116TH CONGRESS
1ST SESSION

S. 245

To authorize appropriations for fiscal year 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.

IN THE SENATE OF THE UNITED STATES

JANUARY 28, 2019

Mr. BURR (for himself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Select Committee on Intelligence

---

A BILL

To authorize appropriations for fiscal year 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.

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 ''Damon Paul Nelson and 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 committees'' has the meaning given such term in section

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

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

SEC. 3. EXPLANATORY STATEMENT.

The explanatory statement regarding this Act, printed in the Senate section of the Congressional Record, by the Chairman of the Select Committee on Intelligence of the Senate, shall have the same effect with respect to the implementation of this Act as if it were a joint explanatory statement of a committee of conference.

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

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

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

(2) The Central Intelligence Agency.

(3) The Department of Defense.

(4) The Defense Intelligence Agency.

(5) The National Security Agency.

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

(7) The Coast Guard.

(8) The Department of State.

(9) The Department of the Treasury.

(10) The Department of Energy.

(11) The Department of Justice.

(12) The Federal Bureau of Investigation.

(13) The Drug Enforcement Administration.

(14) The National Reconnaissance Office.

(15) The National Geospatial-Intelligence Agency.

(16) The Department of Homeland Security.

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

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

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

specified in the classified Schedule of Authorizations prepared to accompany this Act.

(b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AUTHORIZATIONS.—

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

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

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

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

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

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2019 the sum of $522,424,000.

(b) CLASSIFIED AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2019 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a).

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

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

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

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

''(3) COMMENCEMENT OF SURVIVOR ANNUITY.—The annuity payable to the designated individual shall begin on the day after the retired partic-

ipant 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 which is not otherwise authorized by the Constitution or the laws of the United States.

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

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

SEC. 303. MODIFICATION OF SPECIAL PAY AUTHORITY FOR SCIENCE, TECHNOLOGY, ENGINEERING, OR MATHEMATICS POSITIONS AND ADDITION OF SPECIAL PAY AUTHORITY FOR CYBER POSITIONS.

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

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

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

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

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

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

''(2) TREATMENT.—The special rate supplements resulting from the establishment of higher

rates under paragraph (1) shall be basic pay for the same or similar purposes as those specified in section 5305(j) of title 5, United States Code.'';

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

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

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

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

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

''(B) not to exceed the rate of basic pay payable for the Vice President of the United States under section 104 of title 3, United States Code, if the Director certifies to the Sec-

retary of Defense, by name, individuals that have advanced skills and competencies and that perform critical functions that execute the cyber mission of the Agency.

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

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

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

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

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

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

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

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

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

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

SEC. 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 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) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means the following:

(1) The congressional intelligence committees.

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

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

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

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

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

(2) a representative of the General Services Administration;

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

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

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

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

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

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

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

SEC. 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 (b) may include training, advice, assistance, and other services relating to cyber attacks and hostile information collection activities.

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

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

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

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

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

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

SEC. 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) REPEAL OF SUNSET.—Such section is amended by striking subsection (g).

(c) REPORTS.—Such section, as amended by subsection (b), is further amended—

(1) by redesignating subsection (f), as amended by subsection (a), as subsection (g); 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 Damon Paul Nelson and 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 deter-

minations 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 consent of the Senate may not make a classification decision with respect to information related to such officer's nomination.

(b) CLASSIFICATION DETERMINATIONS.—

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

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

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

SEC. 311. JOINT INTELLIGENCE COMMUNITY COUNCIL.

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

(1) by striking ''regular''; and

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

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

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

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

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

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

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

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

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

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

SEC. 312. INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY ENVIRONMENT.

(a) DEFINITIONS.—In this section:

(1) CORE SERVICE.—The term ''core service'' means a capability that is available to multiple elements of the intelligence community and required

for consistent operation of the intelligence community information technology environment.

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

(b) ROLES AND RESPONSIBILITIES.—

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

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

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

(C) Documenting standards and practices of such environment.

(D) Acting as an arbiter among elements of the intelligence community related to any

disagreements arising out of the implementation of such environment.

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

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

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

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

(3) USE OF CORE SERVICES.—

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

(B) EXCEPTION.—The Director of National Intelligence may provide for a written exception to the requirement under subparagraph (A) if the Director determines there is a com-

pelling financial or mission need for such exception.

(c) MANAGEMENT ACCOUNTABILITY.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall designate and maintain one or more accountable executives of the intelligence community information technology environment to be responsible for—

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

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

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

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

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

plan for the intelligence community information technology environment.

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

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

(A) key performance parameters; and

(B) an assessment of current, measured performance.

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

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

(i) Concept refinement and technology maturity demonstration.

(ii) Development, integration, and demonstration.

(iii) Production, deployment, and sustainment.

(iv) System retirement.

(B) Dependencies of such core service capabilities.

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

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

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

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

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

(2) A uniform approach by which each element of the intelligence community shall identify the cost of legacy information technology or alternative capa-

bilities where services of the intelligence community information technology environment will also be available.

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

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

(h) ADDITIONAL NOTIFICATIONS.—The Director of National Intelligence shall provide timely notification to the congressional intelligence committees regarding any policy changes related to or affecting the intelligence community information technology environment, new initia-

tives or strategies related to or impacting such environment, and changes or deficiencies in the execution of the security plan required by subsection (d), long-term roadmap required by subsection (e), and business plan required by subsection (f).

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

SEC. 313. REPORT ON DEVELOPMENT OF SECURE MOBILE VOICE SOLUTION FOR INTELLIGENCE COMMUNITY.

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

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

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

(2) Whether the intelligence community could leverage commercially available technology for classi-

fied voice communications that operates on commercial mobile networks in a secure manner and identifying the accompanying security risks to such networks.

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

SEC. 314. POLICY ON MINIMUM INSIDER THREAT STANDARDS.

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

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

SEC. 315. SUBMISSION OF INTELLIGENCE COMMUNITY POLICIES.

(a) DEFINITIONS.—In this section:

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

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

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

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

(C) any equivalent successor policy instruments.

(b) SUBMISSION OF POLICIES.—

(1) CURRENT POLICY.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees using the electronic repository all nonpublicly available policies issued by the Director of National Intelligence for the intelligence community that are in effect as of the date of the submission.

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

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

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

SEC. 316. EXPANSION OF INTELLIGENCE COMMUNITY RECRUITMENT EFFORTS.

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

TITLE 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 Damon Paul Nelson and 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. TECHNICAL MODIFICATION TO THE EXECUTIVE SCHEDULE.

