Calendar No. 494

115TH CONGRESS
2D SESSION

S. 3153

To authorize appropriations for fiscal years 2018 and 2019 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.

IN THE SENATE OF THE UNITED STATES

JUNE 28, 2018

Mr. BURR, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

---

A BILL

To authorize appropriations for fiscal years 2018 and 2019 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.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019''.

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

SEC. 2. DEFINITIONS.

In this Act:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ''congressional intelligence com-

mittees'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

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

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—Funds are hereby authorized to be appropriated for fiscal years 2018 and 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) CERTAIN SPECIFIC AUTHORIZATION.—Funds appropriated by the Department of Defense Missile Defeat and Defense Enhancements Appropriations Act, 2018 (division B of Public Law 115–96) for intelligence or intelligence-related activities are specifically authorized by Congress for purposes of section 504 of the National Security Act of 1947 (50 U.S.C. 3094), as specified in the classified Schedule of Authorizations pursuant to section 102, and are subject to such section 504.

(c) LIMITATION ON CERTAIN WAIVERS FROM LIMITATIONS ON FUNDING OF INTELLIGENCE ACTIVITIES.—

(1) WAIVERS FOR COVERT ACTIONS.—Section 504 of the National Security Act of 1947 (50 U.S.C. 3094) is amended—

(A) by redesignating subsection (e) as subsection (f); and

(B) by inserting after subsection (d) the following:

''(e) This section cannot be waived for any covert action (as defined in section 503(e)) unless and until the Director of National Intelligence notifies the congressional intelligence committees that the action is urgent for national security purposes.''.

(2) WAIVERS FOR MAJOR SYSTEMS ACQUISITIONS.—Such section, as amended by paragraph (1), is further amended—

(A) by redesignating subsection (f) as subsection (g); and

(B) by inserting after subsection (e), as added by paragraph (1), the following:

''(f) This section cannot be waived for any major system (as defined in section 506A(e)) acquisition unless and until the Director of National Intelligence notifies the congressional intelligence committees that the action is urgent for national security purposes.''.

SEC. 102. CLASSIFIED SCHEDULES OF AUTHORIZATIONS.

(a) SPECIFICATIONS OF AMOUNTS AND PERSONNEL LEVELS.—

(1) FISCAL YEAR 2018.—The amounts authorized to be appropriated under section 101 and, subject to section 103, the authorized personnel ceilings

as of September 30, 2018, 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 for fiscal year 2018 prepared to accompany this Act.

(2) FISCAL YEAR 2019.—The amounts authorized to be appropriated under section 101 and, subject to section 103, the authorized personnel ceilings as of September 30, 2019, 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 for fiscal year 2019 prepared to accompany this Act.

(b) AVAILABILITY OF CLASSIFIED SCHEDULES OF AUTHORIZATIONS.—

(1) AVAILABILITY.—The classified Schedules 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 Schedules 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 Schedules 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. PERSONNEL CEILING ADJUSTMENTS.

(a) AUTHORITY FOR INCREASES.—The Director of National Intelligence may authorize employment of civilian personnel in excess of the number authorized for fiscal year 2018 by the classified Schedules of Authorizations referred to in section 102(a) if the Director of National Intelligence determines that such action is necessary to the performance of important intelligence functions, except that the number of personnel employed in excess of the number authorized under such section may not, for any element of the intelligence community, exceed—

(1) 3 percent of the number of civilian personnel authorized under such schedule for such element; or

(2) 10 percent of the number of civilian personnel authorized under such schedule for such element for the purposes of converting the performance of any function by contractors to performance by civilian personnel.

(b) TREATMENT OF CERTAIN PERSONNEL.—The Director of National Intelligence shall establish guidelines that govern, for each element of the intelligence community, the treatment under the personnel levels authorized under section 102(a), including any exemption from such personnel levels, of employment or assignment in—

(1) a student program, trainee program, or similar program;

(2) a reserve corps or as a reemployed annuitant; or

(3) details, joint duty, or long-term, full-time training.

