relevant current Federal agency capabilities, databases, and systems for sharing information.

(d) GUIDELINES AND REQUIREMENTS.—As soon as possible, but in no event later than 270 days after the date of the enactment of this Act, the President shall—

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, issue guidelines that—

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by—

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

(e) IMPLEMENTATION PLAN REPORT.—Not later than one year after the date of the enactment of this Act, the President shall, with the assistance of the program manager, submit to Congress a report containing an implementation plan for the ISE. The report shall include the following:

(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.

(2) A description of the impact on enterprise architectures of participating agencies.

(3) A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE.

(5) The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized.

(6) Objective, systemwide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.

(9) The recommendations of the program manager, in consultation with the Information Sharing Council, regarding

whether, and under what conditions, the ISE should be expanded to include other intelligence information.

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with—

(A) the authority of the Director of National Intelligence under this title, and the amendments made by this title, to set standards for information sharing throughout the intelligence community; and

(B) the authority of the Secretary of Homeland Security and the Attorney General, and the role of the Department of Homeland Security and the Department of Justice, in coordinating with State, local, and tribal officials and the private sector.

(11) The recommendations of the program manager, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of program manager should continue to remain in existence.

(f) PROGRAM MANAGER.—

(1) DESIGNATION.—Not later than 120 days after the date of the enactment of this Act, with notification to Congress, the President shall designate an individual as the program manager responsible for information sharing across the Federal Government. [The individual designated as the program manager shall serve as program manager until removed from service or replaced by the President (at the President's sole discretion).] *Beginning on the date of the enactment of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019 and 2020, each individual designated as the program manager shall be appointed by the Director of National Intelligence.* The program manager, in consultation with the head of any affected department or agency, shall have and exercise governmentwide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments, agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law.

(2) DUTIES AND RESPONSIBILITIES.—

(A) IN GENERAL.—The program manager shall, in consultation with the Information Sharing Council—

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, as appropriate, to foster the development and proper operation of the ISE;

(iii) consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and

Budget, issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE;

(iv) identify and resolve information sharing disputes between Federal departments, agencies, and components; and

(v) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

(B) CONTENT OF POLICIES, PROCEDURES, GUIDELINES, RULES, AND STANDARDS.—The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall—

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

(g) INFORMATION SHARING COUNCIL.—

(1) ESTABLISHMENT.—There is established an Information Sharing Council that shall assist the President and the program manager in their duties under this section. The Information Sharing Council shall serve until removed from service or replaced by the President (at the sole discretion of the President) with a successor body.

(2) SPECIFIC DUTIES.—In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall—

(A) advise the President and the program manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE;

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address any gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments;

(G) assist the program manager in identifying and resolving information sharing disputes between Federal departments, agencies, and components;

(H) identify appropriate personnel for assignment to the program manager to support staffing needs identified by the program manager; and

(I) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

(3) CONSULTATION.—In performing its duties, the Information Sharing Council shall consider input from persons and entities outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

(4) INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—The Information Sharing Council (including any subsidiary group of the Information Sharing Council) shall not be subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App.).

(5) DETAILEES.—Upon a request by the Director of National Intelligence, the departments and agencies represented on the Information Sharing Council shall detail to the program manager, on a reimbursable basis, appropriate personnel identified under paragraph (2)(H).

(h) PERFORMANCE MANAGEMENT REPORTS.—

(1) IN GENERAL.—Not later than two years after the date of the enactment of this Act, and not later than June 30 of each year thereafter, the President shall submit to Congress a report on the state of the ISE and of information sharing across the Federal Government.

(2) CONTENT.—Each report under this subsection shall include—

(A) a progress report on the extent to which the ISE has been implemented, including how the ISE has fared on the performance measures and whether the performance goals set in the preceding year have been met;

(B) objective system-wide performance goals for the following year;

(C) an accounting of how much was spent on the ISE in the preceding year;

(D) actions taken to ensure that procurement of and investments in systems and technology are consistent with the implementation plan for the ISE;

(E) the extent to which all terrorism watch lists are available for combined searching in real time through the ISE and whether there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors;

(F) the extent to which State, tribal, and local officials are participating in the ISE;

(G) the extent to which private sector data, including information from owners and operators of critical infrastructure, is incorporated in the ISE, and the extent to which individuals and entities outside the government are receiving information through the ISE;

(H) the measures taken by the Federal government to ensure the accuracy of information in the ISE, in particular the accuracy of information about individuals;

(I) an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections; and

(J) an assessment of the security protections used in the ISE.

(i) AGENCY RESPONSIBILITIES.—The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall—

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing; and

(4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

(j) REPORT ON THE INFORMATION SHARING ENVIRONMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the President shall report to the Committee on Homeland Security and Governmental Affairs of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Homeland Security of the House of Representatives, and the Permanent Select Committee on Intelligence of the House of Representatives on the feasibility of—

(A) eliminating the use of any marking or process (including "Originator Control") intended to, or having the effect of, restricting the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, between and among participants in the information sharing environment, unless the President has—

(i) specifically exempted categories of information from such elimination; and

(ii) reported that exemption to the committees of Congress described in the matter preceding this subparagraph; and

(B) continuing to use Federal agency standards in effect on such date of enactment for the collection, sharing, and access to information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, relating to citizens and lawful permanent residents;

(C) replacing the standards described in subparagraph (B) with a standard that would allow mission-based or threat-based permission to access or share information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, for a particular purpose that the Federal Government, through an appropriate process established in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an "authorized use" standard); and

(D) the use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, in any cases in which—

(i) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and

(ii) such use is consistent with any mission of that department, agency, or component (including any mission under a Federal statute or directive of the President) that involves the storage, retention, sharing, or exchange of personally identifiable information.

(2) DEFINITION.—In this subsection, the term "anonymized data" means data in which the individual to whom the data pertains is not identifiable with reasonable efforts, including information that has been encrypted or hidden through the use of other technology.

(k) ADDITIONAL POSITIONS.—The program manager is authorized to hire not more than 40 full-time employees to assist the program manager in—

(1) activities associated with the implementation of the information sharing environment, including—

(A) implementing the requirements under subsection (b)(2); and

(B) any additional implementation initiatives to enhance and expedite the creation of the information sharing environment; and

(2) identifying and resolving information sharing disputes between Federal departments, agencies, and components under subsection (f)(2)(A)(iv).

(l) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $30,000,000 for each of fiscal years 2008 and 2009.

* * * * * * *

SEC. 1019. ASSIGNMENT OF RESPONSIBILITIES RELATING TO ANALYTIC INTEGRITY.

(a) ASSIGNMENT OF RESPONSIBILITIES.—For purposes of carrying out section 102A(h) of the National Security Act of 1947 (as added by section 1011(a)), the Director of National Intelligence shall, not later than 180 days after the date of the enactment of this Act, assign an individual or entity to be responsible for ensuring that finished intelligence products produced by any element or elements of the intelligence community are timely, objective, independent of political considerations, based upon all sources of available intelligence, and employ the standards of proper analytic tradecraft.

(b) RESPONSIBILITIES.—(1) The individual or entity assigned responsibility under subsection (a)—

(A) may be responsible for general oversight and management of analysis and production, but may not be directly responsible for, or involved in, the specific production of any finished intelligence product;

(B) shall perform, on a regular basis, detailed reviews of finished intelligence product or other analytic products by an element or elements of the intelligence community covering a particular topic or subject matter;

(C) shall be responsible for identifying on an annual basis functional or topical areas of analysis for specific review under subparagraph (B); and

(D) upon completion of any review under subparagraph (B), may draft lessons learned, identify best practices, or make recommendations for improvement to the analytic tradecraft employed in the production of the reviewed product or products.

(2) Each review under paragraph (1)(B) should—

(A) include whether the product or products concerned were based on all sources of available intelligence, properly describe the quality and reliability of underlying sources, properly caveat and express uncertainties or confidence in analytic judgments, properly distinguish between underlying intelligence and the assumptions and judgments of analysts, and incorporate, where appropriate, alternative analyses; and

(B) ensure that the analytic methodologies, tradecraft, and practices used by the element or elements concerned in the production of the product or products concerned meet the standards set forth in subsection (a).

(3) Information drafted under paragraph (1)(D) should, as appropriate, be included in analysis teaching modules and case studies for use throughout the intelligence community.

(c) ANNUAL [REPORTS] *BRIEFINGS*.—Not later than December 1 each year, the Director of National Intelligence shall [submit to the congressional intelligence committees, the heads of the relevant elements of the intelligence community, and the heads of analytic training departments a report containing] *provide to the congressional intelligence committees, the heads of the relevant elements of the intelligence community, and the heads of analytic training departments a briefing with* a description, and the associated findings, of each review under subsection (b)(1)(B) during such year.

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

(1) the Select Committee on Intelligence of the Senate; and

(2) the Permanent Select Committee on Intelligence of the House of Representatives.

* * * * * * *

CUBAN LIBERTY AND DEMOCRATIC SOLIDARITY (LIBERTAD) ACT OF 1996

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996".

* * * * * * *

TITLE I—STRENGTHENING INTERNATIONAL SANCTIONS AGAINST THE CASTRO GOVERNMENT

* * * * * * *

[SEC. 108. REPORTS ON COMMERCE WITH, AND ASSISTANCE TO, CUBA FROM OTHER FOREIGN COUNTRIES.

[(a) REPORTS REQUIRED.—Not later than 90 days after the date of the enactment of this Act, and by January 1 of each year thereafter until the President submits a determination under section 203(c)(l), the President shall submit a report to the appropriate congressional committees on commerce with, and assistance to, Cuba from other foreign countries during the preceding 12-month period.

[(b) CONTENTS OF REPORTS.—Each report required by subsection (a) shall, for the period covered by the report, contain the following, to the extent such information is available:

[(1) A description of all bilateral assistance provided to Cuba by other foreign countries, including humanitarian assistance.

[(2) A description of Cuba's commerce with foreign countries, including an identification of Cuba's trading partners and the extent of such trade.

[(3) A description of the joint ventures completed, or under consideration, by foreign nationals and business firms involving facilities in Cuba, including an identification of the location of the facilities involved and a description of the terms of agreement of the joint. ventures and the names of the parties that are involved.

[(4) A determination as to whether or not any of the facilities described in paragraph (3) is the subject of a claim against Cuba by a United States national.

[(5) A determination of the amount of debt of the Cuban Government that is owed to each foreign country, including—

[(A) the amount of debt exchanged, forgiven, or reduced under the terms of each investment or operation in Cuba involving foreign nationals; and

[(B) the amount of debt owed the foreign country that has been exchanged, forgiven, or reduced in return for a grant by the Cuban Government of an equity interest in a property, investment, or operation of the Cuban Government or of a Cuban national.

[(6) A description of the steps taken to assure that raw materials and semifinished or finished goods produced by facilities in Cuba involving foreign nationals do not enter the United States market, either directly or through third countries or parties.

[(7) An identification of countries that purchase, or have purchased, arms or military supplies from Cuba or that otherwise have entered into agreements with Cuba that have a military application, including—

[(A) a description of the military supplies, equipment, or other material sold, bartered, or exchanged between Cuba and such countries,

[(B) a listing of the goods, services, credits, or other consideration received by Cuba in exchange for military supplies, equipment, or material, and

[(C) the terms or conditions of any such agreement.]

* * * * * * *

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE II—INFORMATION ANALYSIS

Subtitle A—Information and Analysis; Access to Information

* * * * * * *

SEC. 210D. INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP.

(a) IN GENERAL.—To improve the sharing of information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) with State, local, tribal, and private sector officials, the Director of National Intelligence, through the program manager for the information sharing environment, in coordination with the Secretary, shall coordinate and oversee the creation of an Interagency Threat Assessment and Coordination Group (referred to in this section as the "ITACG").

(b) COMPOSITION OF ITACG.—The ITACG shall consist of—

(1) an ITACG Advisory Council to set policy and develop processes for the integration, analysis, and dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information; and

(2) an ITACG Detail comprised of State, local, and tribal homeland security and law enforcement officers and intelligence analysts detailed to work in the National Counterterrorism Center with Federal intelligence analysts for the purpose of integrating, analyzing, and assisting in the dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, through appropriate channels identified by the ITACG Advisory Council.

[(c) RESPONSIBILITIES OF PROGRAM MANAGER.—The program manager shall—

[(1) monitor and assess the efficacy of the ITACG;

[(2) not later than 180 days after the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and at least annually thereafter, submit to the Secretary, the Attorney General, the Director of National Intelligence, the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the progress of the ITACG; and

[(3) in each report required by paragraph (2) submitted after the date of the enactment of the Reducing Over-Classification Act, include an assessment of whether the detailees under subsection (d)(5) have appropriate access to all relevant information, as required by subsection (g)(2)(C).**]**

[(d)**]** *(c)* RESPONSIBILITIES OF SECRETARY.—The Secretary, or the Secretary's designee, in coordination with the Director of the National Counterterrorism Center and the ITACG Advisory Council, shall—

(1) create policies and standards for the creation of information products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are suitable for dissemination to State, local, and tribal governments and the private sector;

(2) evaluate and develop processes for the timely dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to State, local, and tribal governments and the private sector;

(3) establish criteria and a methodology for indicating to State, local, and tribal governments and the private sector the reliability of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, disseminated to them;

(4) educate the intelligence community about the requirements of the State, local, and tribal homeland security, law enforcement, and other emergency response providers regarding information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(5) establish and maintain the ITACG Detail, which shall assign an appropriate number of State, local, and tribal homeland security and law enforcement officers and intelligence analysts to work in the National Counterterrorism Center who shall—

(A) educate and advise National Counterterrorism Center intelligence analysts about the requirements of the State, local, and tribal homeland security and law enforcement officers, and other emergency response providers regarding information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

(B) assist National Counterterrorism Center intelligence analysts in integrating, analyzing, and otherwise preparing versions of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information that are unclassified or classified at the lowest possible level and suitable for dissemination to State, local, and tribal homeland security and law enforcement agencies in order to help deter and prevent terrorist attacks;

(C) implement, in coordination with National Counterterrorism Center intelligence analysts, the policies, processes, procedures, standards, and guidelines developed by the ITACG Advisory Council;

(D) assist in the dissemination of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to State, local, and tribal jurisdictions only through appropriate channels identified by the ITACG Advisory Council;

(E) make recommendations, as appropriate, to the Secretary or the Secretary's designee, for the further dissemination of intelligence products that could likely inform or

improve the security of a State, local, or tribal government, (including a State, local, or tribal law enforcement agency) or a private sector entity; and

(F) report directly to the senior intelligence official from the Department under paragraph (6);

(6) detail a senior intelligence official from the Department of Homeland Security to the National Counterterrorism Center, who shall—

(A) manage the day-to-day operations of the ITACG Detail;

(B) report directly to the Director of the National Counterterrorism Center or the Director's designee; and

(C) in coordination with the Director of the Federal Bureau of Investigation, and subject to the approval of the Director of the National Counterterrorism Center, select a deputy from the pool of available detailees from the Federal Bureau of Investigation in the National Counterterrorism Center;

(7) establish, within the ITACG Advisory Council, a mechanism to select law enforcement officers and intelligence analysts for placement in the National Counterterrorism Center consistent with paragraph (5), using criteria developed by the ITACG Advisory Council that shall encourage participation from a broadly representative group of State, local, and tribal homeland security and law enforcement agencies; and

(8) compile an annual assessment of the ITACG Detail's performance, including summaries of customer feedback, in preparing, disseminating, and requesting the dissemination of intelligence products intended for State, local and tribal government (including State, local, and tribal law enforcement agencies) and private sector entities[; and].

[(9) provide the assessment developed pursuant to paragraph (8) to the program manager for use in the annual reports required by subsection (c)(2).]

[(e)] *(d)* MEMBERSHIP.—The Secretary, or the Secretary's designee, shall serve as the chair of the ITACG Advisory Council, which shall include—

(1) representatives of—

(A) the Department;

(B) the Federal Bureau of Investigation;

(C) the National Counterterrorism Center;

(D) the Department of Defense;

(E) the Department of Energy;

(F) the Department of State; and

(G) other Federal entities as appropriate;

(2) the program manager of the information sharing environment, designated under section 1016(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(f)), or the program manager's designee; and

(3) executive level law enforcement and intelligence officials from State, local, and tribal governments.