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

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

SEC. 404. CHIEF FINANCIAL OFFICER OF THE INTELLIGENCE COMMUNITY.

Section 103I(a) of the National Security Act of 1947 (50 U.S.C. 3034(a)) is amended by adding at the end the

following new sentence: ''The Chief Financial Officer shall report directly to the Director of National Intelligence.''.

SEC. 405. CHIEF INFORMATION OFFICER OF THE INTELLIGENCE COMMUNITY.

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

Subtitle B—Central Intelligence Agency

SEC. 411. CENTRAL INTELLIGENCE AGENCY SUBSISTENCE FOR PERSONNEL ASSIGNED TO AUSTERE LOCATIONS.

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

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

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

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

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

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

SEC. 412. EXPANSION OF SECURITY PROTECTIVE SERVICE JURISDICTION OF THE CENTRAL INTELLIGENCE AGENCY.

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

(1) in the subsection heading, by striking ''POLICEMEN'' and inserting ''POLICE OFFICERS''; and

(2) in paragraph (1)—

(A) in subparagraph (B), by striking ''500 feet;'' and inserting ''500 yards;''; and

(B) in subparagraph (D), by striking ''500 feet.'' and inserting ''500 yards.''.

SEC. 413. REPEAL OF FOREIGN LANGUAGE PROFICIENCY REQUIREMENT FOR CERTAIN SENIOR LEVEL POSITIONS IN THE CENTRAL INTELLIGENCE AGENCY.

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

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

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

SEC. 421. CONSOLIDATION OF DEPARTMENT OF ENERGY OFFICES OF INTELLIGENCE AND COUNTERINTELLIGENCE.

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

''OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

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

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

''(c) DIRECTOR.—(1) The head of the Office shall be the Director of the Office of Intelligence and Counterintelligence, who shall be an employee in the Senior Executive Service, the Senior Intelligence Service, the Senior National Intelligence Service, or any other Service that the

Secretary, in coordination with the Director of National Intelligence, considers appropriate. The Director of the Office shall report directly to the Secretary.

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

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

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

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

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

''215. Office of Intelligence and Counterintelligence.''.

SEC. 422. ESTABLISHMENT OF ENERGY INFRASTRUCTURE SECURITY CENTER.

Section 215 of the Department of Energy Organization Act (42 U.S.C. 7144b), as amended by section 421, is further amended by adding at the end the following:

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

''(B) The Secretary shall appoint the head of the Energy Infrastructure Security Center.

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

''(2) In establishing the Energy Infrastructure Security Center, the Director of the Office of Intelligence and Counterintelligence shall address the following missions and objectives to coordinate and disseminate intelligence relating to the security of the energy infrastructure of the United States:

''(A) Establishing a primary organization within the United States Government for analyzing and integrating all intelligence possessed or acquired by

the United States pertaining to the security of the energy infrastructure of the United States.

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

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

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

''(3) The President may waive the requirements of this subsection, and any parts thereof, if the President determines that such requirements do not materially improve the ability of the United States Government to prevent and halt attacks against the energy infrastructure of the

United States. Such waiver shall be made in writing to Congress and shall include a description of how the missions and objectives in paragraph (2) are being met.

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

SEC. 423. REPEAL OF DEPARTMENT OF ENERGY INTELLIGENCE EXECUTIVE COMMITTEE AND BUDGET REPORTING REQUIREMENT.

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

(1) by striking ''(a) DUTY OF SECRETARY.—''; and

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

Subtitle D—Other Elements

SEC. 431. PLAN FOR DESIGNATION OF COUNTERINTELLIGENCE COMPONENT OF DEFENSE SECURITY SERVICE AS AN ELEMENT OF INTELLIGENCE COMMUNITY.

Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence and Under Secretary of Defense for Intelligence, in coordination with the Director of the National Counterintelligence

and Security Center, shall submit to the congressional intelligence committees, the Committee on Armed Services of the Senate, and the Committee on Armed Services of the House of Representatives a plan to designate the counterintelligence component of the Defense Security Service of the Department of Defense as an element of the intelligence community by not later than January 1, 2019. 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. 432. NOTICE NOT REQUIRED FOR PRIVATE ENTITIES.

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

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

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

''(j) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Secretary to provide

notice to any private entity before the Secretary issues a binding operational directive under subsection (b)(2).''.

SEC. 433. FRAMEWORK FOR ROLES, MISSIONS, AND FUNCTIONS OF DEFENSE INTELLIGENCE AGENCY.

(a) IN GENERAL.—The Director of National Intelligence and the Secretary of Defense shall jointly establish a framework to ensure the appropriate balance of resources for the roles, missions, and functions of the Defense Intelligence Agency in its capacity as an element of the intelligence community and as a combat support agency. The framework shall include supporting processes to provide for the consistent and regular reevaluation of the responsibilities and resources of the Defense Intelligence Agency to prevent imbalanced priorities, insufficient or misaligned resources, and the unauthorized expansion of mission parameters.

(b) MATTERS FOR INCLUSION.—The framework required under subsection (a) shall include each of the following:

(1) A lexicon providing for consistent definitions of relevant terms used by both the intelligence community and the Department of Defense, including each of the following:

(A) Defense intelligence enterprise.

(B) Enterprise manager.

(C) Executive agent.

(D) Function.

(E) Functional manager.

(F) Mission.

(G) Mission manager.

(H) Responsibility.

(I) Role.

(J) Service of common concern.

(2) An assessment of the necessity of maintaining separate designations for the intelligence community and the Department of Defense for intelligence functional or enterprise management constructs.

(3) A repeatable process for evaluating the addition, transfer, or elimination of defense intelligence missions, roles, and functions, currently performed or to be performed in the future by the Defense Intelligence Agency, which includes each of the following:

(A) A justification for the addition, transfer, or elimination of a mission, role, or function.

(B) The identification of which, if any, element of the Federal Government performs the considered mission, role, or function.

(C) In the case of any new mission, role, or function—

(i) an assessment of the most appropriate agency or element to perform such mission, role, or function, taking into account the resource profiles, scope of responsibilities, primary customers, and existing infrastructure necessary to support such mission, role, or function; and

(ii) a determination of the appropriate resource profile and an identification of the projected resources needed and the proposed source of such resources over the future-years defense program, to be provided in writing to any elements of the intelligence community or the Department of Defense affected by the assumption, transfer, or elimination of any mission, role, or function.