(c) NOTICE TO CONGRESSIONAL INTELLIGENCE COMMITTEES.—Not later than 15 days prior to the exercise of an authority described in subsection (a), the Director of National Intelligence shall submit to the congressional intelligence committees—

(1) a written notice of the exercise of such authority; and

(2) in the case of an exercise of such authority subject to the limitation in subsection (a)(2), a written justification for the contractor conversion that includes a comparison of whole-of-government costs.

SEC. 104. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—

(1) FISCAL YEAR 2018.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2018 the sum of $546,900,000. Within such amount, funds identified in the classified Schedule of Authorizations referred to in section 102(a) for advanced research and development shall remain available until September 30, 2019.

(2) FISCAL YEAR 2019.—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 $539,624,000. Within such amount, funds identified in the classified Schedule of Authorizations referred to in section 102(a) for advanced research and de-

velopment shall remain available until September 30, 2020.

(b) AUTHORIZED PERSONNEL LEVELS.—The elements within the Intelligence Community Management Account of the Director of National Intelligence are authorized 797 positions as of September 30, 2018. Personnel serving in such elements may be permanent employees of the Office of the Director of National Intelligence or personnel detailed from other elements of the United States Government.

(c) CLASSIFIED AUTHORIZATIONS.—

(1) AUTHORIZATION OF APPROPRIATIONS.—

(A) FISCAL YEAR 2018.—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 2018 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a). Such additional amounts made available for advanced research and development shall remain available until September 30, 2019.

(B) FISCAL YEAR 2019.—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 102(a). Such additional amounts made available for advanced research and development shall remain available until September 30, 2020.

(2) AUTHORIZATION OF PERSONNEL.—In addition to the personnel authorized by subsection (b) for elements of the Intelligence Community Management Account as of September 30, 2018, there are authorized such additional personnel for the Community Management Account as of that date 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 each of fiscal years 2018 and 2019.

SEC. 202. 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 day that 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 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 that 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. 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 re-

quire 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 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. 304. 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. 305. 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 Government 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. 306. SUPPLY CHAIN AND COUNTERINTELLIGENCE RISK MANAGEMENT TASK FORCE.

(a) 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.

(b) MEMBERS.—The Supply Chain and Counterintelligence Risk Management Task Force established under subsection (a) 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) the Director of the National Counterintelligence and Security Center; and

(6) such other members as the Director of National Intelligence determines appropriate.

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

(d) ANNUAL REPORT.—

(1) IN GENERAL.—Not less frequently than once each year, the Supply Chain and Counterintelligence Risk Management Task Force established under subsection (a) shall submit to the appropriate congressional committees a 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.

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

(A) The congressional intelligence committees.

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

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

SEC. 307. 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. 308. 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 (a) 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 (a). The report shall include—

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

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

SEC. 309. MODIFICATION OF AUTHORITY RELATING TO MANAGEMENT OF SUPPLY-CHAIN RISK.

(a) MODIFICATION OF EFFECTIVE DATE.—Subsection (f) of 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 ''the date that is 180 days after''.

(b) EXTENSION.—Subsection (g) of such section is amended by striking ''the date'' and all that follows through the period and inserting ''September 30, 2023.''.

(c) REPORTS.—Such section is amended—

(1) by redesignating subsections (f) and (g), as amended by subsections (a) and (b), as subsections (g) and (h), respectively; and

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

''(f) ANNUAL REPORTS.—

''(1) IN GENERAL.—Except as provided in paragraph (2), not later than 180 days after the date of the enactment of the Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019 and not less frequently than once each calendar year thereafter, the Director of National Intelligence shall, in consultation with each head of a covered agency, submit to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), a report that details the determinations and notifications made under subsection (c) during the most recently completed calendar year.

''(2) INITIAL REPORT.—The first report submitted under paragraph (1) shall detail all the determinations and notifications made under subsection (c) before the date of the submittal of the report.''.

SEC. 310. 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 con-

sent of the Senate may not make a classification decision with respect to information related to such officer.

(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.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

SEC. 401. 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. 402. 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 Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019, each individual designated as the program manager shall be appointed by the Director of National Intelligence.''.

SEC. 403. 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.''.

Subtitle B—Other Elements

SEC. 411. 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).

SEC. 412. 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 coun-

terintelligence 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. 413. 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).''.

TITLE V—ELECTION MATTERS

SEC. 501. 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; 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) 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 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. 502. 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 classified form.