[(f)] *(e)* CRITERIA.—The Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the program manager of the information sharing environment established

under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), shall—

(1) establish procedures for selecting members of the ITACG Advisory Council and for the proper handling and safeguarding of products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by those members; and

(2) ensure that at least 50 percent of the members of the ITACG Advisory Council are from State, local, and tribal governments.

[(g)] *(f)* OPERATIONS.—

(1) IN GENERAL.—Beginning not later than 90 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the ITACG Advisory Council shall meet regularly, but not less than quarterly, at the facilities of the National Counterterrorism Center of the Office of the Director of National Intelligence.

(2) MANAGEMENT.—Pursuant to section 119(f)(E) of the National Security Act of 1947 (50 U.S.C. 404o(f)(E)), the Director of the National Counterterrorism Center, acting through the senior intelligence official from the Department of Homeland Security detailed pursuant to subsection (d)(6), shall ensure that—

(A) the products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, prepared by the National Counterterrorism Center and the ITACG Detail for distribution to State, local, and tribal homeland security and law enforcement agencies reflect the requirements of such agencies and are produced consistently with the policies, processes, procedures, standards, and guidelines established by the ITACG Advisory Council;

(B) in consultation with the ITACG Advisory Council and consistent with sections 102A(f)(1)(B)(iii) and 119(f)(E) of the National Security Act of 1947 (50 U.S.C. 402 et seq.), all products described in subparagraph (A) are disseminated through existing channels of the Department and the Department of Justice and other appropriate channels to State, local, and tribal government officials and other entities;

(C) all detailees under subsection (d)(5) have appropriate access to all relevant information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, available at the National Counterterrorism Center in order to accomplish the objectives under that paragraph;

(D) all detailees under subsection (d)(5) have the appropriate security clearances and are trained in the procedures for handling, processing, storing, and disseminating classified products derived from information within the scope of the information sharing environment, including

homeland security information, terrorism information, and weapons of mass destruction information; and

(E) all detailees under subsection (d)(5) complete appropriate privacy and civil liberties training.

[(h)] *(g)* INAPPLICABILITY OF THE FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the ITACG or any subsidiary groups thereof.

[(i)] *(h)* AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary for each of fiscal years 2008 through 2012 to carry out this section, including to obtain security clearances for the State, local, and tribal participants in the ITACG.

* * * * * * *

CENTRAL INTELLIGENCE AGENCY RETIREMENT ACT

* * * * * * *

TITLE II—THE CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

* * * * * * *

Part C—Computation of Annuities

SEC. 221. COMPUTATION OF ANNUITIES.

(a) ANNUITY OF PARTICIPANT.—

(1) COMPUTATION OF ANNUITY.—The annuity of a participant is the product of—

(A) the participant's high-3 average pay (as defined in paragraph (4)); and

(B) the number of years, not exceeding 35, of service credit (determined in accordance with sections 251 and 252) multiplied by 2 percent.

(2) CREDIT FOR UNUSED SICK LEAVE.—The total service of a participant who retires on an immediate annuity (except under section 231) or who dies leaving a survivor or survivors entitled to an annuity shall include (without regard to the 35-year limitation prescribed in paragraph (1)) the days of unused sick leave to the credit of the participant. Days of unused sick leave may not be counted in determining average basic pay or eligibility for an annuity under this title. A deposit shall not be required for days of unused sick leave credited under this paragraph.

(3) CREDITING OF PART-TIME SERVICE.—

(A) IN GENERAL.—In the case of a participant whose service includes service on a part-time basis performed after April 6, 1986, the participant's annuity shall be the sum of the amounts determined under subparagraphs (B) and (C).

(B) COMPUTATION OF PRE-APRIL 7, 1986, ANNUITY.—The portion of an annuity referred to in subparagraph (A) with respect to service before April 7, 1986, shall be the amount computed under paragraph (1) using the participant's length of service before that date (increased by the unused sick leave to the credit of the participant at the time of retirement) and the participant's high-3 average pay**[**.**]**, *as determined by using the annual rate of basic pay that would be payable for full-time service in that position.*

(C) COMPUTATION OF POST-APRIL 6, 1986, ANNUITY.—The portion of an annuity referred to in subparagraph (A) with respect to service after April 6, 1986, shall be the product of—

(i) the amount computed under paragraph (1), using the participant's length of service after that date and the participant's high-3 average pay, as determined by using the annual rate of basic pay that would be payable for full-time service; and

(ii) the ratio which the participant's actual service after April 6, 1986 (as determined by prorating the participant's total service after that date to reflect the service that was performed on a part-time basis) bears to the total service after that date that would be creditable for the participant if all the service had been performed on a full-time basis.

(D) TREATMENT OF EMPLOYMENT ON TEMPORARY OR INTERMITTENT BASIS.—Employment on a temporary or intermittent basis shall not be considered to be service on a part-time basis for purposes of this paragraph.

(4) HIGH-3 AVERAGE PAY DEFINED.—For purposes of this subsection, a participant's high-3 average pay is the amount of the participant's average basic pay for the highest 3 consecutive years of the participant's service for which full contributions have been made to the fund.

(5) COMPUTATION OF SERVICE.—In determining the aggregate period of service upon which an annuity is to be based, any fractional part of a month shall not be counted.

(b) SPOUSE OR FORMER SPOUSE SURVIVOR ANNUITY.—

(1) REDUCTION IN PARTICIPANT'S ANNUITY TO PROVIDE SPOUSE OR FORMER SPOUSE SURVIVOR ANNUITY.—

(A) GENERAL RULE.—Except to the extent provided otherwise under a written election under subparagraph (B) or (C), if at the time of retirement a participant or former participant is married (or has a former spouse who has not remarried before attaining age 55), the participant shall receive a reduced annuity and provide a survivor annuity for the participant's spouse under this subsection or former spouse under section 222(b), or a combination of such annuities, as the case may be.

(B) JOINT ELECTION FOR WAIVER OR REDUCTION OF SPOUSE SURVIVOR ANNUITY.—A married participant or former participant and the participant's spouse may jointly elect in writing at the time of retirement to waive a survivor annuity for that spouse under this section or to reduce such survivor annuity under this section by desig-

nating a portion of the annuity of the participant as the base for the survivor annuity. If the marriage is dissolved following an election for such a reduced annuity and the spouse qualifies as a former spouse, the base used in calculating any annuity of the former spouse under section 222(b) may not exceed the portion of the participant's annuity designated under this subparagraph.

(C) JOINT ELECTION OF PARTICIPANT AND FORMER SPOUSE.—If a participant or former participant has a former spouse, such participant and the participant's former spouse may jointly elect by spousal agreement under section 264(b) to waive, reduce, or increase a survivor annuity under section 222(b) for that former spouse. Any such election must be made (i) before the end of the [12-month] *2-year* period beginning on the date on which the divorce or annulment involving that former spouse becomes final, or (ii) at the time of retirement of the participant, whichever is later.

(D) UNILATERAL ELECTIONS IN ABSENCE OF SPOUSE OR FORMER SPOUSE.—The Director may prescribe regulations under which a participant or former participant may make an election under subparagraph (B) or (C) without the participant's spouse or former spouse if the participant establishes to the satisfaction of the Director that the participant does not know, and has taken all reasonable steps to determine, the whereabouts of the spouse or former spouse.

(2) AMOUNT OF REDUCTION IN PARTICIPANT'S ANNUITY.—The annuity of a participant or former participant providing a survivor annuity under this section (or section 222(b)), excluding any portion of the annuity not designated or committed as a base for any survivor annuity, shall be reduced by 2½ percent of the first $3,600 plus 10 percent of any amount over $3,600. The reduction under this paragraph shall be calculated before any reduction under section 222(a)(5).

(3) AMOUNT OF SURVIVING SPOUSE ANNUITY.—

(A) IN GENERAL.—If a retired participant receiving a reduced annuity under this subsection dies and is survived by a spouse, a survivor annuity shall be paid to the surviving spouse. The amount of the annuity shall be equal to 55 percent of (i) the full amount of the participant's annuity computed under subsection (a), or (ii) any lesser amount elected as the base for the survivor annuity under paragraph (1)(B).

(B) LIMITATION.—Notwithstanding subparagraph (A), the amount of the annuity calculated under subparagraph (A) for a surviving spouse in any case in which there is also a surviving former spouse of the retired participant who qualifies for an annuity under section 222(b) may not exceed 55 percent of the portion (if any) of the base for survivor annuities which remains available under section 222(b)(4)(B).

(C) EFFECTIVE DATE AND TERMINATION OF ANNUITY.—An annuity payable from the fund to a surviving spouse under this paragraph shall commence on the day after the retired

participant dies and shall terminate on the last day of the month before the surviving spouse's death or remarriage before attaining age 55. If such survivor annuity is terminated because of remarriage, it shall be restored at the same rate commencing on the date such remarriage is dissolved by death, annulment, or divorce if any lump sum paid upon termination of the annuity is returned to the fund.

(c) 18–MONTH OPEN PERIOD AFTER RETIREMENT TO PROVIDE SPOUSE COVERAGE.—

(1) SURVIVOR ANNUITY ELECTIONS.—

(A) ELECTION WHEN SPOUSE COVERAGE WAIVED AT TIME OF RETIREMENT.—A participant or former participant who retires after March 31, 1992 and who—

(i) is married at the time of retirement; and

(ii) elects at that time (in accordance with subsection (b)) to waive a survivor annuity for the spouse,

may, during the 18-month period beginning on the date of the retirement of the participant, elect to have a reduction under subsection (b) made in the annuity of the participant (or in such portion thereof as the participant may designate) in order to provide a survivor annuity for the participant's spouse.

(B) ELECTION WHEN REDUCED SPOUSE ANNUITY ELECTED.—A participant or former participant who retires after March 31, 1992, and—

(i) who, at the time of retirement, is married, and

(ii) who, at that time designates (in accordance with subsection (b)) that a portion of the annuity of such participant is to be used as the base for a survivor annuity,

may, during the 18-month period beginning on the date of the retirement of such participant, elect to have a greater portion of the annuity of such participant so used.

(2) DEPOSIT REQUIRED.—

(A) REQUIREMENT.—An election under paragraph (1) shall not be effective unless the amount specified in subparagraph (B) is deposited into the fund before the end of that 18-month period.

(B) AMOUNT OF DEPOSIT.—The amount to be deposited with respect to an election under this subsection is the amount equal to the sum of the following:

(i) ADDITIONAL COST TO SYSTEM.—The additional cost to the system that is associated with providing a survivor annuity under subsection (b) and that results from such election, taking into account—

(I) the difference (for the period between the date on which the annuity of the participant or former participant commences and the date of the election) between the amount paid to such participant or former participant under this title and the amount which would have been paid if such election had been made at the time the participant or former participant applied for the annuity; and

(II) the costs associated with providing for the later election.

(ii) INTEREST.—Interest on the additional cost determined under clause (i), computed using the interest rate specified or determined under section 8334(e) of title 5, United States Code, for the calendar year in which the amount to be deposited is determined.

(3) VOIDING OF PREVIOUS ELECTIONS.—An election by a participant or former participant under this subsection voids prospectively any election previously made in the case of such participant under subsection (b).

(4) REDUCTIONS IN ANNUITY.—An annuity that is reduced in connection with an election under this subsection shall be reduced by the same percentage reductions as were in effect at the time of the retirement of the participant or former participant whose annuity is so reduced.

(5) RIGHTS AND OBLIGATIONS RESULTING FROM REDUCED ANNUITY ELECTION.—Rights and obligations resulting from the election of a reduced annuity under this subsection shall be the same as the rights and obligations that would have resulted had the participant involved elected such annuity at the time of retirement.

(d) ANNUITIES FOR SURVIVING CHILDREN.—

(1) PARTICIPANTS DYING BEFORE APRIL 1, 1992.—In the case of a retired participant who died before April 1, 1992, and who is survived by a child or children—

(A) if the retired participant was survived by a spouse, there shall be paid from the fund to or on behalf of each such surviving child an annuity determined under paragraph (3)(A); and

(B) if the retired participant was not survived by a spouse, there shall be paid from the fund to or on behalf of each such surviving child an annuity determined under paragraph (3)(B).

(2) PARTICIPANTS DYING ON OR AFTER APRIL 1, 1992.—In the case of a retired participant who dies on or after April 1, 1992, and who is survived by a child or children—

(A) if the retired participant is survived by a spouse or former spouse who is the natural or adoptive parent of a surviving child of the participant, there shall be paid from the fund to or on behalf of each such surviving child an annuity determined under paragraph (3)(A); and

(B) if the retired participant is not survived by a spouse or former spouse who is the natural or adoptive parent of a surviving child of the participant, there shall be paid to or on behalf of each such surviving child an annuity determined under paragraph (3)(B).

(3) AMOUNT OF ANNUITY.—

(A) The annual amount of an annuity for the surviving child of a participant covered by paragraph (1)(A) or (2)(A) of this subsection (or covered by paragraph (1)(A) or (2)(A) of section 232(c)) is the smallest of the following:

(i) 60 percent of the participant's high-3 average pay, as determined under subsection (a)(4), divided by the number of children.

(ii) $900, as adjusted under section 291.

(iii) $2,700, as adjusted under section 291, divided by the number of children.

(B) The amount of an annuity for the surviving child of a participant covered by paragraph (1)(B) or (2)(B) of this subsection (or covered by paragraph (1)(B) or (2)(B) of section 232(c)) is the smallest of the following:

(i) 75 percent of the participant's high-3 average pay, as determined under subsection (a)(4), divided by the number of children.

(ii) $1,080, as adjusted under section 291.

(iii) $3,240, as adjusted under section 291, divided by the number of children.

(4) RECOMPUTATION OF CHILD ANNUITIES.—

(A) In the case of a child annuity payable under paragraph (1), upon the death of a surviving spouse or the termination of the annuity of a child, the annuities of any remaining children shall be recomputed and paid as though the spouse or child had not survived the retired participant.

(B) In the case of a child annuity payable under paragraph (2), upon the death of a surviving spouse or former spouse or termination of the annuity of a child, the annuities of any remaining children shall be recomputed and paid as though the spouse, former spouse, or child had not survived the retired participant. If the annuity of a surviving child who has not been receiving an annuity is initiated or resumed, the annuities of any other children shall be recomputed and paid from that date as though the annuities of all currently eligible children were then being initiated.

(5) DEFINITION OF FORMER SPOUSE.—For purposes of this subsection, the term "former spouse" includes any former wife or husband of the retired participant, regardless of the length of marriage or the amount of creditable service completed by the participant.

(e) COMMENCEMENT AND TERMINATION OF CHILD ANNUITIES.—

(1) COMMENCEMENT.—An annuity payable to a child under subsection (d), or under section 232(c), shall begin on the day after the date on which the participant or retired participant dies or, in the case of an individual over the age of 18 who is not a child within the meaning of section 102(b), shall begin or resume on the first day of the month in which the individual later becomes or again becomes a student as described in section 102(b). Such annuity may not commence until any lumpsum that has been paid is returned to the fund.

(2) TERMINATION.—Such an annuity shall terminate on the last day of the month before the month in which the recipient of the annuity dies or no longer qualifies as a child (as defined in section 102(b)).

(f) PARTICIPANTS NOT MARRIED AT TIME OF RETIREMENT.—

(1) DESIGNATION OF PERSONS WITH INSURABLE INTEREST.—

(A) AUTHORITY TO MAKE DESIGNATION.—Subject to the rights of former spouses under sections 221(b) and 222, at the time of retirement an unmarried participant found by

the Director to be in good health may elect to receive an annuity reduced in accordance with subparagraph (B) and designate in writing an individual having an insurable interest in the participant to receive an annuity under the system after the participant's death. The amount of such an annuity shall be equal to 55 percent of the participant's reduced annuity.