(D) In the case of any mission, role, or function proposed to be assumed, transferred, or eliminated, an assessment, which shall be completed jointly by the heads of each element affected by such assumption, transfer, or elimination, of the risks that would be assumed by

the intelligence community and the Department if such mission, role, or function is assumed, transferred, or eliminated.

(E) A description of how determinations are made regarding the funding of programs and activities under the National Intelligence Program and the Military Intelligence Program, including—

(i) which programs or activities are funded under each such Program;

(ii) which programs or activities should be jointly funded under both such Programs and how determinations are made with respect to funding allocations for such programs and activities; and

(iii) the thresholds and process for changing a program or activity from being funded under one such Program to being funded under the other such Program.

SEC. 434. ESTABLISHMENT OF ADVISORY BOARD FOR NATIONAL RECONNAISSANCE OFFICE.

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

''(d) ADVISORY BOARD.—

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

''(2) DUTIES.—The Board shall—

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

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

''(3) MEMBERS.—

''(A) NUMBER AND APPOINTMENT.—

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

''(ii) NOTIFICATION.—Not later than 30 days after the date on which the Director appoints a member to the Board, the Director shall notify the congressional in-

telligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) of such appointment.

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

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

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

''(E) TRAVEL EXPENSES.—Each member shall receive travel expenses, including per diem in lieu of subsistence, in accordance with applicable provisions under subchapter I of chapter 57 of title 5, United States Code.

''(F) EXECUTIVE SECRETARY.—The Director may appoint an executive secretary, who

shall be an employee of the National Reconnaissance Office, to support the Board.

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

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

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

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

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

SEC. 435. COLLOCATION OF CERTAIN DEPARTMENT OF HOMELAND SECURITY PERSONNEL AT FIELD LOCATIONS.

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

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

TITLE 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;

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

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

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

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

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

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

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

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

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

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

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

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

(A) congressional leadership; and

(B) the appropriate congressional committees.

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

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

(2) submit the updated assessment to—

(A) congressional leadership; and

(B) the appropriate congressional committees.

SEC. 504. STRATEGY FOR COUNTERING RUSSIAN CYBER THREATS TO UNITED STATES ELECTIONS.

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

(1) The congressional intelligence committees.

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

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

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

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

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

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

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

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

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

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

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

(6) Deterrence, including actions and measures that could or should be undertaken against or com-

municated to the Government of Russia or other entities to deter attacks against, or interference with, United States election systems and processes.

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

(8) Public education and communication efforts.

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

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

SEC. 505. ASSESSMENT OF SIGNIFICANT RUSSIAN INFLUENCE CAMPAIGNS DIRECTED AT FOREIGN ELECTIONS AND REFERENDA.

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

(b) ASSESSMENT REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report containing an analytical assessment of the most significant Russian influence campaigns, if any, conducted during the 3-year period preceding the date of the enactment of this Act, as well as the most significant current or planned such Russian influence campaigns, if any. Such assessment shall include—

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

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

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

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

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

SEC. 506. FOREIGN COUNTERINTELLIGENCE AND CYBERSECURITY THREATS TO FEDERAL ELECTION CAMPAIGNS.

(a) REPORTS REQUIRED.—

(1) IN GENERAL.—As provided in paragraph (2), for each Federal election, the Director of National Intelligence, in coordination with the Under Secretary of Homeland Security for Intelligence and Analysis and the Director of the Federal Bureau of Investigation, shall make publicly available on an internet website an advisory report on foreign counterintelligence and cybersecurity threats to election campaigns for Federal offices. Each such report shall include, consistent with the protection of sources and methods, each of the following:

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

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

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

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

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

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

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

(b) TREATMENT OF CAMPAIGNS SUBJECT TO HEIGHTENED THREATS.—If the Director of the Federal

Bureau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis jointly determine that an election campaign for Federal office is subject to a heightened foreign counterintelligence or cybersecurity threat, the Director and the Under Secretary, consistent with the protection of sources and methods, may make available additional information to the appropriate representatives of such campaign.

SEC. 507. INFORMATION SHARING WITH STATE ELECTION OFFICIALS.

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

(b) SECURITY CLEARANCES.—

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

official as appropriate, at the time that such election official assumes such position.

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

(c) INFORMATION SHARING.—

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

(2) COORDINATION.—The Under Secretary of Homeland Security for Intelligence and Analysis shall coordinate with the Director of National Intel-

ligence and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department (as specified in section 103(a)(1)(H) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)(H))) to facilitate the sharing of information to the affected Secretaries of State or States.

SEC. 508. NOTIFICATION OF SIGNIFICANT FOREIGN CYBER INTRUSIONS AND ACTIVE MEASURES CAMPAIGNS DIRECTED AT ELECTIONS FOR FEDERAL OFFICES.

(a) DEFINITIONS.—In this section:

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

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

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

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

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

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

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

(A) The Federal Government.

(B) A State or local government.

(C) A political party.

(D) The election campaign of a candidate.

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

(7) HIGH CONFIDENCE.—The term ''high confidence'', with respect to a determination, means

that the determination is based on high-quality information from multiple sources.

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

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

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

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

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

subsection (c) if such Directors and the Secretary jointly determine—

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

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

(c) BRIEFING.—

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

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

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

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

(D) Any other information such Directors and the Secretary jointly determine appropriate.

(2) ELECTRONIC ELECTION INFRASTRUCTURE BRIEFINGS.—With respect to a significant foreign cyber intrusion covered by a determination under subsection (b), the Secretary of Homeland Security, in consultation with the Director of National Intelligence and the Director of the Federal Bureau of Investigation, shall offer to the owner or operator of any electronic election infrastructure directly affected by such intrusion, a briefing on such intrusion, including steps that may be taken to mitigate such intrusion. Such briefing may be classified and made available only to individuals with appropriate security clearances.

(3) PROTECTION OF SOURCES AND METHODS.—This subsection shall be carried out in a manner that is consistent with the protection of sources and methods.

SEC. 509. 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 Reform of the House of Representatives.

(2) APPROPRIATE INDUSTRY PARTNERS.—The term ''appropriate industry partner'' means a con-

tractor, licensee, or grantee (as defined in section 101(a) of Executive Order 12829 (50 U.S.C. 3161 note; relating to National Industrial Security Program)) that is participating in the National Industrial Security Program established by such Executive order.

(3) CONTINUOUS VETTING.—The term ''continuous vetting'' has the meaning given such term in Executive Order 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for government employment, fitness for contractor employees, and eligibility for access to classified national security information).