SEC. 503. 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) ASSESSMENT AND REPORT.—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 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, 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, 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. 504. STRATEGY FOR COUNTERING RUSSIAN CYBER THREATS TO UNITED STATES ELECTIONS.

(a) 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.

(b) ELEMENTS OF THE STRATEGY.—The strategy required by subsection (a) 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 (a) 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) Improvement 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) Improvement 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.

(c) CONGRESSIONAL BRIEFING.—

(1) IN GENERAL.—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 (a).

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

(A) The congressional intelligence committees.

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

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

SEC. 505. INFORMATION SHARING WITH STATE ELECTION OFFICIALS.

(a) 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.

(b) INFORMATION SHARING.—

(1) IN GENERAL.—The Director of National Intelligence shall assist the Under Secretary of Homeland Security for Intelligence and Analysis 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 (a).

(2) COORDINATION.—The Under Secretary of Homeland Security for Intelligence and Analysis shall coordinate with the Director of National Intelligence to facilitate the sharing of information to the affected Secretaries of State or States.

(c) STATE DEFINED.—In this section, the term ''State'' means any State of the United States, the Dis-

trict of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

SEC. 506. 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 VI—SECURITY CLEARANCES

SEC. 601. 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 Government Reform of the House of Representatives.

(2) COUNCIL.—The term ''Council'' means the Security, Suitability, and Credentialing Performance Accountability Council established pursuant to Executive Order 13467 (73 Fed. Reg. 38103; 50 U.S.C. 3161 note), or any successor entity.

(3) SECURITY EXECUTIVE AGENT.—The term ''Security Executive Agent'' means the Director of National Intelligence acting as the Security Executive Agent in accordance with section 605.

(4) 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 (73 Fed. Reg. 38103; 50 U.S.C. 3161 note), or any successor entity.

SEC. 602. 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 Fed-

eral 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 the following:

(A) A plan to reduce the background investigation inventory to 500,000 by the end of year 2018 and to 200,000 or an otherwise sustain-

able steady-level by the end of year 2019. 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 positions of trust 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 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 vetting, 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 a plan to implement the report's framework and recommendations submitted under paragraph (2)(A).

(4) CONGRESSIONAL NOTIFICATIONS.—Not less frequently than monthly, the Security Executive Agent shall submit a report to the appropriate congressional committees 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. 603. 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 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 support 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 of how requests for clearance sponsorship are issued;

(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 that 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.

SEC. 604. GOALS FOR PROMPTNESS OF DETERMINATIONS REGARDING SECURITY CLEARANCES.

(a) IN GENERAL.—The Council shall take such actions as may be necessary to ensure that, by December 31, 2021, 90 percent of all determinations 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 a security clearance at the same level are recognized in 2 weeks or fewer.

(b) CERTAIN REINVESTIGATIONS.—The Council shall ensure that by December 31, 2021, reinvestigation on a set periodicity is not be required for more than 10 percent of the population that holds a security clearance.

(c) PLAN.—Not later than 180 days after the date of the enactment of this Act, the Council shall submit a plan to carry out this section to the appropriate congressional committees. Such plan shall include recommended interim milestones for the goals set forth in subsections (a) and (b) for 2019, 2020, and 2021.

(d) RECIPROCITY DEFINED.—In this section, the term ''reciprocity'' means reciprocal recognition by Federal departments and agencies of eligibility for access to classified information.

SEC. 605. SECURITY EXECUTIVE AGENT.

(a) IN GENERAL.—The Director of National Intelligence 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 of August 2, 1995, as amended.

(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.

SEC. 606. REPORT ON UNIFIED, SIMPLIFIED, GOVERNMENT-WIDE 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 issue 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. 607. 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 a report to the appropriate congressional committees that describes the requirements, feasibility, and advisability of implementing a clearance in person concept described in subsection (c) for maintaining access to classified information.

(c) CLEARANCE IN PERSON CONCEPT.—The clearance in person concept—

(1) permits an individual to maintain his or her eligibility for access to classified information, networks, and facilities for up to 3 years after the individual's access to classified information would otherwise lapse; and

(2) unless otherwise directed by the Security Executive Agent, recognizes an individual's security clearance and background investigation as current, regardless of employment status.