(B) REDUCTION IN PARTICIPANT'S ANNUITY.—The annuity payable to the participant making such election shall be reduced by 10 percent of an annuity computed under subsection (a) and by an additional 5 percent for each full 5 years the designated individual is younger than the participant. The total reduction under this subparagraph may not exceed 40 percent.

(C) COMMENCEMENT OF SURVIVOR ANNUITY.—The annuity payable to the designated individual shall begin on the day after the retired participant dies and terminate on the last day of the month before the designated individual dies.

(D) RECOMPUTATION OF PARTICIPANT'S ANNUITY ON DEATH OF DESIGNATED INDIVIDUAL.—An annuity which is reduced under this paragraph shall, effective the first day of the month following the death of the designated individual, be recomputed and paid as if the annuity had not been so reduced.

(2) ELECTION OF SURVIVOR ANNUITY UPON SUBSEQUENT MARRIAGE.—A participant who is unmarried at the time of retirement and who later marries may irrevocably elect, in a signed writing received by the Director within [one year] *two years* after the marriage, to receive a reduced annuity as provided in section 221(b). Such election and reduction shall be effective on the first day of the month beginning 9 months after the date of marriage. The election voids prospectively any election previously made under paragraph (1).

(g) EFFECT OF DIVORCE AFTER RETIREMENT.—

(1) RECOMPUTATION OF RETIRED PARTICIPANT'S ANNUITY UPON DIVORCE.—An annuity which is reduced under this section (or any similar prior provision of law) to provide a survivor annuity for a spouse shall, if the marriage of the retired participant to such spouse is dissolved, be recomputed and paid for each full month during which a retired participant is not married (or is remarried, if there is no election in effect under paragraph (2)) as if the annuity had not been so reduced, subject to any reduction required to provide a survivor annuity under subsection (b) or (c) of section 222 or under section 226.

(2) ELECTION OF SURVIVOR ANNUITY UPON SUBSEQUENT REMARRIAGE.—

(A) IN GENERAL.—Upon remarriage, the retired participant may irrevocably elect, by means of a signed writing received by the Director within [one year] *two years* after such remarriage, to receive a reduced annuity for the purpose of providing an annuity for the new spouse of the retired participant in the event such spouse survives the retired participant. Such reduction shall be equal to the reduction in effect immediately before the dissolution of the

previous marriage (unless such reduction is adjusted under section 222(b)(5) or elected under subparagraph (B)).

(B) WHEN ANNUITY PREVIOUSLY NOT (OR NOT FULLY) REDUCED.—

(i) ELECTION.—If the retired participant's annuity was not reduced (or was not fully reduced) to provide a survivor annuity for the participant's spouse or former spouse as of the time of retirement, the retired participant may make an election under the first sentence of subparagraph (A) upon remarriage to a spouse other than the spouse at the time of retirement. For any remarriage that occurred before August 14, 1991, the retired participant may make such an election within 2 years after such date.

(ii) DEPOSIT REQUIRED.—

(I) The retired participant shall, within [one year] *two years* after the date of the remarriage (or by August 14, 1993 for any remarriage that occurred before August 14, 1991), deposit in the fund an amount determined by the Director, as nearly as may be administratively feasible, to reflect the amount by which the retired participant's annuity would have been reduced if the election had been in effect since the date the annuity commenced, plus interest.

(II) The annual rate of interest for each year during which the retired participant's annuity would have been reduced if the election had been in effect since the date the annuity commenced shall be 6 percent.

(III) If the retired participant does not make the deposit, the Director shall collect such amount by offset against the participant's annuity, up to a maximum of 25 percent of the net annuity otherwise payable to the retired participant, and the retired participant is deemed to consent to such offset.

(IV) The deposit required by this subparagraph may be made by the surviving spouse of the retired participant.

(C) EFFECTS OF ELECTION.—An election under this paragraph and the reduction in the participant's annuity shall be effective on the first day of the month beginning 9 months after the date of remarriage. A survivor annuity elected under this paragraph shall be treated in all respects as a survivor annuity under subsection (b).

(h) CONDITIONAL ELECTION OF INSURABLE INTEREST SURVIVOR ANNUITY BY PARTICIPANTS MARRIED AT THE TIME OF RETIREMENT.—

(1) AUTHORITY TO MAKE DESIGNATION.—Subject to the rights of former spouses under subsection (b) and section 222, at the time of retirement a married participant found by the Director to be in good health may elect to receive an annuity reduced in accordance with subsection (f)(1)(B) and designate in writing an individual having an insurable interest in the participant to

receive an annuity under the system after the participant's death, except that any such election to provide an insurable interest survivor annuity to the participant's spouse shall only be effective if the participant's spouse waives the spousal right to a survivor annuity under this Act. The amount of the annuity shall be equal to 55 percent of the participant's reduced annuity.

(2) REDUCTION IN PARTICIPANT'S ANNUITY.—The annuity payable to the participant making such election shall be reduced by 10 percent of an annuity computed under subsection (a) and by an additional 5 percent for each full 5 years the designated individual is younger than the participant. The total reduction under this subparagraph may not exceed 40 percent.

(3) COMMENCEMENT OF SURVIVOR ANNUITY.—The annuity payable to the designated individual shall begin on the day after the retired participant dies and terminate on the last day of the month before the designated individual dies.

(4) RECOMPUTATION OF PARTICIPANT'S ANNUITY ON DEATH OF DESIGNATED INDIVIDUAL.—An annuity that is reduced under this subsection shall, effective the first day of the month following the death of the designated individual, be recomputed and paid as if the annuity had not been so reduced.

[(h)**]** *(i)* COORDINATION OF ANNUITIES.—

(1) SURVIVING SPOUSE.—A surviving spouse whose survivor annuity was terminated because of remarriage before attaining age 55 shall not be entitled under subsection (b)(3)(C) to the restoration of that survivor annuity payable from the fund unless the surviving spouse elects to receive it instead of any other survivor annuity to which the surviving spouse may be entitled under the system or any other retirement system for Government employees by reason of the remarriage.

(2) FORMER SPOUSE.—A surviving former spouse of a participant or retired participant shall not become entitled under section 222(b) or 224 to a survivor annuity or to the restoration of a survivor annuity payable from the fund unless the surviving former spouse elects to receive it instead of any other survivor annuity to which the surviving former spouse may be entitled under this or any other retirement system for Government employees on the basis of a marriage to someone other than the participant.

(3) SURVIVING SPOUSE OF POST-RETIREMENT MARRIAGE.—A surviving spouse who married a participant after the participant's retirement shall be entitled to a survivor annuity payable from the fund only upon electing that annuity instead of any other survivor annuity to which the surviving spouse may be entitled under this or any other retirement system for Government employees on the basis of a marriage to someone other than the retired participant.

[(i)**]** *(j)* SUPPLEMENTAL SURVIVOR ANNUITIES.—

(1) SPOUSE OF RECALLED ANNUITANT.—A married recalled annuitant who reverts to retired status with entitlement to a supplemental annuity under section 271(b) shall, unless the annuitant and the annuitant's spouse jointly elect in writing to the contrary at the time of reversion to retired status, have the supplemental annuity reduced by 10 percent to provide a sup-

plemental survivor annuity for the annuitant's spouse. Such supplemental survivor annuity shall be equal to 55 percent of the supplemental annuity of the annuitant.

(2) REGULATIONS.—The Director shall prescribe regulations to provide for the application of paragraph (1) of this subsection and of subsection (b) of section 271 in any case in which an annuitant has a former spouse who was married to the recalled annuitant at any time during the period of recall service and who qualifies for an annuity under section 222(b).

[(j)] *(k)* OFFSET OF ANNUITIES BY AMOUNT OF SOCIAL SECURITY BENEFIT.—Notwithstanding any other provision of this title, an annuity (including a disability annuity) payable under this title to an individual described in sections 211(d)(1) and 301(c)(1) and any survivor annuity payable under this title on the basis of the service of such individual shall be reduced in a manner consistent with section 8349 of title 5, United States Code, under conditions consistent with the conditions prescribed in that section.

[(k)] *(l)* INFORMATION FROM OTHER AGENCIES.—

(1) OTHER AGENCIES.—For the purpose of ensuring the accuracy of the information used in the determination of eligibility for and the computation of annuities payable from the fund under this title, at the request of the Director—

(A) the Secretary of Defense shall provide information on retired or retainer pay paid under title 10, United States Code;

(B) the Secretary of Veterans Affairs shall provide information on pensions or compensation paid under title 38, United States Code;

(C) the Secretary of Health and Human Services shall provide information contained in the records of the Social Security Administration; and

(D) the Secretary of Labor shall provide information on benefits paid under subchapter I of chapter 81 of title 5, United States Code.

(2) LIMITATION ON INFORMATION REQUESTED.—The Director shall request only such information as the Director determines is necessary.

(3) LIMITATION ON USES OF INFORMATION.—The Director, in consultation with the officials from whom information is requested, shall ensure that information made available under this subsection is used only for the purposes authorized.

[(l)] *(m)* INFORMATION ON RIGHTS UNDER THE SYSTEM.—The Director shall, on an annual basis—

(1) inform each retired participant of the participant's right of election under subsections (c), (f)(2), and (g); and

(2) to the maximum extent practicable, inform spouses and former spouses of participants, former participants, and retired participants of their rights under this Act.

SEC. 222. ANNUITIES FOR FORMER SPOUSES.

(a) FORMER SPOUSE SHARE OF PARTICIPANT'S ANNUITY.—

(1) PRO RATA SHARE.—Unless otherwise expressly provided by a spousal agreement or court order under section 264(b), a former spouse of a participant, former participant, or retired participant is entitled to an annuity—

(A) if married to the participant, former participant, or retired participant throughout the creditable service of the participant, equal to 50 percent of the annuity of the participant; or

(B) if not married to the participant throughout such creditable service, equal to that proportion of 50 percent of such annuity that is the proportion that the number of days of the marriage of the former spouse to the participant during periods of creditable service of such participant under this title bears to the total number of days of such creditable service.

(2) DISQUALIFICATION UPON REMARRIAGE BEFORE AGE 55.—A former spouse is not qualified for an annuity under this subsection if before the commencement of that annuity the former spouse remarries before becoming 55 years of age.

(3) COMMENCEMENT OF ANNUITY.—The annuity of a former spouse under this subsection commences on the day the participant upon whose service the annuity is based becomes entitled to an annuity under this title or on the first day of the month after the divorce or annulment involved becomes final, whichever is later.

(4) TERMINATION OF ANNUITY.—The annuity of such former spouse and the right thereto terminate on—

(A) the last day of the month before the month in which the former spouse dies or remarries before 55 years of age; or

(B) the date on which the annuity of the participant terminates (except in the case of an annuity subject to paragraph (5)(B)).

(5) TREATMENT OF PARTICIPANT'S ANNUITY.—

(A) REDUCTION IN PARTICIPANT'S ANNUITY.—The annuity payable to any participant shall be reduced by the amount of an annuity under this subsection paid to any former spouse based upon the service of that participant. Such reduction shall be disregarded in calculating—

(i) the survivor annuity for any spouse, former spouse, or other survivor under this title; and

(ii) any reduction in the annuity of the participant to provide survivor benefits under subsection (b) or under section 221(b).

(B) TREATMENT WHEN ANNUITANT RETURNS TO SERVICE.—If an annuitant whose annuity is reduced under subparagraph (A) is recalled to service under section 271, or reinstated or reappointed, in the case of a recovered disability annuitant, or if any annuitant is reemployed as provided for under sections 272 and 273, the pay of that annuitant shall be reduced by the same amount as the annuity would have been reduced if it had continued. Amounts equal to the reductions under this subparagraph shall be deposited in the Treasury of the United States to the credit of the fund.

(6) DISABILITY ANNUITANT.—Notwithstanding paragraph (3), in the case of a former spouse of a disability annuitant—

(A) the annuity of that former spouse shall commence on the date on which the participant would qualify on the

basis of the participant's creditable service for an annuity under this title (other than a disability annuity) or the date on which the disability annuity begins, whichever is later, and

(B) the amount of the annuity of the former spouse shall be calculated on the basis of the annuity for which the participant would otherwise so qualify.

(7) ELECTION OF BENEFITS.—A former spouse of a participant, former participant, or retired participant shall not become entitled under this subsection to an annuity payable from the fund unless the former spouse elects to receive it instead of any survivor annuity to which the former spouse may be entitled under this or any other retirement system for Government employees on the basis of a marriage to someone other than the participant.

(8) LIMITATION IN CASE OF MULTIPLE FORMER SPOUSE ANNUITIES.—No spousal agreement or court order under section 264(b) involving a participant may provide for an annuity or a combination of annuities under this subsection that exceeds the annuity of the participant.

(b) FORMER SPOUSE SURVIVOR ANNUITY.—

(1) PRO RATA SHARE.—Subject to any election under section 221(b)(1)(B) and (C) and unless otherwise expressly provided by a spousal agreement or court order under section 264(b), if an annuitant is survived by a former spouse, the former spouse shall be entitled—

(A) if married to the annuitant throughout the creditable service of the annuitant, to a survivor annuity equal to 55 percent of the unreduced amount of the annuitant's annuity, as computed under section 221(a); and

(B) if not married to the annuitant throughout such creditable service, to a survivor annuity equal to that proportion of 55 percent of the unreduced amount of such annuity that is the proportion that the number of days of the marriage of the former spouse to the participant during periods of creditable service of such participant under this title bears to the total number of days of such creditable service.

(2) DISQUALIFICATION UPON REMARRIAGE BEFORE AGE 55.—A former spouse shall not be qualified for an annuity under this subsection if before the commencement of that annuity the former spouse remarries before becoming 55 years of age.

(3) COMMENCEMENT, TERMINATION, AND RESTORATION OF ANNUITY.—An annuity payable from the fund under this title to a surviving former spouse under this subsection shall commence on the day after the annuitant dies and shall terminate on the last day of the month before the former spouse's death or remarriage before attaining age 55. If such a survivor annuity is terminated because of remarriage, it shall be restored at the same rate commencing on the date such remarriage is dissolved by death, annulment, or divorce if any lump sum paid upon termination of the annuity is returned to the fund.

(4) SURVIVOR ANNUITY AMOUNT.—

(A) MAXIMUM AMOUNT.—The maximum survivor annuity or combination of survivor annuities under this subsection

(and section 221(b)(3)) with respect to any participant may not exceed 55 percent of the full amount of the participant's annuity, as calculated under section 221(a).

(B) LIMITATION ON OTHER SURVIVOR ANNUITIES BASED ON SERVICE OF SAME PARTICIPANT.—Once a survivor annuity has been provided under this subsection for any former spouse, a survivor annuity for another individual may thereafter be provided under this subsection (or section 221(b)(3)) with respect to the participant only for that portion (if any) of the maximum available which is not committed for survivor benefits for any former spouse whose prospective right to such annuity has not terminated by reason of death or remarriage.

(C) FINALITY OF COURT ORDER UPON DEATH OF PARTICIPANT.—After the death of a participant or retired participant, a court order under section 264(b) may not adjust the amount of the annuity of a former spouse of that participant or retired participant under this section.

(5) EFFECT OF TERMINATION OF FORMER SPOUSE ENTITLEMENT.—

(A) RECOMPUTATION OF PARTICIPANT'S ANNUITY.—If a former spouse of a retired participant dies or remarries before attaining age 55, the annuity of the retired participant, if reduced to provide a survivor annuity for that former spouse, shall be recomputed and paid, effective on the first day of the month beginning after such death or remarriage, as if the annuity had not been so reduced, unless an election is in effect under subparagraph (B).

(B) ELECTION OF SPOUSE ANNUITY.—Subject to paragraph (4)(B), the participant may elect in writing within [one year] *two years* after receipt of notice of the death or remarriage of the former spouse to continue the reduction in order to provide a higher survivor annuity under section 221(b)(3) for any spouse of the participant.

(c) OPTIONAL ADDITIONAL SURVIVOR ANNUITIES FOR OTHER FORMER SPOUSE OR SURVIVING SPOUSE.—

(1) IN GENERAL.—In the case of any participant providing a survivor annuity under subsection (b) for a former spouse—

(A) such participant may elect, or

(B) a spousal agreement or court order under section 264(b) may provide for,

an additional survivor annuity under this subsection for any other former spouse or spouse surviving the participant, if the participant satisfactorily passes a physical examination as prescribed by the Director.