(4) COUNCIL.—The term ''Council'' means the Security, Suitability, and Credentialing Performance Accountability Council established pursuant to such Executive order, or any successor entity.

(5) SECURITY EXECUTIVE AGENT.—The term ''Security Executive Agent'' means the officer serving as the Security Executive Agent pursuant to section 803 of the National Security Act of 1947, as added by section 605.

(6) SUITABILITY AND CREDENTIALING EXECUTIVE AGENT.—The term ''Suitability and Credentialing Executive Agent'' means the Director of the Of-

fice of Personnel Management acting as the Suitability and Credentialing Executive Agent in accordance with Executive Order 13467 (50 U.S.C. 3161 note; relating to reforming processes related to suitability for government employment, fitness for contractor employees, and eligibility for access to classified national security information), or any successor entity.

SEC. 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 Federal Government is of the highest priority to national security and public safety;

(2) the President and Congress should prioritize the modernization of the personnel security framework to improve its efficiency, effectiveness, and accountability;

(3) the current system for security clearance, suitability and fitness for employment, and credentialing lacks efficiencies and capabilities to meet the current threat environment, recruit and re-

tain a trusted workforce, and capitalize on modern technologies; and

(4) changes to policies or processes to improve this system should be vetted through the Council to ensure standardization, portability, and reciprocity in security clearances across the Federal Government.

(b) ACCOUNTABILITY PLANS AND REPORTS.—

(1) PLANS.—Not later than 90 days after the date of the enactment of this Act, the Council shall submit to the appropriate congressional committees and make available to appropriate industry partners the following:

(A) A plan, with milestones, to reduce the background investigation inventory to 200,000, or an otherwise sustainable steady-level, by the end of year 2020. Such plan shall include notes of any required changes in investigative and adjudicative standards or resources.

(B) A plan to consolidate the conduct of background investigations associated with the processing for security clearances in the most effective and efficient manner between the National Background Investigation Bureau and the Defense Security Service, or a successor or-

ganization. Such plan shall address required funding, personnel, contracts, information technology, field office structure, policy, governance, schedule, transition costs, and effects on stakeholders.

(2) REPORT ON THE FUTURE OF PERSONNEL SECURITY.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Chairman of the Council, in coordination with the members of the Council, shall submit to the appropriate congressional committees and make available to appropriate industry partners a report on the future of personnel security to reflect changes in threats, the workforce, and technology.

(B) CONTENTS.—The report submitted under subparagraph (A) shall include the following:

(i) A risk framework for granting and renewing access to classified information.

(ii) A discussion of the use of technologies to prevent, detect, and monitor threats.

(iii) A discussion of efforts to address reciprocity and portability.

(iv) A discussion of the characteristics of effective insider threat programs.

(v) An analysis of how to integrate data from continuous evaluation, insider threat programs, and human resources data.

(vi) Recommendations on interagency governance.

(3) PLAN FOR IMPLEMENTATION.—Not later than 180 days after the date of the enactment of this Act, the Chairman of the Council, in coordination with the members of the Council, shall submit to the appropriate congressional committees and make available to appropriate industry partners a plan to implement the report's framework and recommendations submitted under paragraph (2)(A).

(4) CONGRESSIONAL NOTIFICATIONS.—Not less frequently than quarterly, the Security Executive Agent shall make available to the public a report regarding the status of the disposition of requests received from departments and agencies of the Federal Government for a change to, or approval under, the Federal investigative standards, the national adju-

dicative 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 and make available to appropriate industry partners a report that includes the following:

(1) A review of whether the information requested on the Questionnaire for National Security Positions (Standard Form 86) and by the Federal Investigative Standards prescribed by the Office of Personnel Management and the Office of the Director of National Intelligence appropriately supports the adjudicative guidelines under Security Executive Agent Directive 4 (known as the ''National Security Adjudicative Guidelines''). Such review shall include identification of whether any such information currently collected is unnecessary to support the adjudicative guidelines.

(2) An assessment of whether such questionnaire, standards, and guidelines should be revised to

account for the prospect of a holder of a security clearance becoming an insider threat.

(3) Recommendations to improve the background investigation process by—

(A) simplifying the Questionnaire for National Security Positions (Standard Form 86) and increasing customer support to applicants completing such questionnaire;

(B) using remote techniques and centralized locations to support or replace field investigation work;

(C) using secure and reliable digitization of information obtained during the clearance process;

(D) building the capacity of the background investigation labor sector; and

(E) replacing periodic reinvestigations with continuous evaluation techniques in all appropriate circumstances.

(b) POLICY, STRATEGY, AND IMPLEMENTATION.—Not later than 180 days after the date of the enactment of this Act, the Security Executive Agent shall, in coordination with the members of the Council, establish the following:

(1) A policy and implementation plan for the issuance of interim security clearances.

(2) A policy and implementation plan to ensure contractors are treated consistently in the security clearance process across agencies and departments of the United States as compared to employees of such agencies and departments. Such policy shall address—

(A) prioritization of processing security clearances based on the mission the contractors will be performing;

(B) standardization in the forms that agencies issue to initiate the process for a security clearance;

(C) digitization of background investigation-related forms;

(D) use of the polygraph;

(E) the application of the adjudicative guidelines under Security Executive Agent Directive 4 (known as the ''National Security Adjudicative Guidelines'');

(F) reciprocal recognition of clearances across agencies and departments of the United States, regardless of status of periodic reinvestigation;

(G) tracking of clearance files as individuals move from employment with an agency or department of the United States to employment in the private sector;

(H) collection of timelines for movement of contractors across agencies and departments;

(I) reporting on security incidents and job performance, consistent with section 552a of title 5, United States Code (commonly known as the ''Privacy Act of 1974''), that may affect the ability to hold a security clearance;

(J) any recommended changes to the Federal Acquisition Regulations (FAR) necessary to ensure that information affecting contractor clearances or suitability is appropriately and expeditiously shared between and among agencies and contractors; and

(K) portability of contractor security clearances between or among contracts at the same agency and between or among contracts at different agencies that require the same level of clearance.

(3) A strategy and implementation plan that—

(A) provides for periodic reinvestigations as part of a security clearance determination only on an as-needed, risk-based basis;

(B) includes actions to assess the extent to which automated records checks and other continuous evaluation methods may be used to expedite or focus reinvestigations; and

(C) provides an exception for certain populations if the Security Executive Agent—

(i) determines such populations require reinvestigations at regular intervals; and

(ii) provides written justification to the appropriate congressional committees for any such determination.