(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. 608. BUDGET REQUEST DOCUMENTATION ON FUNDING FOR CLEARANCES.

(a) IN GENERAL.—As part of the fiscal year 2020 budget request submitted to Congress pursuant to section 1105(a) of title 31, United States Code, the President shall include exhibits that identify the resources allocated by each agency to processing security clearances, disaggregated by type of security clearance.

(b) CONTENTS.—Each exhibit submitted under subsection (a) shall include, with respect to security clearances, details on the costs of—

(1) background investigations and reinvestigations;

(2) additional screening mechanisms, such as polygraphs, medical exams, and psychological exams;

(3) adjudications;

(4) other means of continuous vetting, such as continuous evaluation and user activity monitoring; and

(5) the average per person cost for each type of security clearance.

SEC. 609. REPORTS ON RECIPROCITY FOR SECURITY CLEARANCES INSIDE OF DEPARTMENTS AND AGENCIES.

(a) 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.

(b) ANNUAL REPORT.—Not less frequently than once each year, the Security Executive Agent shall submit to the appropriate congressional committees an annual report that summarizes the information received pursuant to subsection (a) during the period covered by such report.

(c) 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.

SEC. 610. INTELLIGENCE COMMUNITY REPORTS ON SECURITY CLEARANCES.

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 adding ''and'' at the end;

(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:

''(b) INTELLIGENCE COMMUNITY REPORTS.—(1) Not later than March 1 of each year, the Director of National Intelligence shall submit a report 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 regarding the security clearances processed by each element of the intelligence community during the preceding fiscal year. Each report submitted under this paragraph 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, for each element of the intelligence community for the fiscal year covered by the report, the following:

''(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 of such adjudications that were adjudicated favorably and granted access to classified information; and

''(ii) the total number of such adjudications 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 of such adjudications that were adjudicated favorably; and

''(ii) the total number of such adjudications 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, categorized as follows:

''(i) For 180 days or shorter.

''(ii) For longer than 180 days, but shorter than 12 months.

''(iii) For 12 months or longer, but shorter than 18 months.

''(iv) For 18 months or longer, but shorter than 24 months.

''(v) For 24 months or longer.

''(F) For any 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 striking ''subsection (a)(1)'' and inserting ''subsections (a)(1) and (b)''.

SEC. 611. PERIODIC REPORT ON POSITIONS IN THE INTELLIGENCE COMMUNITY WHICH 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. 612. INFORMATION SHARING PROGRAM FOR POSITIONS OF TRUST.

(a) AGENCY DEFINED.—In this section, the term ''agency'' has the meaning given the term ''Executive agency'' in section 105 of title 5, United Stats Code.

(b) PROGRAM REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Security Executive Agent shall establish a program to share between and among agencies and industry partners of the Federal Government information regarding individuals applying for and in positions of trust, including derogatory and suitability information.

(c) GOAL.—The goal of the program required by subsection (b) shall be to alert agencies and industry partners

as to individuals who may require further vetting or should be subject to certain insider threat programs regarding granted access, or continued access, to classified information, especially when such individuals change agencies, employers, or contracts.

(d) PRIVACY SAFEGUARDS.—The Security Executive Agent shall ensure that the program required by subsection (b) includes such safeguards for privacy as the Security Executive Agent considers appropriate.

(e) PROVISION OF INFORMATION TO THE PRIVATE SECTOR.—The Security Executive Agent shall ensure that under the program required by subsection (b)—

(1) sufficient information is provided to the private sector so that employers in the private sector can make informed decisions about hiring and retention in positions of trust; and

(2) agencies and private sector entities that receive information under the program have the capabilities in place to safeguard personnel privacy in compliance with applicable law and policy.

(f) IMPLEMENTATION PLAN.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Security Executive Agent shall submit a plan to the appro-

priate congressional committees for the implementation of the program required under subsection (b).

(2) CONTENTS.—The plan required under paragraph (1) shall include—

(A) matters that address privacy, security, and human resources processes; and

(B) any recommendations of the Security Executive Agent for legislative or administrative action to carry out or improve the program.