(2) LIMITATION.—Neither the total amount of survivor annuity or annuities under this subsection with respect to any participant, nor the survivor annuity or annuities for any one surviving spouse or former spouse of such participant under this section or section 221, may exceed 55 percent of the unreduced amount of the participant's annuity, as computed under section 221(a).

(3) CONTRIBUTION FOR ADDITIONAL ANNUITIES.—

(A) PROVISION OF ADDITIONAL SURVIVOR ANNUITY.—In accordance with regulations which the Director shall pre-

scribe, the participant involved may provide for any annuity under this subsection—

(i) by a reduction in the annuity or an allotment from the basic pay of the participant;

(ii) by a lump-sum payment or installment payments to the fund; or

(iii) by any combination thereof.

(B) ACTUARIAL EQUIVALENCE TO BENEFIT.—The present value of the total amount to accrue to the fund under subparagraph (A) to provide any annuity under this subsection shall be actuarially equivalent in value to such annuity, as calculated upon such tables of mortality as may from time to time be prescribed for this purpose by the Director.

(C) EFFECT OF FORMER SPOUSE'S DEATH OR DISQUALIFICATION.—If a former spouse predeceases the participant or remarries before attaining age 55 (or, in the case of a spouse, the spouse predeceases the participant or does not qualify as a former spouse upon dissolution of the marriage)—

(i) if an annuity reduction or pay allotment under subparagraph (A) is in effect for that spouse or former spouse, the annuity shall be recomputed and paid as if it had not been reduced or the pay allotment terminated, as the case may be; and

(ii) any amount accruing to the fund under subparagraph (A) shall be refunded, but only to the extent that such amount may have exceeded the actuarial cost of providing benefits under this subsection for the period such benefits were provided, as determined under regulations prescribed by the Director.

(D) RECOMPUTATION UPON DEATH OR REMARRIAGE OF FORMER SPOUSE.—Under regulations prescribed by the Director, an annuity shall be recomputed (or a pay allotment terminated or adjusted), and a refund provided (if appropriate), in a manner comparable to that provided under subparagraph (C), in order to reflect a termination or reduction of future benefits under this subsection for a spouse in the event a former spouse of the participant dies or remarries before attaining age 55 and an increased annuity is provided for that spouse in accordance with this section.

(4) COMMENCEMENT AND TERMINATION OF ADDITIONAL SURVIVOR ANNUITY.—An annuity payable under this subsection to a spouse or former spouse shall commence on the day after the participant dies and shall terminate on the last day of the month before the spouse's or the former spouse's death or remarriage before attaining age 55.

(5) NONAPPLICABILITY OF COLA PROVISION.—Section 291 does not apply to an annuity under this subsection, unless authorized under regulations prescribed by the Director.

* * * * * * *

Part D—Benefits Accruing to Certain Participants

* * * * * * *

SEC. 232. DEATH IN SERVICE.

(a) RETURN OF CONTRIBUTIONS WHEN NO ANNUITY PAYABLE.—If a participant dies and no claim for an annuity is payable under this title, the participant's lump-sum credit and any voluntary contributions made under section 281, with interest, shall be paid in the order of precedence shown in section 241(c).

(b) SURVIVOR ANNUITY FOR SURVIVING SPOUSE OR FORMER SPOUSE.—

(1) IN GENERAL.—If a participant dies before separation or retirement from the Agency and is survived by a spouse or by a former spouse qualifying for a survivor annuity under section 222(b), such surviving spouse shall be entitled to an annuity equal to 55 percent of the annuity computed in accordance with paragraphs (2) and (3) of this subsection and section 221(a), and any such surviving former spouse shall be entitled to an annuity computed in accordance with section 222(b) and paragraph (2) of this subsection as if the participant died after being entitled to an annuity under this title. The annuity of such surviving spouse or former spouse shall commence on the day after the participant dies and shall terminate on the last day of the month before the death or remarriage before attaining age 55 of the surviving spouse or former spouse (subject to the payment and restoration provisions of sections 221(b)(3)(C), ⟦221(h),⟧ *221(i),* and 222(b)(3)).

(2) COMPUTATION.—The annuity payable under paragraph (1) shall be computed in accordance with section 221(a), except that the computation of the annuity of the participant under such section shall be at least the smaller of (A) 40 percent of the participant's high-3 average pay, or (B) the sum obtained under such section after increasing the participant's length of service by the difference between the participant's age at the time of death and age 60.

(3) LIMITATION.—Notwithstanding paragraph (1), if the participant had a former spouse qualifying for an annuity under section 222(b), the annuity of a surviving spouse under this section shall be subject to the limitation of section 221(b)(3)(B), and the annuity of a former spouse under this section shall be subject to the limitation of section 222(b)(4)(B).

(4) PRECEDENCE OF SECTION 224 SURVIVOR ANNUITY OVER DEATH-IN-SERVICE ANNUITY.—If a former spouse who is eligible for a death-in-service annuity under this section is or becomes eligible for an annuity under section 224, the annuity provided under this section shall not be payable and shall be superseded by the annuity under section 224.

(c) ANNUITIES FOR SURVIVING CHILDREN.—

(1) PARTICIPANTS DYING BEFORE APRIL 1, 1992.—In the case of a participant who before April 1, 1992, died before separation or retirement from the Agency and who was survived by a child or children—

(A) if the participant was survived by a spouse, there shall be paid from the fund to or on behalf of each such surviving child an annuity determined under section 221(d)(3)(A); and

(B) if the participant was not survived by a spouse, there shall be paid from the fund to or on behalf of each such surviving child an annuity determined under section 221(d)(3)(B).

(2) PARTICIPANTS DYING ON OR AFTER APRIL 1, 1992.—In the case of a participant who on or after April 1, 1992, dies before separation or retirement from the Agency and who is survived by a child or children—

(A) if the participant is survived by a spouse or former spouse who is the natural or adoptive parent of a surviving child of the participant, there shall be paid from the fund to or on behalf of each such surviving child an annuity determined under section 221(d)(3)(A); and

(B) if the participant is not survived by a spouse or former spouse who is the natural or adoptive parent of a surviving child of the participant, there shall be paid to or on behalf of each such surviving child an annuity determined under section 221(d)(3)(B).

(3) FORMER SPOUSE DEFINED.—For purposes of this subsection, the term "former spouse" includes any former wife or husband of a participant, regardless of the length of marriage or the amount of creditable service completed by the participant.

* * * * * * *

Part F—Period of Service for Annuities

* * * * * * *

SEC. 252. PRIOR SERVICE CREDIT.

(a) IN GENERAL.—A participant may, subject to the provisions of this section, include in the participant's period of service—

(1) civilian service in the Government before becoming a participant that would be creditable toward retirement under subchapter III of chapter 83 of title 5, United States Code (as determined under section 8332(b) of such title); and

(2) honorable active service in the Armed Forces before the date of the separation upon which eligibility for an annuity is based, or honorable active service in the Regular or Reserve Corps of the Public Health Service after June 30, 1960, or as a commissioned officer of the National Oceanic and Atmospheric Administration after June 30, 1961.

(b) LIMITATIONS.—

(1) IN GENERAL.—Except as provided in paragraphs (2) and (3), the total service of any participant shall exclude—

(A) any period of civilian service on or after October 1, 1982, for which retirement deductions or deposits have not been made,

(B) any period of service for which a refund of contributions has been made, or

(C) any period of service for which contributions were not transferred pursuant to subsection (c)(1);

unless the participant makes a deposit to the fund in an amount equal to the percentages of basic pay received for such service as specified in the table contained in section 8334(c) of title 5, United States Code, together with interest computed in accordance with section 8334(e) of such title. The deposit may be made in one or more installments (including by allotment from pay), as determined by the Director.

(2) EFFECT OF RETIREMENT DEDUCTIONS NOT MADE.—If a participant has not paid a deposit for civilian service performed before October 1, 1982, for which retirement deductions were not made, such participant's annuity shall be reduced by 10 percent of the deposit described in paragraph (1) remaining unpaid, unless the participant elects to eliminate the service involved for the purpose of the annuity computation.

(3) EFFECT OF REFUND OF RETIREMENT CONTRIBUTIONS.—A participant who received a refund of retirement contributions under this or any other retirement system for Government employees covering service for which the participant may be allowed credit under this title may deposit the amount received, with interest computed under paragraph (1). Credit may not be allowed for the service covered by the refund until the deposit is made, except that a participant who—

(A) separated from Government service before [October 1, 1990] *March 31, 1991*, and received a refund of the participant's retirement contributions covering a period of service ending before [October 1, 1990] *March 31, 1991*;

(B) is entitled to an annuity under this title (other than a disability annuity) which commences after December 1, 1992; and

(C) does not make the deposit required to receive credit for the service covered by the refund;

shall be entitled to an annuity actuarially reduced in accordance with section 8334(d)(2)(B) of title 5, United States Code.

(4) ENTITLEMENT UNDER ANOTHER SYSTEM.—Credit toward retirement under the system shall not be allowed for any period of civilian service on the basis of which the participant is receiving (or will in the future be entitled to receive) an annuity under another retirement system for Government employees, unless the right to such annuity is waived and a deposit is made under paragraph (1) covering that period of service, or a transfer is made pursuant to subsection (c).

(c) TRANSFER FROM OTHER GOVERNMENT RETIREMENT SYSTEMS.—

(1) IN GENERAL.—If an employee who is under another retirement system for Government employees becomes a participant in the system by direct transfer, the Government's contributions (including interest accrued thereon computed in accordance with section 8334(e) of title 5, United States Code) under such retirement system on behalf of the employee as well as such employee's total contributions and deposits (including interest accrued thereon), except voluntary contributions, shall be transferred to the employee's credit in the fund

effective as of the date such employee becomes a participant in the system.

(2) CONSENT OF EMPLOYEE.—Each such employee shall be deemed to consent to the transfer of such funds, and such transfer shall be a complete discharge and acquittance of all claims and demands against the other Government retirement fund on account of service rendered before becoming a participant in the system.

(3) ADDITIONAL CONTRIBUTIONS; REFUNDS.—A participant whose contributions are transferred pursuant to paragraph (1) shall not be required to make additional contributions for periods of service for which full contributions were made to the other Government retirement fund, nor shall any refund be made to any such participant on account of contributions made during any period to the other Government retirement fund at a higher rate than that fixed for employees by section 8334(c) of title 5, United States Code, for contributions to the fund.

(d) TRANSFER TO OTHER GOVERNMENT RETIREMENT SYSTEMS.—

(1) IN GENERAL.—If a participant in the system becomes an employee under another Government retirement system by direct transfer to employment covered by such system, the Government's contributions (including interest accrued thereon computed in accordance with section 8334(e) of title 5, United States Code) to the fund on the participant's behalf as well as the participant's total contributions and deposits (including interest accrued thereon), except voluntary contributions, shall be transferred to the participant's credit in the fund of such other retirement system effective as of the date on which the participant becomes eligible to participate in such other retirement system.

(2) CONSENT OF EMPLOYEE.—Each such employee shall be deemed to consent to the transfer of such funds, and such transfer shall be a complete discharge and acquittance of all claims and demands against the fund on account of service rendered before the participant's becoming eligible for participation in that other system.

(e) PRIOR MILITARY SERVICE CREDIT.—

(1) APPLICATION TO OBTAIN CREDIT.—If a deposit required to obtain credit for prior military service described in subsection (a)(2) was not made to another Government retirement fund and transferred under subsection (c)(1), the participant may obtain credit for such military service, subject to the provisions of this subsection and subsections (f) through (h), by applying for it to the Director before retirement or separation from the Agency.

(2) EMPLOYMENT STARTING BEFORE, ON, OR AFTER OCTOBER 1, 1982.—Except as provided in paragraph (3)—

(A) the service of a participant who first became a Federal employee before October 1, 1982, shall include credit for each period of military service performed before the date of separation on which entitlement to an annuity under this title is based, subject to section 252(f); and

(B) the service of a participant who first becomes a Federal employee on or after October 1, 1982, shall include credit for—

(i) each period of military service performed before January 1, 1957, and

(ii) each period of military service performed after December 31, 1956, and before the separation on which entitlement to an annuity under this title is based, only if a deposit (with interest, if any) is made with respect to that period, as provided in subsection (h).

(3) EFFECT OF RECEIPT OF MILITARY RETIRED PAY.—In the case of a participant who is entitled to retired pay based on a period of military service, the participant's service may not include credit for such period of military service unless the retired pay is paid—

(A) on account of a service-connected disability—

(i) incurred in combat with an enemy of the United States; or

(ii) caused by an instrumentality of war and incurred in the line of duty during a period of war (as defined in section 1101 of title 38, United States Code); or

(B) under chapter 67 of title 10, United States Code.

(4) SURVIVOR ANNUITY.—Notwithstanding paragraph (3), the survivor annuity of a survivor of a participant—

(A) who was awarded retired pay based on any period of military service, and

(B) whose death occurs before separation from the Agency,

shall be computed in accordance with section 8332(c)(3) of title 5, United States Code.

(f) EFFECT OF ENTITLEMENT TO SOCIAL SECURITY BENEFITS.—

(1) IN GENERAL.—Notwithstanding any other provision of this section (except paragraph (3) of this subsection) or section 253, any military service (other than military service covered by military leave with pay from a civilian position) performed by a participant after December 1956 shall be excluded in determining the aggregate period of service on which an annuity payable under this title to such participant or to the participant's spouse, former spouse, previous spouse, or child is based, if such participant, spouse, former spouse, previous spouse, or child is entitled (or would upon proper application be entitled), at the time of such determination, to monthly old-age or survivors' insurance benefits under section 202 of the Social Security Act (42 U.S.C. 402), based on such participant's wages and self-employment income. If the military service is not excluded under the preceding sentence, but upon attaining age 62, the participant or spouse, former spouse, or previous spouse becomes entitled (or would upon proper application be entitled) to such benefits, the aggregate period of service on which the annuity is based shall be redetermined, effective as of the first day of the month in which the participant or spouse, former spouse, or previous spouse attains age 62, so as to exclude such service.

(2) LIMITATION.—The provisions of paragraph (1) relating to credit for military service do not apply to—

(A) any period of military service of a participant with respect to which the participant has made a deposit with interest, if any, under subsection (h); or

(B) the military service of any participant described in subsection (e)(2)(B).

(3) EFFECT OF ENTITLEMENT BEFORE SEPTEMBER 8, 1982.—(A) The annuity recomputation required by paragraph (1) shall not apply to any participant who was entitled to an annuity under this title on or before September 8, 1982, or who is entitled to a deferred annuity based on separation from the Agency occurring on or before such date. Instead of an annuity recomputation, the annuity of such participant shall be reduced at age 62 by an amount equal to a fraction of the participant's old-age or survivors' insurance benefits under section 202 of the Social Security Act. The reduction shall be determined by multiplying the participant's monthly Social Security benefit by a fraction, the numerator of which is the participant's total military wages and deemed additional wages (within the meaning of section 229 of the Social Security Act (42 U.S.C. 429)) that were subject to Social Security deductions and the denominator of which is the total of all the participant's wages, including military wages, and all self-employment income that were subject to Social Security deductions before the calendar year in which the determination month occurs.

(B) The reduction determined in accordance with subparagraph (A) shall not be greater than the reduction that would be required under paragraph (1) if such paragraph applied to the participant. The new formula shall be applicable to any annuity payment payable after October 1, 1982, including annuity payments to participants who had previously reached age 62 and whose annuities had already been recomputed.

(C) For purposes of this paragraph, the term "determination month" means—

(i) the first month for which the participant is entitled to old-age or survivors' insurance benefits (or would be entitled to such benefits upon application therefor); or

(ii) October 1982, in the case of any participant entitled to such benefits for that month.

(g) DEPOSITS PAID BY SURVIVORS.—For the purpose of survivor annuities, deposits authorized by subsections (b) and (h) may also be made by the survivor of a participant.