(4) A policy and implementation plan for agencies and departments of the United States, as a part of the security clearance process, to accept automated records checks generated pursuant to a security clearance applicant's employment with a prior employer.

(5) A policy for the use of certain background materials on individuals collected by the private sector for background investigation purposes.

(6) Uniform standards for agency continuous evaluation programs to ensure quality and reciprocity in accepting enrollment in a continuous vetting program as a substitute for a periodic investigation for continued access to classified information.

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

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

(b) IN GENERAL.—The Council shall reform the security clearance process with the objective that, by December 31, 2021, 90 percent of all determinations, other than determinations regarding populations identified under section 603(b)(3)(C), regarding—

(1) security clearances—

(A) at the secret level are issued in 30 days or fewer; and

(B) at the top secret level are issued in 90 days or fewer; and

(2) reciprocity of security clearances at the same level are recognized in 2 weeks or fewer.

(c) CERTAIN REINVESTIGATIONS.—The Council shall reform the security clearance process with the goal that

by December 31, 2021, reinvestigation on a set periodicity is not required for more than 10 percent of the population that holds a security clearance.

(d) EQUIVALENT METRICS.—

(1) IN GENERAL.—If the Council develops a set of performance metrics that it certifies to the appropriate congressional committees should achieve substantially equivalent outcomes as those outlined in subsections (b) and (c), the Council may use those metrics for purposes of compliance within this provision.

(2) NOTICE.—If the Council uses the authority provided by paragraph (1) to use metrics as described in such paragraph, the Council shall, not later than 30 days after communicating such metrics to departments and agencies, notify the appropriate congressional committees that it is using such authority.

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

SEC. 605. SECURITY EXECUTIVE AGENT.

(a) IN GENERAL.—Title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.) is amended—

(1) by redesignating sections 803 and 804 as sections 804 and 805, respectively; and

(2) by inserting after section 802 the following:

"SEC. 803. SECURITY EXECUTIVE AGENT.

''(a) IN GENERAL.—The Director of National Intelligence, or such other officer of the United States as the President may designate, shall serve as the Security Executive Agent for all departments and agencies of the United States.

''(b) DUTIES.—The duties of the Security Executive Agent are as follows:

''(1) To direct the oversight of investigations, reinvestigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information or eligibility to hold a sensitive position made by any Federal agency.

''(2) To review the national security background investigation and adjudication programs of Federal agencies to determine whether such programs are being implemented in accordance with this section.

''(3) To develop and issue uniform and consistent policies and procedures to ensure the effec-

tive, efficient, timely, and secure completion of investigations, polygraphs, and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position.

''(4) Unless otherwise designated by law, to serve as the final authority to designate a Federal agency or agencies to conduct investigations of persons who are proposed for access to classified information or for eligibility to hold a sensitive position to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position, as applicable.

''(5) Unless otherwise designated by law, to serve as the final authority to designate a Federal agency or agencies to determine eligibility for access to classified information or eligibility to hold a sensitive position in accordance with Executive Order 12968 (50 U.S.C. 3161 note; relating to access to classified information).

''(6) To ensure reciprocal recognition of eligibility for access to classified information or eligibility to hold a sensitive position among Federal agencies, including acting as the final authority to arbitrate and resolve disputes among such agencies involving

the reciprocity of investigations and adjudications of eligibility.

''(7) To execute all other duties assigned to the Security Executive Agent by law.

''(c) AUTHORITIES.—The Security Executive Agent shall—

''(1) issue guidelines and instructions to the heads of Federal agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and security in processes relating to determinations by such agencies of eligibility for access to classified information or eligibility to hold a sensitive position, including such matters as investigations, polygraphs, adjudications, and reciprocity;

''(2) have the authority to grant exceptions to, or waivers of, national security investigative requirements, including issuing implementing or clarifying guidance, as necessary;

''(3) have the authority to assign, in whole or in part, to the head of any Federal agency (solely or jointly) any of the duties of the Security Executive Agent described in subsection (b) or the authorities described in paragraphs (1) and (2), provided that the exercise of such assigned duties or authorities is subject to the oversight of the Security Executive

Agent, including such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate; and

''(4) define and set standards for continuous evaluation for continued access to classified information and for eligibility to hold a sensitive position.''.

(b) REPORT ON RECOMMENDATIONS FOR REVISING AUTHORITIES.—Not later than 30 days after the date on which the Chairman of the Council submits to the appropriate congressional committees the report required by section 602(b)(2)(A), the Chairman shall submit to the appropriate congressional committees such recommendations as the Chairman may have for revising the authorities of the Security Executive Agent.

(c) CONFORMING AMENDMENT.—Section 103H(j)(4)(A) of such Act (50 U.S.C. 3033(j)(4)(A)) is amended by striking ''in section 804'' and inserting ''in section 805''.

(d) CLERICAL AMENDMENT.—The table of contents in the matter preceding section 2 of such Act (50 U.S.C. 3002) is amended by striking the items relating to sections 803 and 804 and inserting the following:

''Sec. 803. Security Executive Agent.
''Sec. 804. Exceptions.
''Sec. 805. Definitions.''.

SEC. 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 submit to the appropriate congressional committees and make available to appropriate industry partners a report regarding the advisability and the risks, benefits, and costs to the Government and to industry of consolidating to not more than 3 tiers for positions of trust and security clearances.

SEC. 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 to the appropriate congressional committees and make available to appropriate industry partners a report that describes the requirements,

feasibility, and advisability of implementing a clearance in person concept described in subsection (c).

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

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

(2) recognizes, unless otherwise directed by the Security Executive Agent, an individual's security clearance and background investigation as current, regardless of employment status, contingent on enrollment in a continuous vetting program.

(d) CONTENTS.—The report required under subsection (b) shall address—

(1) requirements for an individual to voluntarily remain in a continuous evaluation program validated by the Security Executive Agent even if the individual is not in a position requiring access to classified information;

(2) appropriate safeguards for privacy;

(3) advantages to government and industry;

(4) the costs and savings associated with implementation;

(5) the risks of such implementation, including security and counterintelligence risks;

(6) an appropriate funding model; and

(7) fairness to small companies and independent contractors.

SEC. 608. BUDGET REQUEST DOCUMENTATION ON FUNDING FOR BACKGROUND INVESTIGATIONS.

(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 expended by each agency during the prior fiscal year for processing background investigations and continuous evaluation programs, disaggregated by tier and whether the individual was a Government employee or contractor.