SEC. 613. 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 evaluation programs, including those involving user activity monitoring, protect the confidentiality of whistleblower-related communications.

TITLE VII—REPORTS AND OTHER MATTERS

Subtitle A—Matters Relating to Russia and Other Foreign Powers

SEC. 701. LIMITATION RELATING TO ESTABLISHMENT OR SUPPORT OF CYBERSECURITY UNIT WITH THE GOVERNMENT OF RUSSIA.

(a) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(1) the congressional intelligence committees; and

(2) the Committee on Armed Services of the Senate and the Committee on Armed Services 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 con-

gressional 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 (a) 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 any other head of an element of the intelligence community, to share or receive foreign intelligence on a case-by-case basis.

SEC. 702. 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 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. 703. 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 individuals involved in organized crime.

(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. 704. 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; and

(B) the Committee on Armed Services of the Senate and the Committee on Armed Services 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 (a) shall include information concerning actions taken by the United States to expose or halt an attempt referred to in subsection (a).

SEC. 705. 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.

Subtitle B—Reports

SEC. 711. 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. 712. REPORTS ON AUTHORITIES OF THE CHIEF INTELLIGENCE OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) HOMELAND SECURITY INTELLIGENCE ENTERPRISE DEFINED.—In this section, 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) REQUIREMENT FOR REPORT.—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 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 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. 713. REPORT ON CYBER EXCHANGE PROGRAM.

(a) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the potential establishment of a fully voluntary exchange program between elements of the intelligence community and private technology companies under which—

(1) an employee of an element of the intelligence community with demonstrated expertise and work experience in cybersecurity or related disciplines may elect to be temporarily detailed to a private technology company that has elected to receive the detailee; and

(2) an employee of a private technology company with demonstrated expertise and work experience in cybersecurity or related disciplines may elect to be temporarily detailed to an element of the intel-

ligence community that has elected to receive the detailee.

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

(1) An assessment of the feasibility of establishing the exchange program described in such subsection.

(2) Identification of any challenges in establishing the exchange program.

(3) An evaluation of the benefits to the intelligence community that would result from the exchange program.

SEC. 714. 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) identification of the most significant benefits and drawbacks of such process with respect to the role of the Director, including any benefits or drawbacks relating to the time allotted to the Director to prepare such materials; and

(3) recommendations to improve such process.

SEC. 715. 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 of 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. 716. BIENNIAL REPORT ON FOREIGN INVESTMENT RISKS.

(a) INTELLIGENCE COMMUNITY INTERAGENCY WORKING GROUP.—

(1) REQUIREMENT TO ESTABLISH.—The Director of National Intelligence shall establish an intel-

ligence 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 biennially 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 an 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 investment 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. 717. 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; 22 U.S.C. 254a note) is amended by striking ''the number'' and inserting ''a best estimate''.

SEC. 718. 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. 719. CONGRESSIONAL NOTIFICATION OF DESIGNATION OF COVERED INTELLIGENCE OFFICER AS PERSONA NON GRATA.

(a) 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 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. 720. INSPECTORS GENERAL REPORTS ON CLASSIFICATION.

(a) REPORTS.—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.—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. 721. 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 congres-

sional 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. 722. REPORTS ON GLOBAL WATER INSECURITY AND NATIONAL SECURITY IMPLICATIONS.

(a) 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.

(b) ASSESSMENT SCOPE AND FOCUS.—Each report submitted under subsection (a) shall include an assessment of water insecurity described in such subsection with a global scope, but focus on areas of the world—

(1) of strategic, economic, or humanitarian interest to the United States—

(A) that are, as of the date of the report, at the greatest risk of instability, conflict, human insecurity, or mass displacement; or

(B) 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

(2) where challenges relating to water insecurity are likely to imperil the national security interests of the United States or allies of the United States.

(c) CONSULTATION.—In researching a report required by subsection (a), the Director shall consult with—

(1) such stakeholders within the intelligence community, the Department of Defense, and the Department of State as the Director considers appropriate; and

(2) such additional Federal agencies and persons in the private sector as the Director considers appropriate.

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

SEC. 723. 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. 724. REPEAL OF REPORT REQUIREMENT FOR INSPECTORS GENERAL OF CERTAIN ELEMENTS OF INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—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.