(h)(1)(A) Each participant who has performed military service before the date of separation on which entitlement to an annuity under this title is based may pay to the Agency an amount equal to 7 percent of the amount of basic pay paid under section 204 of title 37, United States Code, to the participant for each period of military service after December 1956; except, the amount to be paid for military service performed beginning on January 1, 1999, through December 31, 2000, shall be as follows:

7.25 percent of basic pay.	January 1, 1999, to December 31, 1999.
7.4 percent of basic pay.	January 1, 2000, to December 31, 2000.

(B) The amount of such payments shall be based on such evidence of basic pay for military service as the participant may provide or, if the Director determines sufficient evidence has not been provided to adequately determine basic pay for military service, such payment shall be based upon estimates of such basic pay provided to the Director under paragraph (4).

(2) Any deposit made under paragraph (1) more than two years after the later of—

(A) October 1, 1983, or

(B) the date on which the participant making the deposit first becomes an employee of the Federal Government,

shall include interest on such amount computed and compounded annually beginning on the date of expiration of the two-year period. The interest rate that is applicable in computing interest in any year under this paragraph shall be equal to the interest rate that is applicable for such year under section 8334(e) of title 5, United States Code.

(3) Any payment received by the Director under this subsection shall be deposited in the Treasury of the United States to the credit of the fund.

(4) The provisions of section [221(k)] *221(l)* shall apply with respect to such information as the Director determines to be necessary for the administration of this subsection in the same manner that such section applies concerning information described in that section.

* * * * * * *

Part H—Retired Participants Recalled, Reinstated, or Reappointed in the Agency or Reemployed in the Government

* * * * * * *

SEC. 273. REEMPLOYMENT COMPENSATION.

(a) DEDUCTION FROM BASIC PAY.—An annuitant who has retired under this title and who is reemployed in the Federal Government service in any appointive position (either on a part-time or full-time basis) shall be entitled to receive the annuity payable under this title, but there shall be deducted from the annuitant's basic pay a sum equal to the annuity allocable to the period of actual employment.

(b) PART-TIME REEMPLOYED ANNUITANTS.—The Director shall have the authority to reemploy an annuitant on a part-time basis in accordance with section 8344(l) of title 5, United States Code.

[(b)] *(c)* RECOVERY OF OVERPAYMENTS.—In the event of an overpayment under this section, the amount of the overpayment shall be recovered by withholding the amount involved from the basic pay payable to such reemployed annuitant or from any other moneys, including the annuitant's annuity, payable in accordance with this title.

[(c)] *(d)* DEPOSIT IN THE FUND.—Sums deducted from the basic pay of a reemployed annuitant under this section shall be deposited in the Treasury of the United States to the credit of the fund.

* * * * * * *

CENTRAL INTELLIGENCE AGENCY ACT OF 1949

* * * * * * *

GENERAL AUTHORITIES

SEC. 5. (a) IN GENERAL.—In the performance of its functions, the Central Intelligence Agency is authorized to—

(1) Transfer to and receive from other Government agencies such sums as may be approved by the Office of Management and Budget, for the performance of any of the functions or activities authorized under section 104A of the National Security Act of 1947 [(50 U.S.C. 403–4a).,] *(50 U.S.C. 403–4a),* and any other Government agency is authorized to transfer to or receive from the Agency such sums without regard to any provisions of law limiting or prohibiting transfers between appropriations. Sums transferred to the Agency in accordance with this paragraph may be expended for the purposes and under the authority of this Act without regard to limitations of appropriations from which transferred;

(2) Exchange funds without regard to section 3651 Revised Statutes (31 U.S.C. 543);

(3) Reimburse other Government agencies for services of personnel assigned to the Agency, and such other Government agencies are hereby authorized, without regard to provisions of law to the contrary, so to assign or detail any officer or employee for duty with the Agency;

(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 protection of classified materials and information, the training of Agency personnel and other authorized persons in the use of firearms, the protection of Agency installations and property, the protection of current and former Agency personnel and their immediate families, defectors and their immediate families, and other persons in the United States under Agency auspices, and the protection of the Director of National Intelligence and [such personnel of the Office of the Director of National Intelligence as the Director of National Intelligence may designate;] *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;*

(5) Make alterations, improvements, and repairs on premises rented by the Agency, and pay rent therefor;

(6) Determine and fix the minimum and maximum limits of age within which an original appointment may be made to an operational position within the Agency, notwithstanding the provision of any other law, in accordance with such criteria as the Director, in his discretion, may prescribe; [and]

(7) Notwithstanding section 1341(a)(1) of title 31, United States Code, enter into multiyear leases for up to 15 years[.]*; and*

(8) Upon the approval of the Director, provide, during any fiscal year, with or without reimbursement, subsistence to any personnel assigned to an overseas location designated by the Agency as an austere location.

(b) SCOPE OF AUTHORITY FOR EXPENDITURE.—(1) The authority to enter into a multiyear lease under subsection (a)(7) shall be subject to appropriations provided in advance for—

(A) the entire lease; or

(B) the first 12 months of the lease and the Government's estimated termination liability.

(2) In the case of any such lease entered into under subparagraph (B) of paragraph (1)—

(A) such lease shall include a clause that provides that the contract shall be terminated if budget authority (as defined by section 3(2) of the Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. 622(2))) is not provided specifically for that project in an appropriations Act in advance of an obligation of funds in respect thereto;

(B) notwithstanding section 1552 of title 31, United States Code, amounts obligated for paying termination costs with respect to such lease shall remain available until the costs associated with termination of such lease are paid;

(C) funds available for termination liability shall remain available to satisfy rental obligations with respect to such lease in subsequent fiscal years in the event such lease is not terminated early, but only to the extent those funds are in excess of the amount of termination liability at the time of their use to satisfy such rental obligations; and

(D) funds appropriated for a fiscal year may be used to make payments on such lease, for a maximum of 12 months, beginning any time during such fiscal year.

(c) TRANSFERS FOR ACQUISITION OF LAND.—(1) Sums appropriated or otherwise made available to the Agency for the acquisition of land that are transferred to another department or agency for that purpose shall remain available for 3 years.

(2) The Director shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on the transfer of sums described in paragraph (1) each time that authority is exercised.

* * * * * * *

RETIREMENT EQUITY FOR SPOUSES OF CERTAIN EMPLOYEES

SEC. 14. (a) The provisions of sections 102, 221(b) (1)–(3), 221(f), 221(g), [221(h)(2), 221(i), 221(l),] *221(i)(2), 221(j), 221(m),* 222, 223, 224, 225, 232(b), 241(b), 241(d), and 264(b) of the Central Intelligence Agency Retirement Act (50 U.S.C. 403 note) establishing certain requirements, limitations, rights, entitlements, and benefits relating to retirement annuities, survivor benefits, and lump-sum payments for a spouse or former spouse of an Agency employee who is a participant in the Central Intelligence Agency Retirement

and Disability System shall apply in the same manner and to the same extent in the case of an Agency employee who is a participant in the Civil Service Retirement and Disability System.

(b) The Director of the Office of Personnel Management, in consultation with the Director of the Central Intelligence Agency, shall prescribe such regulations as may be necessary to implement the provisions of this section.

SECURITY PERSONNEL AT AGENCY INSTALLATIONS

SEC. 15. (a)(1) The Director may authorize Agency personnel within the United States to perform the same functions as officers and agents of the Department of Homeland Security, as provided in section 1315(b)(2) of title 40, United States Code, with the powers set forth in that section, except that such personnel shall perform such functions and exercise such powers—

(A) within the Agency Headquarters Compound and the property controlled and occupied by the Federal Highway Administration located immediately adjacent to such Compound;

(B) in the streets, sidewalks, and the open areas within the zone beginning at the outside boundary of such Compound and property and extending outward [500 feet;] *500 yards;*

(C) within any other Agency installation and protected property; and

(D) in the streets, sidewalks, and open areas within the zone beginning at the outside boundary of any installation or property referred to in subparagraph (C) and extending outward [500 feet.] *500 yards.*

(2) The performance of functions and exercise of powers under subparagraph (B) or (D) of paragraph (1) shall be limited to those circumstances where such personnel can identify specific and articulable facts giving such personnel reason to believe that the performance of such functions and exercise of such powers is reasonable to protect against physical damage or injury, or threats of physical damage or injury, to Agency installations, property, or employees.

(3) Nothing in this subsection shall be construed to preclude, or limit in any way, the authority of any Federal, State, or local law enforcement agency, or any other Federal police or Federal protective service.

(4) The rules and regulations enforced by such personnel shall be the rules and regulations prescribed by the Director and shall only be applicable to the areas referred to in subparagraph (A) or (C) of paragraph (1).

(b) The Director is authorized to establish penalties for violations of the rules or regulations promulgated by the Director under subsection (a) of this section. Such penalties shall not exceed those specified in section 1315(c)(2) of title 40, United States Code.

(c) Agency personnel designated by the Director under subsection (a) of this section shall be clearly identifiable as United States Government security personnel while engaged in the performance of the functions to which subsection (a) of this section refers.

(d)(1) Notwithstanding any other provision of law, any Agency personnel designated by the Director under subsection (a), or designated by the Director under section 5(a)(4) to carry firearms for the protection of current or former Agency personnel and their im-

mediate families, defectors and their immediate families, and other persons in the United States under Agency auspices, shall be considered for purposes of chapter 171 of title 28, United States Code, or any other provision of law relating to tort liability, to be acting within the scope of their office or employment when such Agency personnel take reasonable action, which may include the use of force, to—

(A) protect an individual in the presence of such Agency personnel from a crime of violence;

(B) provide immediate assistance to an individual who has suffered or who is threatened with bodily harm; or

(C) prevent the escape of any individual whom such Agency personnel reasonably believe to have committed a crime of violence in the presence of such Agency personnel.

(2) Paragraph (1) shall not affect the authorities of the Attorney General under section 2679 of title 28, United States Code.

(3) In this subsection, the term "crime of violence" has the meaning given that term in section 16 of title 18, United States Code.

* * * * * * *

SEC. 19A. SPECIAL RULES FOR CERTAIN INDIVIDUALS INJURED BY REASON OF WAR, INSURGENCY, HOSTILE ACT, OR TERRORIST ACTIVITIES.

(a) DEFINITIONS.—In this section:

(1) COVERED DEPENDENT.—The term "covered dependent" means a family member (as defined by the Director) of a covered employee who, on or after September 11, 2001—

(A) accompanies the covered employee to an assigned duty station in a foreign country; and

(B) becomes injured by reason of a qualifying injury.

(2) COVERED EMPLOYEE.—The term "covered employee" means an officer or employee of the Central Intelligence Agency who, on or after September 11, 2001, becomes injured by reason of a qualifying injury.

(3) COVERED INDIVIDUAL.—The term "covered individual" means an individual who—

(A)(i) is detailed to the Central Intelligence Agency from other agencies of the United States Government or from the Armed Forces; or

(ii) is affiliated with the Central Intelligence Agency, as determined by the Director; and

(B) who, on or after September 11, 2001, becomes injured by reason of a qualifying injury.

(4) QUALIFYING INJURY.—The term "qualifying injury" means the following:

(A) With respect to a covered dependent, an injury incurred—

(i) during a period in which the covered dependent is accompanying the covered employee to an assigned duty station in a foreign country;

(ii) in connection with war, insurgency, hostile act, terrorist activity, or other incident designated by the Director; and

(iii) that was not the result of the willful misconduct of the covered dependent.

(B) With respect to a covered employee or a covered individual, an injury incurred—

(i) during a period of assignment to a duty station in a foreign country;

(ii) in connection with a war, insurgency, hostile act, terrorist activity, or other incident designated by the Director; and

(iii) that was not the result of the willful misconduct of the covered employee or the covered individual.

(b) ADJUSTMENT OF COMPENSATION FOR CERTAIN INJURIES.—

(1) INCREASE.—The Director may increase the amount of monthly compensation paid to a covered employee under section 8105 of title 5, United States Code. Subject to paragraph (2), the Director may determine the amount of each such increase by taking into account—

(A) the severity of the qualifying injury;

(B) the circumstances by which the covered employee became injured; and

(C) the seniority of the covered employee.

(2) MAXIMUM.—Notwithstanding chapter 81 of title 5, United States Code, the total amount of monthly compensation increased under paragraph (1) may not exceed the monthly pay of the maximum rate of basic pay for GS–15 of the General Schedule under section 5332 of such title.

(c) COSTS FOR TREATING QUALIFYING INJURIES.—The Director may pay the costs of treating a qualifying injury of a covered employee, a covered individual, or a covered dependent, or may reimburse a covered employee, a covered individual, or a covered dependent for such costs, that are not otherwise covered by chapter 81 of title 5, United States Code, or other provision of Federal law.

(d) TREATMENT OF AMOUNTS.—For purposes of section 104 of the Internal Revenue Code of 1986, amounts paid pursuant to this section shall be treated as amounts paid under chapter 81 of title 5, United States Code.

* * * * * * *

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2012

* * * * * * *

TITLE III

GENERAL PROVISIONS

* * * * * * *

SEC. 309. ENHANCED PROCUREMENT AUTHORITY TO MANAGE SUPPLY CHAIN RISK.

(a) DEFINITIONS.—In this section:

(1) COVERED AGENCY.—The term "covered agency" means any element of the intelligence community other than an element within the Department of Defense.

(2) COVERED ITEM OF SUPPLY.—The term "covered item of supply" means an item of information technology (as that term is defined in section 11101 of title 40, United States Code) that

is purchased for inclusion in a covered system, and the loss of integrity of which could result in a supply chain risk for a covered system.

(3) COVERED PROCUREMENT.—The term "covered procurement" means—

(A) a source selection for a covered system or a covered item of supply involving either a performance specification, as provided in section 3306(a)(3)(B) of title 41, United States Code, or an evaluation factor, as provided in section 3306(b)(1) of such title, relating to supply chain risk;

(B) the consideration of proposals for and issuance of a task or delivery order for a covered system or a covered item of supply, as provided in section 4106(d)(3) of title 41, United States Code, where the task or delivery order contract concerned includes a contract clause establishing a requirement relating to supply chain risk; or

(C) any contract action involving a contract for a covered system or a covered item of supply where such contract includes a clause establishing requirements relating to supply chain risk.

(4) COVERED PROCUREMENT ACTION.—The term "covered procurement action" means any of the following actions, if the action takes place in the course of conducting a covered procurement:

(A) The exclusion of a source that fails to meet qualifications standards established in accordance with the requirements of section 3311 of title 41, United States Code, for the purpose of reducing supply chain risk in the acquisition of covered systems.

(B) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order.

(C) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.

(5) COVERED SYSTEM.—The term "covered system" means a national security system, as that term is defined in section 3542(b) of title 44, United States Code.

(6) SUPPLY CHAIN RISK.—The term "supply chain risk" means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

(b) AUTHORITY.—Subject to subsection (c) and in consultation with the Director of National Intelligence, the head of a covered agency may, in conducting intelligence and intelligence-related activities—

(1) carry out a covered procurement action; and

(2) limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information relating to the basis for carrying out a covered procurement action.

(c) DETERMINATION AND NOTIFICATION.—The head of a covered agency may exercise the authority provided in subsection (b) only after—

(1) any appropriate consultation with procurement or other relevant officials of the covered agency;

(2) making a determination in writing, which may be in classified form, that—

(A) use of the authority in subsection (b)(1) is necessary to protect national security by reducing supply chain risk;

(B) less intrusive measures are not reasonably available to reduce such supply chain risk; and

(C) in a case where the head of the covered agency plans to limit disclosure of information under subsection (b)(2), the risk to national security due to the disclosure of such information outweighs the risk due to not disclosing such information;

(3) notifying the Director of National Intelligence that there is a significant supply chain risk to the covered system concerned, unless the head of the covered agency making the determination is the Director of National Intelligence; and

(4) providing a notice, which may be in classified form, of the determination made under paragraph (2) to the congressional intelligence committees that includes a summary of the basis for the determination, including a discussion of less intrusive measures that were considered and why they were not reasonably available to reduce supply chain risk.