(b) CONTENTS.—Each exhibit submitted under subsection (a) shall include details on—

(1) the costs of background investigations or reinvestigations;

(2) the costs associated with background investigations for Government or contract personnel;

(3) costs associated with continuous evaluation initiatives monitoring for each person for whom a

background investigation or reinvestigation was conducted, other than costs associated with adjudication;

(4) the average per person cost for each type of background investigation; and

(5) a summary of transfers and reprogrammings that were executed in the previous year to support the processing of security clearances.

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

(a) RECIPROCALLY RECOGNIZED DEFINED.—In this section, the term ''reciprocally recognized'' means reciprocal recognition by Federal departments and agencies of eligibility for access to classified information.

(b) REPORTS TO SECURITY EXECUTIVE AGENT.—The head of each Federal department or agency shall submit an annual report to the Security Executive Agent that—

(1) identifies the number of individuals whose security clearances take more than 2 weeks to be reciprocally recognized after such individuals move to another part of such department or agency; and

(2) breaks out the information described in paragraph (1) by type of clearance and the reasons for any delays.

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

SEC. 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)(A) Not later than March 1 of each year, the Director of Na-

tional Intelligence shall submit a report to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on Oversight and Reform of the House of Representatives regarding the security clearances processed by each element of the intelligence community during the preceding fiscal year.

''(B) The Director shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives such portions of the report submitted under subparagraph (A) as the Director determines address elements of the intelligence community that are within the Department of Defense.

''(C) 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)(A) 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 reinves-

tigations, 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 THAT CAN BE CONDUCTED WITHOUT ACCESS TO CLASSIFIED INFORMATION, NETWORKS, OR FACILITIES.

Not later than 180 days after the date of the enactment of this Act and not less frequently than once every 5 years thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a report that reviews the intelligence community for which positions can be conducted without access to classified in-

formation, networks, or facilities, or may only require a security clearance at the secret level.

SEC. 612. INFORMATION SHARING PROGRAM FOR POSITIONS OF TRUST AND SECURITY CLEARANCES.

(a) PROGRAM REQUIRED.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall establish and implement a program to share between and among agencies of the Federal Government and industry partners of the Federal Government relevant background information regarding individuals applying for and currently occupying national security positions and positions of trust, in order to ensure the Federal Government maintains a trusted workforce.

(2) DESIGNATION.—The program established under paragraph (1) shall be known as the ''Trusted Information Provider Program'' (in this section referred to as the ''Program'').

(b) PRIVACY SAFEGUARDS.—The Security Executive Agent and the Suitability and Credentialing Executive Agent shall ensure that the Program includes such safeguards for privacy as the Security Executive Agent and

the Suitability and Credentialing Executive Agent consider appropriate.

(c) PROVISION OF INFORMATION TO THE FEDERAL GOVERNMENT.—The Program shall include requirements that enable investigative service providers and agencies of the Federal Government to leverage certain pre-employment information gathered during the employment or military recruiting process, and other relevant security or human resources information obtained during employment with or for the Federal Government, that satisfy Federal investigative standards, while safeguarding personnel privacy.

(d) INFORMATION AND RECORDS.—The information and records considered under the Program shall include the following:

(1) Date and place of birth.

(2) Citizenship or immigration and naturalization information.

(3) Education records.

(4) Employment records.

(5) Employment or social references.

(6) Military service records.

(7) State and local law enforcement checks.

(8) Criminal history checks.

(9) Financial records or information.

(10) Foreign travel, relatives, or associations.

(11) Social media checks.

(12) Such other information or records as may be relevant to obtaining or maintaining national security, suitability, fitness, or credentialing eligibility.

(e) IMPLEMENTATION PLAN.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a plan for the implementation of the Program.

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

(A) Mechanisms that address privacy, national security, suitability or fitness, credentialing, and human resources or military recruitment processes.

(B) Such recommendations for legislative or administrative action as the Security Executive Agent and the Suitability and Credentialing Executive Agent consider appropriate to carry out or improve the Program.

(f) PLAN FOR PILOT PROGRAM ON TWO-WAY INFORMATION SHARING.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a plan for the implementation of a pilot program to assess the feasibility and advisability of expanding the Program to include the sharing of information held by the Federal Government related to contract personnel with the security office of the employers of those contractor personnel.

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

(A) Mechanisms that address privacy, national security, suitability or fitness, credentialing, and human resources or military recruitment processes.

(B) Such recommendations for legislative or administrative action as the Security Executive Agent and the Suitability and Credentialing Executive Agent consider appropriate to carry out or improve the pilot program.

(g) REVIEW.—Not later than 1 year after the date of the enactment of this Act, the Security Executive Agent and the Suitability and Credentialing Executive Agent shall jointly submit to the appropriate congressional committees and make available to appropriate industry partners a review of the plans submitted under subsections (e)(1) and (f)(1) and utility and effectiveness of the programs described in such plans.

SEC. 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 vetting 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 RUSSIAN FEDERATION.

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

(1) the congressional intelligence committees;

(2) the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and

(3) the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(b) LIMITATION.—

(1) IN GENERAL.—No amount may be expended by the Federal Government, other than the Department of Defense, to enter into or implement any bilateral agreement between the United States and the Russian Federation regarding cybersecurity, including the establishment or support of any cybersecurity unit, unless, at least 30 days prior to the

conclusion of any such agreement, the Director of National Intelligence submits to the appropriate congressional committees a report on such agreement that includes the elements required by subsection (c).

(2) DEPARTMENT OF DEFENSE AGREEMENTS.—Any agreement between the Department of Defense and the Russian Federation regarding cybersecurity shall be conducted in accordance with section 1232 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328), as amended by section 1231 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91).

(c) ELEMENTS.—If the Director submits a report under subsection (b) with respect to an agreement, such report shall include a description of each of the following:

(1) The purpose of the agreement.

(2) The nature of any intelligence to be shared pursuant to the agreement.

(3) The expected value to national security resulting from the implementation of the agreement.

(4) Such counterintelligence concerns associated with the agreement as the Director may have and

such measures as the Director expects to be taken to mitigate such concerns.

(d) RULE OF CONSTRUCTION.—This section shall not be construed to affect any existing authority of the Director of National Intelligence, the Director of the Central Intelligence Agency, or another head of an element of the intelligence community, to share or receive foreign intelligence on a case-by-case basis.

SEC. 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, and the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives (only with respect to the unclassified report), a report on the intel-

ligence 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 organized criminals.

(2) An assessment with respect to any trends or patterns in threat finance activities relating to Russia, including common methods of conducting such activities and global nodes of money laundering used by Russian threat actors described in paragraph (1) and associated entities.