(b) CONFORMING AMENDMENTS.—

(1) NATIONAL SECURITY ACT OF 1947.—Section 507(a) of the National Security Act of 1947 (50 U.S.C. 3106(a)) is amended—

(A) by striking paragraph (1); and

(B) by redesignating paragraphs (2) through (5) as paragraphs (1) through (4).

(2) INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004.—Section 3001(j)(1)(C) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)(C)) is amended by striking ''and (h)'' and inserting ''and (g)''.

SEC. 725. REPEAL OF REQUIREMENT FOR ANNUAL PERSONNEL LEVEL ASSESSMENTS FOR THE INTELLIGENCE COMMUNITY.

Section 506B of the National Security Act of 1947 (50 U.S.C. 3098) is hereby repealed.

SEC. 726. REPORT ON OUTREACH STRATEGY ADDRESSING THREATS FROM UNITED STATES ADVERSARIES TO THE UNITED STATES TECHNOLOGY SECTOR.

(a) 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 En-

terprise 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.

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

(1) A review of the current outreach efforts of the intelligence community and the Defense Intelligence Enterprise described in subsection (a), 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 (a).

(B) The necessity and advisability of granting security clearances to company or community leadership, when necessary and ap-

propriate, 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 (a), 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 (a), 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 (a).

(F) Such other matters as the Director of National Intelligence may consider necessary.

(c) CONSULTATION ENCOURAGED.—In preparing the report required by subsection (a), the Director is encour-

aged to consult with other government agencies, think tanks, academia, representatives of the financial industry, or such other entities as the Director considers appropriate.

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

(e) 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 Government Reform of the House of Representatives.

SEC. 727. 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 feasibility 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. 728. 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,''.

Subtitle C—Other Matters

SEC. 731. 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);

(3) by redesignating subparagraphs (G), (H), and (I) as subparagraphs (F), (G), and (H), respectively; and

(4) in subparagraph (H), as so redesignated, by realigning the margin of such subparagraph 2 ems to the left.

SEC. 732. SECURING ENERGY 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 and the Committee on Energy and Natural Resources of the Senate; and

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

(2) COVERED ENTITY.—The term ''covered entity'' means an entity identified pursuant to section 9(a) of Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11742), relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(3) EXPLOIT.—The term ''exploit'' means a software tool designed to take advantage of a security vulnerability.

(4) INDUSTRIAL CONTROL SYSTEM.—The term ''industrial control system'' means an operational technology used to measure, control, or manage industrial functions, and includes supervisory control and data acquisition systems, distributed control systems, and programmable logic or embedded controllers.

(5) NATIONAL LABORATORY.—The term ''National Laboratory'' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(6) PROGRAM.—The term ''Program'' means the pilot program established under subsection (b).

(7) SECRETARY.—The term ''Secretary'' means the Secretary of Energy.

(8) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(b) PILOT PROGRAM FOR SECURING ENERGY INFRASTRUCTURE.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall establish a 2-year control systems implementation pilot program within the National Laboratories for the purposes of—

(1) partnering with covered entities in the energy sector (including critical component manufacturers in the supply chain) that voluntarily participate in the Program to identify new classes of security vulnerabilities of the covered entities; and

(2) evaluating technology and standards, in partnership with covered entities, to isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities, including—

(A) analog and nondigital control systems;

(B) purpose-built control systems; and

(C) physical controls.

(c) WORKING GROUP TO EVALUATE PROGRAM STANDARDS AND DEVELOP STRATEGY.—

(1) ESTABLISHMENT.—The Secretary shall establish a working group—

(A) to evaluate the technology and standards used in the Program under subsection (b)(2); and

(B) to develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities.

(2) MEMBERSHIP.—The working group established under paragraph (1) shall be composed of not fewer than 10 members, to be appointed by the Secretary, at least 1 member of which shall represent each of the following:

(A) The Department of Energy.

(B) The energy industry, including electric utilities and manufacturers recommended by the Energy Sector coordinating councils.

(C)(i) The Department of Homeland Security; or

(ii) the Industrial Control Systems Cyber Emergency Response Team.

(D) The North American Electric Reliability Corporation.