(d) DELEGATION.—The head of a covered agency may not delegate the authority provided in subsection (b) or the responsibility to make a determination under subsection (c) to an official below the level of the service acquisition executive for the agency concerned.

(e) SAVINGS.—The authority under this section is in addition to any other authority under any other provision of law. The authority under this section shall not be construed to alter or effect the exercise of any other provision of law.

(f) EFFECTIVE DATE.—The requirements of this section shall take effect on the date that is 180 days after the date of the enactment of this Act and shall apply to contracts that are awarded on or after such date.

[(g) SUNSET.—The authority provided in this section shall expire on the date that section 806 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383; 10 U.S.C. 2304 note) expires.]

* * * * * * *

TITLE 5, UNITED STATES CODE

* * * * * * *

PART III—EMPLOYEES

* * * * * * *

SUBPART D—PAY AND ALLOWANCES

* * * * * * *

CHAPTER 53—PAY RATES AND SYSTEMS

* * * * * * *

SUBCHAPTER II—EXECUTIVE SCHEDULE PAY RATES

* * * * * * *

§ 5315. Positions at level IV

Level IV of the Executive Schedule applies to the following positions, for which the annual rate of basic pay shall be the rate determined with respect to such level under chapter 11 of title 2, as adjusted by section 5318 of this title:

Deputy Administrator of General Services.

Associate Administrator of the National Aeronautics and Space Administration.

Assistant Administrators, Agency for International Development (6).

Regional Assistant Administrators, Agency for International Development (4).

Assistant Secretaries of Agriculture (3).

Assistant Secretaries of Commerce (11).

Assistant Secretaries of Defense (14).

Assistant Secretaries of the Air Force (4).

Assistant Secretaries of the Army (5).

Assistant Secretaries of the Navy (4).

Assistant Secretaries of Health and Human Services (6).

Assistant Secretaries of the Interior (6).

Assistant Attorneys General (11).

Assistant Secretaries of Labor (10), one of whom shall be the Assistant Secretary of Labor for Veterans' Employment and Training.

Administrator, Wage and Hour Division, Department of Labor.

Assistant Secretaries of State (24) and 4 other State Department officials to be appointed by the President, by and with the advice and consent of the Senate.

Assistant Secretaries of the Treasury (10).

Members, United States International Trade Commission (5).

Assistant Secretaries of Education (10).

General Counsel, Department of Education.

Director of Civil Defense, Department of the Army.

Deputy Director of the Office of Emergency Planning.

Deputy Director of the Office of Science and Technology.

Deputy Director of the Peace Corps.

Assistant Directors of the Office of Management and Budget (3).

General Counsel of the Department of Agriculture.

General Counsel of the Department of Commerce.

General Counsel of the Department of Defense.

General Counsel of the Department of Health and Human Services.

Solicitor of the Department of the Interior.
Solicitor of the Department of Labor.
General Counsel of the National Labor Relations Board.
General Counsel of the Department of the Treasury.
First Vice President of the Export-Import Bank of Washington.
Members, Council of Economic Advisers.
Members, Board of Directors of the Export-Import Bank of Washington.
Members, Federal Communications Commission.
Member, Board of Directors of the Federal Deposit Insurance Corporation.
Directors, Federal Housing Finance Board.
Members, Federal Energy Regulatory Commission.
Members, Federal Trade Commission.
Members, Surface Transportation Board.
Members, National Labor Relations Board.
Members, Securities and Exchange Commission.
Members, Merit Systems Protection Board.
Members, Federal Maritime Commission.
Members, National Mediation Board.
Members, Railroad Retirement Board.
Director of Selective Service.
Associate Director of the Federal Bureau of Investigation, Department of Justice.
Members, Equal Employment Opportunity Commission (4).
Director, Community Relations Service.
Members, National Transportation Safety Board.
General Counsel, Department of Transportation.
Deputy Administrator, Federal Aviation Administration.
Assistant Secretaries of Transportation (5).
Deputy Federal Highway Administrator.
Administrator of the Saint Lawrence Seaway Development Corporation.
Assistant Secretary for Science, Smithsonian Institution.
Assistant Secretary for History and Art, Smithsonian Institution.
Deputy Administrator of the Small Business Administration.
Assistant Secretaries of Housing and Urban Development (8).
General Counsel of the Department of Housing and Urban Development.
Commissioner of Interama.
Federal Insurance Administrator, Federal Emergency Management Agency.
Executive Vice President, Overseas Private Investment Corporation.
Members, National Credit Union Administration Board (2).
Members, Postal Regulatory Commission (4).
Members, Occupational Safety and Health Review Commission.
Deputy Under Secretaries of the Treasury (or Assistant Secretaries of the Treasury) (2).
Members, Consumer Product Safety Commission (4).
Members, Commodity Futures Trading Commission.

Director of Nuclear Reactor Regulation, Nuclear Regulatory Commission.

Director of Nuclear Material Safety and Safeguards, Nuclear Regulatory Commission.

Director of Nuclear Regulatory Research, Nuclear Regulatory Commission.

Executive Director for Operations, Nuclear Regulatory Commission.

President, Government National Mortgage Association, Department of Housing and Urban Development.

Assistant Secretary of Commerce for Oceans and Atmosphere, the incumbent of which also serves as Deputy Administrator of the National Oceanic and Atmospheric Administration.

Director, Bureau of Prisons, Department of Justice.

Assistant Secretaries of Energy (8).

General Counsel of the Department of Energy.

Administrator, Economic Regulatory Administration, Department of Energy.

Administrator, Energy Information Administration, Department of Energy.

Director, Office of Indian Energy Policy and Programs, Department of Energy.

Director, Office of Science, Department of Energy.

Assistant Secretary of Labor for Mine Safety and Health.

Members, Federal Mine Safety and Health Review Commission.

President, National Consumer Cooperative Bank.

Special Counsel of the Merit Systems Protection Board.

Chairman, Federal Labor Relations Authority.

Assistant Secretaries, Department of Homeland Security.

Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency.

Assistant Director for Infrastructure Security, Cybersecurity and Infrastructure Security Agency.

General Counsel, Department of Homeland Security.

Officer for Civil Rights and Civil Liberties, Department of Homeland Security.

Chief Financial Officer, Department of Homeland Security.

Chief Information Officer, Department of Homeland Security.

Deputy Director, Institute for Scientific and Technological Cooperation.

Director of the National Institute of Justice.

Director of the Bureau of Justice Statistics.

Chief Counsel for Advocacy, Small Business Administration.

Assistant Administrator for Toxic Substances, Environmental Protection Agency.

Assistant Administrator, Office of Solid Waste, Environmental Protection Agency.

Assistant Administrators, Environmental Protection Agency (8).

Director of Operational Test and Evaluation, Department of Defense.

Director of Cost Assessment and Program Evaluation, Department of Defense.

Special Representatives of the President for arms control, nonproliferation, and disarmament matters, Department of State.

Ambassadors at Large.

Assistant Secretary of Commerce and Director General of the United States and Foreign Commercial Service.

Assistant Secretaries, Department of Veterans Affairs (7).

General Counsel, Department of Veterans Affairs.

Commissioner of Food and Drugs, Department of Health and Human Services

Chairman, Board of Veterans' Appeals.

Administrator, Office of Juvenile Justice and Delinquency Prevention.

Director, United States Marshals Service.

Chairman, United States Parole Commission.

Director, Bureau of the Census, Department of Commerce.

Director of the Institute of Museum and Library Services.

Chief Financial Officer, Department of Agriculture.

Chief Financial Officer, Department of Commerce.

Chief Financial Officer, Department of Education.

Chief Financial Officer, Department of Energy.

Chief Financial Officer, Department of Health and Human Services.

Chief Financial Officer, Department of Housing and Urban Development.

Chief Financial Officer, Department of the Interior.

Chief Financial Officer, Department of Justice.

Chief Financial Officer, Department of Labor.

Chief Financial Officer, Department of State.

Chief Financial Officer, Department of Transportation.

Chief Financial Officer, Department of the Treasury.

Chief Financial Officer, Department of Veterans Affairs.

Chief Financial Officer, Environmental Protection Agency.

Chief Financial Officer, National Aeronautics and Space Administration.

Commissioner, Office of Navajo and Hopi Indian Relocation.

Deputy Under Secretary of Defense for Research and Engineering.

Deputy Under Secretary of Defense for Acquisition and Sustainment.

Deputy Under Secretary of Defense for Policy.

Deputy Under Secretary of Defense for Personnel and Readiness.

Deputy Under Secretary of Defense (Comptroller).

Deputy Under Secretary of Defense for Intelligence.

General Counsel of the Department of the Army.

General Counsel of the Department of the Navy.

General Counsel of the Department of the Air Force.

Liaison for Community and Junior Colleges, Department of Education.

Director of the Office of Educational Technology.

Director of the International Broadcasting Bureau.

The Commissioner of Labor Statistics, Department of Labor.

Chief Information Officer, Department of Agriculture.
Chief Information Officer, Department of Commerce.
Chief Information Officer, Department of Defense (unless the official designated as the Chief Information Officer of the Department of Defense is an official listed under section 5312, 5313, or 5314 of this title).
Chief Information Officer, Department of Education.
Chief Information Officer, Department of Energy.
Chief Information Officer, Department of Health and Human Services.
Chief Information Officer, Department of Housing and Urban Development.
Chief Information Officer, Department of the Interior.
Chief Information Officer, Department of Justice.
Chief Information Officer, Department of Labor.
Chief Information Officer, Department of State.
Chief Information Officer, Department of Transportation.
Chief Information Officer, Department of the Treasury.
Chief Information Officer, Department of Veterans Affairs.
Chief Information Officer, Environmental Protection Agency.
Chief Information Officer, National Aeronautics and Space Administration.
Chief Information Officer, Agency for International Development.
Chief Information Officer, Federal Emergency Management Agency.
Chief Information Officer, General Services Administration.
Chief Information Officer, National Science Foundation.
Chief Information Officer, Nuclear Regulatory Agency.
Chief Information Officer, Office of Personnel Management.
Chief Information Officer, Small Business Administration.
Chief Information Officer of the Intelligence Community.
General Counsel of the Central Intelligence Agency.
Principal Deputy Administrator, National Nuclear Security Administration.
Additional Deputy Administrators of the National Nuclear Security Administration (3), but if the Deputy Administrator for Naval Reactors is an officer of the Navy on active duty, (2).
Deputy Under Secretary of Commerce for Intellectual Property and Deputy Director of the United States Patent and Trademark Office.
General Counsel of the Office of the Director of National Intelligence.
Chief Medical Officer, Department of Homeland Security.
Director of the National Counterintelligence and Security Center.

* * * * * * *

SUBPART J—ENHANCED PERSONNEL SECURITY PROGRAMS

* * * * * * *

CHAPTER 110—ENHANCED PERSONNEL SECURITY PROGRAMS

§ 11001. Enhanced personnel security programs

(a) ENHANCED PERSONNEL SECURITY PROGRAM.—The Director of National Intelligence shall direct each agency to implement a program to provide enhanced security review of covered individuals—

(1) in accordance with this section; and

(2) not later than the earlier of—

(A) the date that is 5 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2016; or

(B) the date on which the backlog of overdue periodic reinvestigations of covered individuals is eliminated, as determined by the Director of National Intelligence.

(b) COMPREHENSIVENESS.—

(1) SOURCES OF INFORMATION.—The enhanced personnel security program of an agency shall integrate relevant and appropriate information from various sources, including government, publicly available, and commercial data sources, consumer reporting agencies, social media, and such other sources as determined by the Director of National Intelligence.

(2) TYPES OF INFORMATION.—Information obtained and integrated from sources described in paragraph (1) may include—

(A) information relating to any criminal or civil legal proceeding;

(B) financial information relating to the covered individual, including the credit worthiness of the covered individual;

(C) publicly available information, whether electronic, printed, or other form, including relevant security or counterintelligence information about the covered individual or information that may suggest ill intent, vulnerability to blackmail, compulsive behavior, allegiance to another country, change in ideology, or that the covered individual lacks good judgment, reliability, or trustworthiness; and

(D) data maintained on any terrorist or criminal watch list maintained by any agency, State or local government, or international organization.

(c) REVIEWS OF COVERED INDIVIDUALS.—

(1) REVIEWS.—

(A) IN GENERAL.—The enhanced personnel security program of an agency shall require that, not less than 2 times every 5 years, the head of the agency shall conduct or request the conduct of automated record checks and checks of information from sources under subsection (b) to ensure the continued eligibility of each covered individual to access classified information and hold a sensitive position unless more frequent reviews of automated record checks and checks of information from sources under subsection (b) are conducted on the covered individual.

(B) SCOPE OF REVIEWS.—Except for a covered individual who is subject to more frequent reviews to ensure the continued eligibility of the covered individual to access classified information and hold a sensitive position, the reviews under subparagraph (A) shall consist of random or aperiodic checks of covered individuals, such that each covered individual is subject to at least 2 reviews during the 5-year period beginning on the date on which the agency implements the enhanced personnel security program of an agency, and during each 5-year period thereafter.

(C) INDIVIDUAL REVIEWS.—A review of the information relating to the continued eligibility of a covered individual to access classified information and hold a sensitive position under subparagraph (A) may not be conducted until after the end of the 120-day period beginning on the date the covered individual receives the notification required under paragraph (3).

(2) RESULTS.—The head of an agency shall take appropriate action if a review under paragraph (1) finds relevant information that may affect the continued eligibility of a covered individual to access classified information and hold a sensitive position.

(3) INFORMATION FOR COVERED INDIVIDUALS.—The head of an agency shall ensure that each covered individual is adequately advised of the types of relevant security or counterintelligence information the covered individual is required to report to the head of the agency.

(4) LIMITATION.—Nothing in this subsection shall be construed to affect the authority of an agency to determine the appropriate weight to be given to information relating to a covered individual in evaluating the continued eligibility of the covered individual.

(5) AUTHORITY OF THE PRESIDENT.—Nothing in this subsection shall be construed as limiting the authority of the President to direct or perpetuate periodic reinvestigations of a more comprehensive nature or to delegate the authority to direct or perpetuate such reinvestigations.

(6) EFFECT ON OTHER REVIEWS.—Reviews conducted under paragraph (1) are in addition to investigations and reinvestigations conducted pursuant to section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341).

(d) [AUDIT] *REVIEW*.—

(1) IN GENERAL.—Beginning 2 years after the date of the implementation of the enhanced personnel security program of an agency under subsection (a), the Inspector General of the agency shall conduct at least 1 [audit] *review* to assess the effectiveness and fairness, which shall be determined in accordance with performance measures and standards established by the Director of National Intelligence, to covered individuals of the enhanced personnel security program of the agency.

(2) SUBMISSIONS TO DNI.—The results of each [audit] *review* conducted under paragraph (1) shall be submitted to the Director of National Intelligence to assess the effectiveness and fairness of the enhanced personnel security programs across the Federal Government.

(e) DEFINITIONS.—In this section—

(1) the term "agency" has the meaning given that term in section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341);

(2) the term "consumer reporting agency" has the meaning given that term in section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a);

(3) the term "covered individual" means an individual employed by an agency or a contractor of an agency who has been determined eligible for access to classified information or eligible to hold a sensitive position;

(4) the term "enhanced personnel security program" means a program implemented by an agency at the direction of the Director of National Intelligence under subsection (a); and

* * * * * * *

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2005

* * * * * * *

TITLE VI—EDUCATION

* * * * * * *

Subtitle B—Improvement in Intelligence Community Foreign Language Skills

SEC. 611. FOREIGN LANGUAGE PROFICIENCY FOR CERTAIN SENIOR LEVEL POSITIONS IN THE CENTRAL INTELLIGENCE AGENCY.