(3) An assessment of any connections between Russian individuals involved in money laundering and the Government of Russia.

(4) A summary of engagement and coordination with international partners on threat finance relating to Russia, especially in Europe, including examples of such engagement and coordination.

(5) An identification of any resource and collection gaps.

(6) An identification of—

(A) entry points of money laundering by Russian and associated entities into the United States;

(B) any vulnerabilities within the United States legal and financial system, including specific sectors, which have been or could be exploited in connection with Russian threat finance activities; and

(C) the counterintelligence threat posed by Russian money laundering and other forms of threat finance, as well as the threat to the United States financial system and United States efforts to enforce sanctions and combat organized crime.

(7) Any other matters the Director determines appropriate.

(d) FORM OF REPORT.—The report required under subsection (b) may be submitted in classified form.

SEC. 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;

(B) the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and

(C) the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

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

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

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

(b) REQUIREMENT FOR NOTIFICATION.—The Director of National Intelligence, in cooperation with the Director of the Federal Bureau of Investigation and the head of any other relevant agency, shall notify the congressional leadership and the Chairman and Vice Chairman or Ranking Member of each of the appropriate congressional committees, and of other relevant committees of jurisdiction, each time the Director of National Intelligence determines there is credible information that a foreign power has, is, or will attempt to employ a covert influence or active measures campaign with regard to the modernization, employment, doctrine, or force posture of the nuclear deterrent or missile defense.

(c) CONTENT OF NOTIFICATION.—Each notification required by subsection (b) shall include information concerning actions taken by the United States to expose or halt an attempt referred to in subsection (b).

SEC. 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.

SEC. 706. REPORT ON OUTREACH STRATEGY ADDRESSING THREATS FROM UNITED STATES ADVERSARIES TO THE UNITED STATES TECHNOLOGY SECTOR.

(a) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

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

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

(b) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report detailing outreach by the intelligence community and the Defense Intelligence Enterprise to United States industrial, commercial, scientific, technical, and academic communities on matters relating to the efforts of adversaries of the United States to acquire critical United States technology, intellectual property, and research and development information.

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

(1) A review of the current outreach efforts of the intelligence community and the Defense Intelligence Enterprise described in subsection (b), including the type of information conveyed in the outreach.

(2) A determination of the appropriate element of the intelligence community to lead such outreach efforts.

(3) An assessment of potential methods for improving the effectiveness of such outreach, including an assessment of the following:

(A) Those critical technologies, infrastructure, or related supply chains that are at risk from the efforts of adversaries described in subsection (b).

(B) The necessity and advisability of granting security clearances to company or community leadership, when necessary and appropriate, to allow for tailored classified briefings on specific targeted threats.

(C) The advisability of partnering with entities of the Federal Government that are not elements of the intelligence community and relevant regulatory and industry groups described in subsection (b), to convey key messages across sectors targeted by United States adversaries.

(D) Strategies to assist affected elements of the communities described in subparagraph (C) in mitigating, deterring, and protecting against the broad range of threats from the ef-

forts of adversaries described in subsection (b), with focus on producing information that enables private entities to justify business decisions related to national security concerns.

(E) The advisability of the establishment of a United States Governmentwide task force to coordinate outreach and activities to combat the threats from efforts of adversaries described in subsection (b).

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

(d) CONSULTATION ENCOURAGED.—In preparing the report required by subsection (b), the Director is encouraged to consult with other government agencies, think tanks, academia, representatives of the financial industry, or such other entities as the Director considers appropriate.

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

SEC. 707. REPORT ON IRANIAN SUPPORT OF PROXY FORCES IN SYRIA AND LEBANON.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Armed Services, the Committee on Foreign Relations, and the Select Committee on Intelligence of the Senate; and

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

(2) ARMS OR RELATED MATERIAL.—The term ''arms or related material'' means—

(A) nuclear, biological, chemical, or radiological weapons or materials or components of such weapons;

(B) ballistic or cruise missile weapons or materials or components of such weapons;

(C) destabilizing numbers and types of advanced conventional weapons;

(D) defense articles or defense services, as those terms are defined in paragraphs (3) and (4), respectively, of section 47 of the Arms Export Control Act (22 U.S.C. 2794);

(E) defense information, as that term is defined in section 644 of the Foreign Assistance Act of 1961 (22 U.S.C. 2403); or

(F) items designated by the President for purposes of the United States Munitions List under section 38(a)(1) of the Arms Export Control Act (22 U.S.C. 2778(a)(1)).

(b) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report on Iranian support of proxy forces in Syria and Lebanon and the threat posed to Israel, other United States regional allies, and other specified interests of the United States as a result of such support.

(c) MATTERS FOR INCLUSION.—The report required under subsection (b) shall include information relating to the following matters with respect to both the strategic and tactical implications for the United States and its allies:

(1) A description of arms or related materiel transferred by Iran to Hizballah since March 2011, including the number of such arms or related materiel and whether such transfer was by land, sea, or

air, as well as financial and additional technological capabilities transferred by Iran to Hizballah.

(2) A description of Iranian and Iranian-controlled personnel, including Hizballah, Shiite militias, and Iran's Revolutionary Guard Corps forces, operating within Syria, including the number and geographic distribution of such personnel operating within 30 kilometers of the Israeli borders with Syria and Lebanon.

(3) An assessment of Hizballah's operational lessons learned based on its recent experiences in Syria.

(4) A description of any rocket-producing facilities in Lebanon for nonstate actors, including whether such facilities were assessed to be built at the direction of Hizballah leadership, Iranian leadership, or in consultation between Iranian leadership and Hizballah leadership.

(5) An analysis of the foreign and domestic supply chains that significantly facilitate, support, or otherwise aid Hizballah's acquisition or development of missile production facilities, including the geographic distribution of such foreign and domestic supply chains.

(6) An assessment of the provision of goods, services, or technology transferred by Iran or its affiliates to Hizballah to indigenously manufacture or otherwise produce missiles.

(7) An identification of foreign persons that are based on credible information, facilitating the transfer of significant financial support or arms or related materiel to Hizballah.

(8) A description of the threat posed to Israel and other United States allies in the Middle East by the transfer of arms or related material or other support offered to Hizballah and other proxies from Iran.

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

SEC. 708. ANNUAL REPORT ON IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.