(E) The Nuclear Regulatory Commission.

(F)(i) The Office of the Director of National Intelligence; or

(ii) the intelligence community.

(G)(i) The Department of Defense; or

(ii) the Assistant Secretary of Defense for Homeland Security and America's Security Affairs.

(H) A State or regional energy agency.

(I) A national research body or academic institution.

(J) The National Laboratories.

(d) REPORTS ON THE PROGRAM.—

(1) INTERIM REPORT.—Not later than 180 days after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate congressional committees an interim report that—

(A) describes the results of the Program;

(B) includes an analysis of the feasibility of each method studied under the Program; and

(C) describes the results of the evaluations conducted by the working group established under subsection (c)(1).

(2) FINAL REPORT.—Not later than 2 years after the date on which funds are first disbursed under the Program, the Secretary shall submit to the appropriate congressional committees a final report that—

(A) describes the results of the Program;

(B) includes an analysis of the feasibility of each method studied under the Program; and

(C) describes the results of the evaluations conducted by the working group established under subsection (c)(1).

(e) EXEMPTION FROM DISCLOSURE.—Information shared by or with the Federal Government or a State, Tribal, or local government under this section—

(1) shall be deemed to be voluntarily shared information;

(2) shall be exempt from disclosure under section 552 of title 5, United States Code, or any provision of any State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law

requiring the disclosure of information or records; and

(3) shall be withheld from the public, without discretion, under section 552(b)(3) of title 5, United States Code, and any provision of any State, Tribal, or local law requiring the disclosure of information or records.

(f) PROTECTION FROM LIABILITY.—

(1) IN GENERAL.—A cause of action against a covered entity for engaging in the voluntary activities authorized under subsection (b)—

(A) shall not lie or be maintained in any court; and

(B) shall be promptly dismissed by the applicable court.

(2) VOLUNTARY ACTIVITIES.—Nothing in this section subjects any covered entity to liability for not engaging in the voluntary activities authorized under subsection (b).

(g) NO NEW REGULATORY AUTHORITY FOR FEDERAL AGENCIES.—Nothing in this section authorizes the Secretary or the head of any other department or agency of the Federal Government to issue new regulations.

(h) AUTHORIZATION OF APPROPRIATIONS.—

(1) PILOT PROGRAM.—There is authorized to be appropriated $10,000,000 to carry out subsection (b).

(2) WORKING GROUP AND REPORT.—There is authorized to be appropriated $1,500,000 to carry out subsections (c) and (d).

(3) AVAILABILITY.—Amounts made available under paragraphs (1) and (2) shall remain available until expended.

SEC. 733. SENSE OF CONGRESS ON WIKILEAKS.

It is the sense of Congress that WikiLeaks and the senior leadership of WikiLeaks resemble a nonstate hostile intelligence service often abetted by state actors and should be treated as such a service by the United States.

SEC. 734. BUG BOUNTY PROGRAMS.

(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 and the Committee on Armed Services of the Senate; and

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

(2) BUG BOUNTY PROGRAM.—The term ''bug bounty program'' means a program under which an approved computer security specialist or security researcher is temporarily authorized to identify and report vulnerabilities within the information system of an agency or department of the United States in exchange for compensation.

(3) INFORMATION SYSTEM.—The term ''information system'' has the meaning given such term in section 3502 of title 44, United States Code.

(b) BUG BOUNTY PROGRAM PLAN.—

(1) REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, in consultation with the Secretary of Defense, shall submit to the appropriate committees of Congress a strategic plan for appropriate agencies and departments of the United States to implement bug bounty programs.

(2) CONTENTS.—The plan required by paragraph (1) shall include—

(A) an assessment of—

(i) the ''Hack the Pentagon'' pilot program carried out by the Department of Defense in 2016 and subsequent bug bounty programs in identifying and reporting vulnerabilities within the information systems of the Department of Defense; and

(ii) private sector bug bounty programs, including such programs implemented by leading technology companies in the United States; and

(B) recommendations on the feasibility of initiating bug bounty programs at appropriate agencies and departments of the United States.

SEC. 735. 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.

SEC. 736. 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, 2022''.