(a) IN GENERAL.—Section 104A of the National Security Act of 1947, amended by section 1011(a) of the National Security Intelligence Reform Act of 2004, is further amended by adding at the end the following new subsection:

"(g) FOREIGN LANGUAGE PROFICIENCY FOR CERTAIN SENIOR LEVEL POSITIONS IN CENTRAL INTELLIGENCE AGENCY.—(1) Except as provided pursuant to paragraph (2), an individual may not be appointed to a position in the Senior Intelligence Service in the Directorate of Intelligence or the Directorate of Operations of the Central Intelligence Agency unless the Director of the Central Intelligence Agency determines that the individual—

"(A) has been certified as having a professional speaking and reading proficiency in a foreign language, such proficiency being at least level 3 on the Interagency Language Roundtable Language Skills Level or commensurate proficiency level using such other indicator of proficiency as the Director of the Central Intelligence Agency considers appropriate; and

"(B) is able to effectively communicate the priorities of the United States and exercise influence in that foreign language.

"(2) The Director of the Central Intelligence Agency may, in the discretion of the Director, waive the application of paragraph (1) to any position or category of positions otherwise covered by that

paragraph if the Director determines that foreign language proficiency is not necessary for the successful performance of the duties and responsibilities of such position or category of positions.".

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall apply with respect to appointments made on or after the date that is one year after the date of the enactment of this Act.

[(c) REPORT ON WAIVERS.—The Director of the Central Intelligence Agency shall submit to Congress a report that identifies positions within the Senior Intelligence Service in the Directorate of Intelligence or the Directorate of Operations of the Central Intelligence Agency that are determined by the Director to require waiver from the requirements of section 104A(g) of the National Security Act of 1947, as added by subsection (a). The report shall include a rationale for any waiver granted under section 104A(g)(2), as so added, for each position or category of positions so identified.]

* * * * * * *

DEPARTMENT OF ENERGY ORGANIZATION ACT

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Department of Energy Organization Act".

TABLE OF CONTENTS

TITLE II—ESTABLISHMENT OF THE DEPARTMENT

* * * * * * *

ESTABLISHMENT OF SECURITY, COUNTERINTELLIGENCE, AND INTELLIGENCE POLICIES

SEC. 214. [(a)] The Secretary shall be responsible for developing and promulgating the security, counterintelligence, and intelligence policies of the Department. The Secretary may use the immediate staff of the Secretary to assist in developing and promulgating those policies.

[(b)(1) There is within the Department an Intelligence Executive Committee. The Committee shall consist of the Deputy Secretary of Energy, who shall chair the Committee, and each Under Secretary of Energy.

[(2) The Committee shall be staffed by the Director of the Office of Intelligence and the Director of the Office of Counterintelligence.

[(3) The Secretary shall use the Committee to assist in developing and promulgating the counterintelligence and intel-

ligence policies, requirements, and priorities of the Department.

[(c) In the budget justification materials submitted to Congress in support of each budget submitted by the President to Congress under title 31, United States Code, the amounts requested for the Department for intelligence functions and the amounts requested for the Department for counterintelligence functions shall each be specified in appropriately classified individual, dedicated program elements. Within the amounts requested for counterintelligence functions, the amounts requested for the National Nuclear Security Administration shall be specified separately from the amounts requested for other elements of the Department.]

[OFFICE OF COUNTERINTELLIGENCE

[SEC. 215. (a) There is within the Department an Office of Counterintelligence.

[(b)(1) The head of the Office shall be the Director of the Office of Counterintelligence, who shall be an employee in the Senior Executive Service, the Senior Intelligence Service, the Senior National Intelligence Service, or any other Service that the Secretary, in coordination with the Director of National Intelligence, considers appropriate. The Director of the Office shall report directly to the Secretary.

[(2) The Secretary shall select the Director of the Office from among individuals who have substantial expertise in matters relating to counterintelligence.

[(3) The Director of the Federal Bureau of Investigation may detail, on a reimbursable basis, any employee of the Bureau to the Department for service as Director of the Office. The service of an employee of the Bureau as Director of the Office shall not result in any loss of status, right, or privilege by the employee within the Bureau.

[(c)(1) The Director of the Office shall be responsible for establishing policy for counterintelligence programs and activities at Department facilities in order to reduce the threat of disclosure or loss of classified and other sensitive information at such facilities.

[(2) The Director of the Office shall be responsible for establishing policy for the personnel assurance programs of the Department.

[(3) The Director shall inform the Secretary, the Director of Central Intelligence, and the Director of the Federal Bureau of Investigation on a regular basis, and upon specific request by any such official, regarding the status and effectiveness of the counterintelligence programs and activities at Department facilities.

[(d)(1) Not later than March 1 each year, the Director of the Office shall submit a report on the status and effectiveness of the counterintelligence programs and activities at each Department facility during the preceding year. Each such report shall be submitted to the following:

[(A) The Secretary.

[(B) The Director of Central Intelligence.

[(C) The Director of the Federal Bureau of Investigation.

[(D) The Committee on Armed Services and the Permanent Select Committee on Intelligence of the House of Representatives.

[(E) The Committee on Armed Services and the Select Committee on Intelligence of the Senate.

[(2) Each such report shall include for the year covered by the report the following:

[(A) A description of the status and effectiveness of the counterintelligence programs and activities at Department facilities.

[(B) A description of any violation of law or other requirement relating to intelligence, counterintelligence, or security at such facilities, including—

[(i) the number of violations that were investigated; and

[(ii) the number of violations that remain unresolved.

[(C) A description of the number of foreign visitors to Department facilities, including the locations of the visits of such visitors.

[(D) The adequacy of the Department's procedures and policies for protecting national security information, making such recommendations to Congress as may be appropriate.

[(E) A determination of whether each Department of Energy national laboratory is in full compliance with all departmental security requirements and, in the case of any such laboratory that is not, what measures are being taken to bring that laboratory into compliance.

[(3) Not less than 30 days before the date that the report required by paragraph (1) is submitted, the director of each Department of Energy national laboratory shall certify in writing to the Director of the Office whether that laboratory is in full compliance with all departmental security requirements and, if not, what measures are being taken to bring that laboratory into compliance and a schedule for implementing those measures.

[(4) Each report under this subsection as submitted to the committees referred to in subparagraphs (D) and (E) of paragraph (1) shall be submitted in unclassified form, but may include a classified annex.]

OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

SEC. 215. (a) DEFINITIONS.—In this section, the terms "intelligence community" and "National Intelligence Program" have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(b) IN GENERAL.—There is in the Department an Office of Intelligence and Counterintelligence. Such office shall be under the National Intelligence Program.

(c) DIRECTOR.—(1) The head of the Office shall be the Director of the Office of Intelligence and Counterintelligence, who shall be an employee in the Senior Executive Service, the Senior Intelligence Service, the Senior National Intelligence Service, or any other Service that the Secretary, in coordination with the Director of National Intelligence, considers appropriate. The Director of the Office shall report directly to the Secretary.

(2) The Secretary shall select an individual to serve as the Director from among individuals who have substantial expertise in matters relating to the intelligence community, including foreign intelligence and counterintelligence.

(d) DUTIES.—(1) Subject to the authority, direction, and control of the Secretary, the Director shall perform such duties and exercise such powers as the Secretary may prescribe.

(2) The Director shall be responsible for establishing policy for intelligence and counterintelligence programs and activities at the Department.

(e) ENERGY INFRASTRUCTURE SECURITY CENTER.—(1)(A) The President shall establish an Energy Infrastructure Security Center, taking into account all appropriate government tools to analyze and disseminate intelligence relating to the security of the energy infrastructure of the United States.

(B) The Director of Intelligence and Counterintelligence shall appoint the head of the Energy Infrastructure Security Center.

(C) The Energy Infrastructure Security Center shall be located within the Office of Intelligence and Counterintelligence.

(2) In establishing the Energy Infrastructure Security Center, the Director of the Office of Intelligence and Counterintelligence shall address the following missions and objectives to coordinate and disseminate intelligence relating to the security of the energy infrastructure of the United States:

(A) Establishing a primary organization within the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to the security of the energy infrastructure of the United States.

(B) Ensuring that appropriate departments and agencies have full access to and receive intelligence support needed to execute the plans or activities of the agencies, and perform independent, alternative analyses.

(C) Establishing a central repository on known and suspected foreign threats to the energy infrastructure of the United States, including with respect to any individuals, groups, or entities engaged in activities targeting such infrastructure, and the goals, strategies, capabilities, and networks of such individuals, groups, or entities.

(D) Disseminating intelligence information relating to the security of the energy infrastructure of the United States, including threats and analyses, to the President, to the appropriate departments and agencies, and to the appropriate committees of Congress.

(3) The President may waive the requirements of this subsection, and any parts thereof, if the President determines that such requirements do not materially improve the ability of the United States Government to prevent and halt attacks against the energy infrastructure of the United States. Such waiver shall be made in writing to Congress and shall include a description of how the missions and objectives in paragraph (2) are being met.

(4) If the President decides not to exercise the waiver authority granted by paragraph (3), the President shall submit to Congress from time to time updates and plans regarding the establishment of an Energy Infrastructure Security Center.

[OFFICE OF INTELLIGENCE

[SEC. 216. (a) There is within the Department an Office of Intelligence.

[(b)(1) The head of the Office shall be the Director of the Office of Intelligence, who shall be an employee in the Senior Executive Service, the Senior Intelligence Service, the Senior National Intelligence Service, or any other Service that the Secretary, in coordination with the Director of National Intelligence, considers appropriate. The Director of the Office shall report directly to the Secretary.

[(2) The Secretary shall select the Director of the Office from among individuals who have substantial expertise in matters relating to foreign intelligence.

[(c) Subject to the authority, direction, and control of the Secretary, the Director of the Office shall perform such duties and exercise such powers as the Secretary may prescribe.]

* * * * * * *

TITLE 44, UNITED STATES CODE

* * * * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

* * * * * * *

SUBCHAPTER II—INFORMATION SECURITY

* * * * * * *

§ 3553. Authority and functions of the Director and the Secretary

(a) DIRECTOR.—The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) ensuring that the Secretary carries out the authorities and functions under subsection (b);

(4) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the max-

imum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(5) overseeing agency compliance with the requirements of this subchapter and section 1326 of title 41, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; and

(6) coordinating information security policies and procedures with related information resources management policies and procedures.

(b) SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

(1) assisting the Director in carrying out the authorities and functions under paragraphs (1), (2), (3), (5), and (6) of subsection (a);

(2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be revised or repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—

(A) requirements for reporting security incidents to the Federal information security incident center established under section 3556;

(B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1);

(C) requirements for the mitigation of exigent risks to information systems; and

(D) other operational requirements as the Director or Secretary, in consultation with the Director, may determine necessary;

(3) monitoring agency implementation of information security policies and practices;

(4) convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;

(5) coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology;

(6) providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by—

(A) operating the Federal information security incident center established under section 3556;

(B) upon request by an agency, deploying, operating, and maintaining technology to assist the agency to continu-

ously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

(C) compiling and analyzing data on agency information security; and

(D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems; and

(7) other actions as the Director or the Secretary, in consultation with the Director, may determine necessary to carry out this subsection.

(c) REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—

(1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

(2) a description of the threshold for reporting major information security incidents;

(3) a summary of the results of evaluations required to be performed under section 3555;

(4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and

(5) an assessment of agency compliance with data breach notification policies and procedures issued by the Director.

(d) NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in subsection (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

(e) DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY SYSTEMS.—(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of National Intelligence in the case of systems described in paragraph (3).

(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are systems that are operated by an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

(f) CONSIDERATION.—

(1) IN GENERAL.—In carrying out the responsibilities under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of

Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40.

(2) DIRECTIVES.—The Secretary shall—

(A) consult with the Director of the National Institute of Standards and Technology regarding any binding operational directive that implements standards and guidelines developed by the National Institute of Standards and Technology; and

(B) ensure that binding operational directives issued under subsection (b)(2) do not conflict with the standards and guidelines issued under section 11331 of title 40.

(3) RULE OF CONSTRUCTION.—Nothing in this subchapter shall be construed as authorizing the Secretary to direct the Secretary of Commerce in the development and promulgation of standards and guidelines under section 11331 of title 40.

(g) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority under this section subject to direction by the President, in coordination with the Director.

(h) DIRECTION TO AGENCIES.—

(1) AUTHORITY.—

(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described subsection (d) or to a system described in paragraph (2) or (3) of subsection (e).

(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

(A) in coordination with the Director, and in consultation with Federal contractors as appropriate, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

(i) thresholds and other criteria;

(ii) privacy and civil liberties protections; and

(iii) providing notice to potentially affected third parties;

(B) specify the reasons for the required action and the duration of the directive;

(C) minimize the impact of a directive under this subsection by—

(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

(ii) limiting directives to the shortest period practicable;

(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;

(E) consult with the Director of the National Institute of Standards and Technology regarding any directive under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

(G) consider any applicable standards or guidelines developed by the National Institute of Standards and Technology issued by the Secretary of Commerce under section 11331 of title 40; and

(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

(3) IMMINENT THREATS.—

(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the use under this subsection of the intrusion detection and prevention capabilities established under section 230(b)(1) of the Homeland Security Act of 2002 for the purpose of ensuring the security of agency information systems, if—

(i) the Secretary determines there is an imminent threat to agency information systems;

(ii) the Secretary determines a directive under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

(iii) the Secretary determines the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of the intrusion detection and prevention capabilities under the control of the Secretary;

(iv) the Secretary provides prior notice to the Director, and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to this paragraph, and notifies the appropriate congressional committees and authorizing committees of each such agency within 7 days of taking an action under this paragraph of—

(I) any action taken under this paragraph; and

(II) the reasons for and duration and nature of the action;

(v) the action of the Secretary is consistent with applicable law; and

(vi) the Secretary authorizes the use of the intrusion detection and prevention capabilities in accordance with the advance procedures established under subparagraph (C).

(B) LIMITATION ON DELEGATION.—The authority under this paragraph may not be delegated by the Secretary.

(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director, and in consultation with the heads of Federal agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of the intrusion detection and prevention capabilities under subparagraph (A). The Secretary shall submit the procedures to Congress.

(4) LIMITATION.—The Secretary may direct or authorize lawful action or the use of the intrusion detection and prevention capabilities under this subsection only to—

(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

(B) require the remediation of or protect against identified information security risks with respect to—

(i) information collected or maintained by or on behalf of an agency; or

(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director and the Secretary shall submit to the appropriate congressional committees a report regarding the specific actions the Director and the Secretary have taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

(j) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Secretary to provide notice to any private entity before the Secretary issues a binding operational directive under subsection (b)(2).

[(j)**]** *(k)* APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term "appropriate congressional committees" means—

(1) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.

* * * * * * *

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2010

* * * * * * *

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

* * * * * * *

Subtitle E—Other Matters

* * * * * * *

[SEC. 368. CORRECTING LONG-STANDING MATERIAL WEAKNESSES.

[(a) DEFINITIONS.—In this section:

[(1) COVERED ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term "covered element of the intelligence community" means—

[(A) the Central Intelligence Agency;

[(B) the Defense Intelligence Agency;

[(C) the National Geospatial-Intelligence Agency;

[(D) the National Reconnaissance Office; or

[(E) the National Security Agency.

[(2) INDEPENDENT AUDITOR.—The term "independent auditor" means an individual who—

[(A)(i) is a Federal, State, or local government auditor who meets the independence standards included in generally accepted government auditing standards; or

[(ii) is a public accountant who meets such independence standards; and

[(B) is designated as an auditor by the Director of National Intelligence or the head of a covered element of the intelligence community, as appropriate.

[(3) INDEPENDENT REVIEW.—The term "independent review" means an audit, attestation, or examination conducted by an independent auditor in accordance with generally accepted government auditing standards.

[(4) LONG-STANDING, CORRECTABLE MATERIAL WEAKNESS.—The term "long-standing, correctable material weakness" means a material weakness—

[(A) that was first reported in the annual financial report of a covered element of the intelligence community for a fiscal year prior to fiscal year 2007; and

[(B) the correction of which is not substantially dependent on a business system that was not implemented prior to the end of fiscal year 2010.

[(5) MATERIAL WEAKNESS.—The term "material weakness" has the meaning given that term under the Office of Management and Budget Circular A-123, entitled "Management's Responsibility for Internal Control," revised December 21, 2004.

[(6) SENIOR INTELLIGENCE MANAGEMENT OFFICIAL.—The term "senior intelligence management official" means an official within a covered element of the intelligence community who is—

[(A)(i) compensated under the Senior Intelligence Service pay scale; or

[(ii) the head of a covered element of the intelligence community; and

[(B) compensated for employment with funds appropriated pursuant to an authorization of appropriations in this Act.

[(b) IDENTIFICATION OF SENIOR INTELLIGENCE MANAGEMENT OFFICIALS.—

[(1) REQUIREMENT TO IDENTIFY.—Not later than 30 days after the date of the enactment of this Act, the head of a covered element of the intelligence community shall designate a senior intelligence management official of such element to be responsible for correcting each long-standing, correctable material weakness of such element.

[(2) HEAD OF A COVERED ELEMENT OF THE INTELLIGENCE COMMUNITY.—The head of a covered element of the intelligence community may designate himself or herself as the senior intelligence management official responsible for correcting a long-standing, correctable material weakness under paragraph (1).

[(3) REQUIREMENT TO UPDATE DESIGNATION.—If the head of a covered element of the intelligence community determines that a senior intelligence management official designated under paragraph (1) is no longer responsible for correcting a long-standing, correctable material weakness, the head of such element shall designate the successor to such official not later than 10 days after the date of such determination.

[(c) NOTIFICATION.—Not later than 10 days after the date on which the head of a covered element of the intelligence community has designated a senior intelligence management official pursuant to paragraph (1) or (3) of subsection (b), the head of such element shall provide written notification of such designation to the Director of National Intelligence and to such senior intelligence management official.

[(d) CORRECTION OF LONG-STANDING, MATERIAL WEAKNESS.—

[(1) DETERMINATION OF CORRECTION OF DEFICIENCY.—If a long-standing, correctable material weakness is corrected, the senior intelligence management official who is responsible for correcting such long-standing, correctable material weakness shall make and issue a determination of the correction.

[(2) BASIS FOR DETERMINATION.—The determination of the senior intelligence management official under paragraph (1) shall be based on the findings of an independent review.

[(3) NOTIFICATION AND SUBMISSION OF FINDINGS.—A senior intelligence management official who makes a determination under paragraph (1) shall—

[(A) notify the head of the appropriate covered element of the intelligence community of such determination at the time the determination is made; and

[(B) ensure that the independent auditor whose findings are the basis of a determination under paragraph (1) submits to the head of the covered element of the intelligence community and the Director of National Intelligence the findings that such determination is based on not later than 5 days after the date on which such determination is made.

[(e) CONGRESSIONAL OVERSIGHT.—The head of a covered element of the intelligence community shall notify the congressional intelligence committees not later than 30 days after the date—

[(1) on which a senior intelligence management official is designated under paragraph (1) or (3) of subsection (b) and notified under subsection (c); or

[(2) of the correction of a long-standing, correctable material weakness, as verified by an independent auditor under subsection (d)(2).]

* * * * * * *

INSPECTOR GENERAL ACT OF 1978

* * * * * * *

SEC. 8H. (a)(1)(A) An employee of the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, or the National Security Agency, or of a contractor of any of those Agencies, who intends to report to Congress a complaint or information with respect to an urgent concern may report the complaint or information to the Inspector General of the Department of Defense (or designee).

(B) An employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community, who intends to report to Congress a complaint or information with respect to an urgent concern may report such complaint or information to the Inspector General of the Intelligence Community.

(C) An employee of the Federal Bureau of Investigation, or of a contractor of the Bureau, who intends to report to Congress a complaint or information with respect to an urgent concern may report the complaint or information to the Inspector General of the Department of Justice (or designee).

(D) Any other employee of, or contractor to, an executive agency, or element or unit thereof, determined by the President under section 2302(a)(2)(C)(ii) of title 5, United States Code, to have as its principal function the conduct of foreign intelligence or counterintelligence activities, who intends to report to Congress a complaint or information with respect to an urgent concern may report the complaint or information to the appropriate Inspector General (or designee) under this Act, section 17 of the Central Intelligence Agency Act of 1949, or section 103H(k) of the National Security Act of 1947 (50 U.S.C. 3033(k)).

(2) If a designee of an Inspector General under this section receives a complaint or information of an employee with respect to an urgent concern, that designee shall report the complaint or information to the Inspector General within 7 calendar days of receipt.

(3) The Inspectors General of the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency shall be designees of the Inspector General of the Department of Defense for purposes of this section.

(b)(1) Not later than the end of the 14-calendar day period beginning on the date of receipt of an employee complaint or information under subsection (a), the Inspector General shall determine whether the complaint or information appears credible. Upon making such a determination, the Inspector General shall transmit to the head of the establishment notice of that determination, together with the complaint or information.

(2) If the head of an establishment determines that a complaint or information transmitted under paragraph (1) would create a conflict of interest for the head of the establishment, the head of the establishment shall return the complaint or information to the Inspector General with that determination and the Inspector General shall make the transmission to the Director of National Intelligence and, if the establishment is within the Department of Defense, to the Secretary of Defense. In such a case, the requirements of this section for the head of the establishment apply to each recipient of the Inspector General's transmission.

(c) Upon receipt of a transmittal from the Inspector General under subsection (b), the head of the establishment shall, within 7 calendar days of such receipt, forward such transmittal to the intelligence committees, together with any comments the head of the establishment considers appropriate.

(d)(1) If the Inspector General does not find credible under subsection (b) a complaint or information submitted to the Inspector General under subsection (a), or does not transmit the complaint or information to the head of the establishment in accurate form under subsection (b), the employee (subject to paragraph (2)) may submit the complaint or information to Congress by contacting either or both of the intelligence committees directly.

(2) The employee may contact the intelligence committees directly as described in paragraph (1) only if the employee—

(A) before making such a contact, furnishes to the head of the establishment, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the intelligence committees directly; and

(B) obtains and follows from the head of the establishment, through the Inspector General, direction on how to contact the intelligence committees in accordance with appropriate security practices.

(3) A member or employee of one of the intelligence committees who receives a complaint or information under paragraph (1) does so in that member or employee's official capacity as a member or employee of that committee.

(e) The Inspector General shall notify an employee who reports a complaint or information under this section of each action taken under this section with respect to the complaint or information. Such notice shall be provided not later than 3 days after any such action is taken.

(f) An action taken by the head of an establishment or an Inspector General under subsections (a) through (e) shall not be subject to judicial review.

[(g)(1) The Inspector General of the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency shall each submit to the congressional intelligence committees each year a report that sets forth the following:

[(A) The personnel and funds requested by such Inspector General for the fiscal year beginning in such year for the activities of the office of such Inspector General in such fiscal year.

[(B) The plan of such Inspector General for such activities, including the programs and activities scheduled for review by the office of such Inspector General during such fiscal year.

[(C) An assessment of the current ability of such Inspector General to hire and retain qualified personnel for the office of such Inspector General.

[(D) Any matters that such Inspector General considers appropriate regarding the independence and effectiveness of the office of such Inspector General.

[(2) The submittal date for a report under paragraph (1) each year shall be the date provided in section 507 of the National Security Act of 1947.

[(3) In this subsection, the term "congressional intelligence committees" shall have the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 401a).]

[(h)] *(g)* An individual who has submitted a complaint or information to an Inspector General under this section may notify any member of the Permanent Select Committee on Intelligence of the House of Representatives or the Select Committee on Intelligence of the Senate, or a staff member of either such Committee, of the fact that such individual has made a submission to that particular Inspector General, and of the date on which such submission was made.

[(i)] *(h)* In this section:

(1) The term "urgent concern" means any of the following:

(A) A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters.

(B) A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity.

(C) An action, including a personnel action described in section 2302(a)(2)(A) of title 5, United States Code, constituting reprisal or threat of reprisal prohibited under section 7(c) in response to an employee's reporting an urgent concern in accordance with this section.

(2) The term "intelligence committees" means the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

* * * * * * *

PUBLIC INTEREST DECLASSIFICATION ACT OF 2000

TITLE VII—DECLASSIFICATION OF INFORMATION

* * * * * * *

SEC. 710. EFFECTIVE DATE; SUNSET.

(a) EFFECTIVE DATE.—This title shall take effect on the date that is 120 days after the date of the enactment of this Act.

(b) SUNSET.—The provisions of this title shall expire on [December 31, 2018] *December 31, 2028*.

* * * * * * *

NATIONAL NUCLEAR SECURITY ADMINISTRATION ACT

* * * * * * *

TITLE XXXII—NATIONAL NUCLEAR SECURITY ADMINISTRATION

* * * * * * *

Subtitle A—Establishment and Organization

* * * * * * *

SEC. 3212. ADMINISTRATOR FOR NUCLEAR SECURITY.

(a) IN GENERAL.—(1) There is at the head of the Administration an Administrator for Nuclear Security (in this title referred to as the "Administrator").

(2) Pursuant to subsection (c) of section 202 of the Department of Energy Organization Act (42 U.S.C. 7132), the Under Secretary for Nuclear Security of the Department of Energy serves as the Administrator.

(b) FUNCTIONS.—The Administrator has authority over, and is responsible for, all programs and activities of the Administration (except for the functions of the Deputy Administrator for Naval Reactors specified in the Executive order referred to in section 3216(b)), including the following:

(1) Strategic management.

(2) Policy development and guidance.

(3) Budget formulation, guidance, and execution, and other financial matters.

(4) Resource requirements determination and allocation.

(5) Program management and direction.

(6) Safeguards and security.

(7) Emergency management.

(8) Integrated safety management.

(9) Environment, safety, and health operations.

(10) Administration of contracts, including the management and operations of the nuclear weapons production facilities and the national security laboratories.

[(11) Intelligence.

[(12) Counterintelligence.]

[(13)] *(11)* Personnel, including the selection, appointment, distribution, supervision, establishing of compensation, and separation of personnel in accordance with subtitle C of this title.

[(14)] *(12)* Procurement of services of experts and consultants in accordance with section 3109 of title 5, United States Code.

[(15)] *(13)* Legal matters.

[(16)] *(14)* Legislative affairs.

[(17)] *(15)* Public affairs.

[(18)] *(16)* Eliminating inventories of surplus fissile materials usable for nuclear weapons.

[(19)] *(17)* Liaison with other elements of the Department of Energy and with other Federal agencies, State, tribal, and local governments, and the public.

(c) PROCUREMENT AUTHORITY.—The Administrator is the senior procurement executive for the Administration for the purposes of section 1702(c) of title 41, United States Code.

(d) POLICY AUTHORITY.—The Administrator may establish Administration-specific policies, unless disapproved by the Secretary of Energy.

(e) MEMBERSHIP ON JOINT NUCLEAR WEAPONS COUNCIL.—The Administrator serves as a member of the Joint Nuclear Weapons Council under section 179 of title 10, United States Code.

(f) REORGANIZATION AUTHORITY.—Except as provided by subsections (b) and (c) of section 3291:

(1) The Administrator may establish, abolish, alter, consolidate, or discontinue any organizational unit or component of the Administration, or transfer any function of the Administration.

(2) Such authority does not apply to the abolition of organizational units or components established by law or the transfer of functions vested by law in any organizational unit or component.

* * * * * * *

Subtitle B—Matters Relating to Security

* * * * * * *

SEC. 3233. COUNTERINTELLIGENCE PROGRAMS.

(a) NATIONAL SECURITY LABORATORIES AND NUCLEAR WEAPONS PRODUCTION FACILITIES.—The Secretary of Energy shall, at each national security laboratory and nuclear weapons production facility, establish and maintain a counterintelligence program adequate to protect national security information at that laboratory or production facility.

(b) OTHER FACILITIES.—The Secretary of Energy shall, at each [Administration] *Department* facility not described in subsection (a) at which Restricted Data is located, assign an employee of the Office of *Intelligence and* Counterintelligence of the Department of Energy who shall be responsible for and assess counterintelligence matters at that facility.

* * * * * * *

ATOMIC ENERGY DEFENSE ACT

* * * * * * *

DIVISION D—ATOMIC ENERGY DEFENSE PROVISIONS

* * * * * * *

TITLE XLV—SAFEGUARDS AND SECURITY MATTERS

* * * * * * *

Subtitle B—Classified Information

* * * * * * *

SEC. 4524. PROTECTION OF CLASSIFIED INFORMATION DURING LABORATORY-TO-LABORATORY EXCHANGES.

(a) PROVISION OF TRAINING.—The Secretary of Energy shall ensure that all Department of Energy employees and Department of Energy contractor employees participating in laboratory-to-laboratory cooperative exchange activities are fully trained in matters relating to the protection of classified information and to potential espionage and counterintelligence threats.

(b) COUNTERING OF ESPIONAGE AND INTELLIGENCE-GATHERING ABROAD.—(1) The Secretary shall establish a pool of Department employees and Department contractor employees who are specially trained to counter threats of espionage and intelligence-gathering by foreign nationals against Department employees and Department contractor employees who travel abroad for laboratory-to-laboratory exchange activities or other cooperative exchange activities on behalf of the Department.

(2) The Director of *Intelligence and* Counterintelligence of the Department of Energy may assign at least one employee from the pool established under paragraph (1) to accompany a group of Department employees or Department contractor employees who travel to any nation designated to be a sensitive country for laboratory-to-laboratory exchange activities or other cooperative exchange activities on behalf of the Department.

* * * * * * *

DISCLOSURE OF DIRECTED RULE MAKING

H.R. 3494 does not specifically direct any rule makings within the meaning of 5 U.S.C. 551.

DUPLICATION OF FEDERAL PROGRAMS

H.R. 3494 does not duplicate or reauthorize an established program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

HEARINGS

For the purposes of Section 103(i) of H. Res. 6 of the 116th Congress, the following hearings were used to develop or consider H.R. 3494—

1. The Committee held a hearing "National Security Implications of the Rise of Authoritarianism Around the World" on February 26, 2019. The Committee received testimony from the Honorable Madeleine K. Albright, the Honorable Anders Fogh Rasmussen, Dr. Teng Biao and Dr. Andrea Kendall-Taylor.
2. The Committee held a hearing "Putin's Playbook: The Kremlin's Use of Oligarchs, Money, and Intelligence in 2016 and Beyond" on Thursday, March 28, 2019. The Committee received testimony from the Honorable Michael McFaul, Mr. Steven Hall, Ms. Heather Conley, and Mr. Eric Lorber.
3. The Committee held a closed hearing "Fiscal Year 2020 Intelligence Community Budget Request Overview" on April 3, 2019.
4. The Committee held a closed hearing "Fiscal Year 2020 Central Intelligence Agency Program Budget Request Hearing" on May 2, 2019.
5. The Committee held a closed hearing "Fiscal Year 2020 National Security Program Budget Request Hearing" on May 8, 2019.
6. The Defense Intelligence and Warfighter Support Subcommittee held a closed hearing "Fiscal Year 2020 Defense Intelligence Agency and Military Services Budget Request Hearing" on May 9, 2019.
7. The Committee held a closed hearing "Compartmented FY 2020 Budget Request" on May 14, 2019.
8. The Committee held a hearing "Mission Imperative: Diversity and Inclusion in the Intelligence Community" on May 23, 2019. The Committee received testimony from the Honorable Kari Bingen, Mrs. Rita Sampson, and Mr. Harry Coker.
9. The Committee held a hearing "National Security Implications of Climate Change" on June 5, 2019. The Committee received testimony from Mr. Peter Kiemel, Mr. Jeff Ringhausen, and Dr. Rod Schoonover.
10. The Committee held a hearing "Lessons from the Mueller Report: Counterintelligence Implications of Volume 1" on June 12, 2019. The Committee received testimony from Mrs. Stephanie Douglas, Mr. Robert Anderson, and Mr. Andrew McCarthy.
11. The Committee held a hearing "National Security Challenges of Artificial Intelligence, Manipulated Media, and "Deepfakes" on June 13, 2019. The Committee received testimony from Mrs. Danielle Citron, Mr. Jack Clark, Dr. David Doermann, and Mr. Clint Watts.

In addition, the Committee held numerous briefings, roundtables, and a markup to develop and consider H.R. 3494.

○