SEC. 737. MODIFICATION OF AUTHORITIES RELATING TO THE NATIONAL INTELLIGENCE UNIVERSITY.

(a) CIVILIAN FACULTY MEMBERS; EMPLOYMENT AND COMPENSATION.—

(1) IN GENERAL.—Section 1595(c) of title 10, United States Code, is amended by adding at the end the following:

''(5) The National Intelligence University.''.

(2) COMPENSATION PLAN.—The Secretary of Defense shall provide each person employed as a professor, instructor, or lecturer at the National Intelligence University on the date of the enactment of this Act an opportunity to elect to be paid under the compensation plan in effect on the day before the

date of the enactment of this Act (with no reduction in pay) or under the authority of section 1595 of title 10, United States Code, as amended by paragraph (1).

(b) ACCEPTANCE OF FACULTY RESEARCH GRANTS.—Section 2161 of such title is amended by adding at the end the following:

''(d) ACCEPTANCE OF FACULTY RESEARCH GRANTS.—The Secretary of Defense may authorize the President of the National Intelligence University to accept qualifying research grants in the same manner and to the same degree as the President of the National Defense University under section 2165(e) of this title.''.

(c) ADMISSION OF PRIVATE SECTOR CIVILIANS.—

(1) IN GENERAL.—Chapter 108 of such title is amended by inserting after section 2167a the following:

''§ 2167b. National Intelligence University: admission of private sector civilians to receive instruction

''(a) AUTHORITY FOR ADMISSION.—(1) The Secretary of Defense may permit eligible private sector employees who work in organizations relevant to national security to receive instruction at the National Intelligence University in accordance with this section.

''(2) No more than the equivalent of 35 full-time student positions may be filled at any one time by private sector employees enrolled under this section.

''(3) Upon successful completion of the course of instruction in which enrolled, any such private sector employee may be awarded an appropriate diploma or degree under section 2161 of this title.

''(b) ELIGIBLE PRIVATE SECTOR EMPLOYEES.—(1) For purposes of this section, an eligible private sector employee is an individual employed by a private firm that is engaged in providing to the Department of Defense, the intelligence community, or other Government departments or agencies significant and substantial intelligence or defense-related systems, products, or services or whose work product is relevant to national security policy or strategy.

''(2) A private sector employee admitted for instruction at the National Intelligence University remains eligible for such instruction only so long as that person remains employed by the same firm, holds appropriate security clearances, and complies with any other applicable security protocols.

''(c) ANNUAL CERTIFICATION BY SECRETARY OF DEFENSE.—Private sector employees may receive instruction at the National Intelligence University during any academic year only if, before the start of that academic year,

the Secretary of Defense determines, and certifies to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives, that providing instruction to private sector employees under this section during that year will further the national security interests of the United States.

''(d) PROGRAM REQUIREMENTS.—The Secretary of Defense shall ensure that—

''(1) the curriculum in which private sector employees may be enrolled under this section is not readily available through other schools and concentrates on national security relevant issues; and

''(2) the course offerings at the National Intelligence University are determined by the needs of the Department of Defense and the intelligence community.

''(e) TUITION.—The President of the National Intelligence University shall charge students enrolled under this section a rate that—

''(1) is at least the rate charged for employees of the United States outside the Department of Defense, less infrastructure costs; and

''(2) considers the value to the school and course of the private sector student.

''(f) STANDARDS OF CONDUCT.—While receiving instruction at the National Intelligence University, students enrolled under this section, to the extent practicable, are subject to the same regulations governing academic performance, attendance, norms of behavior, and enrollment as apply to Government civilian employees receiving instruction at the university.

''(g) USE OF FUNDS.—(1) Amounts received by the National Intelligence University for instruction of students enrolled under this section shall be retained by the university to defray the costs of such instruction.

''(2) The source, and the disposition, of such funds shall be specifically identified in records of the university.''.

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 108 of such title is amended by inserting after the item relating to section 2167a the following:

''2167b. National Intelligence University: admission of private sector civilians to receive instruction.''.

Calendar No. 494

115TH CONGRESS
2D SESSION

S. 3153

A BILL

To authorize appropriations for fiscal years 2018 and 2019 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.

JUNE 28, 2018

Read twice and placed on the calendar