(a) ANNUAL REPORT REQUIRED.—Not later than 90 days after the date of the enactment of this Act and not less frequently than once each year thereafter, the Director of National Intelligence shall submit to Congress a report describing Iranian expenditures in the previous cal-

endar year on military and terrorist activities outside the country, including each of the following:

(1) The amount spent in such calendar year on activities by the Islamic Revolutionary Guard Corps, including activities providing support for—

(A) Hizballah;

(B) Houthi rebels in Yemen;

(C) Hamas;

(D) proxy forces in Iraq and Syria; or

(E) any other entity or country the Director determines to be relevant.

(2) The amount spent in such calendar year for ballistic missile research and testing or other activities that the Director determines are destabilizing to the Middle East region.

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

SEC. 709. EXPANSION OF SCOPE OF COMMITTEE TO COUNTER ACTIVE MEASURES AND REPORT ON ESTABLISHMENT OF FOREIGN MALIGN INFLUENCE CENTER.

(a) SCOPE OF COMMITTEE TO COUNTER ACTIVE MEASURES.—

(1) IN GENERAL.—Section 501 of the Intelligence Authorization Act for Fiscal Year 2017 (Public Law 115–31; 50 U.S.C. 3001 note) is amended—

(A) in subsections (a) through (h)—

(i) by inserting ", the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or other nation state" after "Russian Federation" each place it appears; and

(ii) by inserting ", China, Iran, North Korea, or other nation state" after "Russia" each place it appears; and

(B) in the section heading, by inserting "**, THE PEOPLE'S REPUBLIC OF CHINA, THE ISLAMIC REPUBLIC OF IRAN, THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA, OR OTHER NATION STATE**" after "**RUSSIAN FEDERATION**".

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 501 and inserting the following new item:

''Sec. 501. Committee to counter active measures by the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, and other nation states to exert covert influence over peoples and governments.''.

(b) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with such elements of the intelligence community as the Director considers relevant, shall submit to the congressional intelligence committees a report on the feasibility and advisability of establishing a center, to be known as the ''Foreign Malign Influence Response Center'', that—

(A) is comprised of analysts from all appropriate elements of the intelligence community, including elements with related diplomatic and law enforcement functions;

(B) has access to all intelligence and other reporting acquired by the United States Government on foreign efforts to influence, through overt and covert malign activities, United States political processes and elections;

(C) provides comprehensive assessment, and indications and warning, of such activities; and

(D) provides for enhanced dissemination of such assessment to United States policy makers.

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

(A) A discussion of the desirability of the establishment of such center and any barriers to such establishment.

(B) Such recommendations and other matters as the Director considers appropriate.

Subtitle B—Reports

SEC. 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) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

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

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

(2) HOMELAND SECURITY INTELLIGENCE ENTERPRISE.—The term ''Homeland Security Intelligence Enterprise'' has the meaning given such term in Department of Homeland Security Instruction Number 264–01–001, or successor authority.

(b) REPORT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security, in consultation with the Under Secretary of Homeland Security for Intelligence and Analysis, shall submit to the appropriate committees of Congress a report on the authorities of the Under Secretary.

(c) ELEMENTS.—The report required by subsection (b) shall include each of the following:

(1) An analysis of whether the Under Secretary has the legal and policy authority necessary to organize and lead the Homeland Security Intelligence

Enterprise, with respect to intelligence, and, if not, a description of—

(A) the obstacles to exercising the authorities of the Chief Intelligence Officer of the Department and the Homeland Security Intelligence Council, of which the Chief Intelligence Officer is the chair; and

(B) the legal and policy changes necessary to effectively coordinate, organize, and lead intelligence activities of the Department of Homeland Security.

(2) A description of the actions that the Secretary has taken to address the inability of the Under Secretary to require components of the Department, other than the Office of Intelligence and Analysis of the Department to—

(A) coordinate intelligence programs; and

(B) integrate and standardize intelligence products produced by such other components.

SEC. 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 intelligence 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. REVIEW OF INTELLIGENCE COMMUNITY WHISTLEBLOWER MATTERS.

(a) REVIEW OF WHISTLEBLOWER MATTERS.—The Inspector General of the Intelligence Community, in consultation with the inspectors general for the Central Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the Defense Intelligence Agency, and the National Reconnaissance Office, shall conduct a review of the authorities, policies, investigatory standards, and other practices and procedures relating to intelligence community whistleblower matters, with respect to such inspectors general.

(b) OBJECTIVE OF REVIEW.—The objective of the review required under subsection (a) is to identify any discrepancies, inconsistencies, or other issues, which frustrate the timely and effective reporting of intelligence community whistleblower matters to appropriate inspectors general and to the congressional intelligence committees, and the fair and expeditious investigation and resolution of such matters.

(c) CONDUCT OF REVIEW.—The Inspector General of the Intelligence Community shall take such measures as the Inspector General determines necessary in order to ensure that the review required by subsection (a) is conducted in an independent and objective fashion.

(d) REPORT.—Not later than 270 days after the date of the enactment of this Act, the Inspector General of the Intelligence Community shall submit to the congressional intelligence committees a written report containing the results of the review required under subsection (a), along with recommendations to improve the timely and effective reporting of intelligence community whistleblower matters to inspectors general and to the congressional intelligence committees and the fair and expeditious investigation and resolution of such matters.

SEC. 715. REPORT ON ROLE OF DIRECTOR OF NATIONAL INTELLIGENCE WITH RESPECT TO CERTAIN FOREIGN INVESTMENTS.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community determined appropriate by the Director, shall submit to the congressional intelligence committees a report on the role of the Director in preparing analytic materials in connection with the evaluation by the Federal Government of national security risks associated with potential foreign investments into the United States.

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

(1) a description of the current process for the provision of the analytic materials described in subsection (a);

(2) an identification of the most significant benefits and drawbacks of such process with respect to the role of the Director, including the sufficiency of resources and personnel to prepare such materials; and

(3) recommendations to improve such process.

SEC. 716. REPORT ON SURVEILLANCE BY FOREIGN GOVERNMENTS AGAINST UNITED STATES TELECOMMUNICATIONS NETWORKS.

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

(1) The congressional intelligence committees.

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

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

(b) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in coordination with the Director of the

Central Intelligence Agency, the Director of the National Security Agency, the Director of the Federal Bureau of Investigation, and the Secretary of Homeland Security, submit to the appropriate congressional committees a report describing—

(1) any attempts known to the intelligence community by foreign governments to exploit cybersecurity vulnerabilities in United States telecommunications networks (including Signaling System No. 7) to target for surveillance United States persons, including employees of the Federal Government; and

(2) any actions, as of the date of the enactment of this Act, taken by the intelligence community to protect agencies and personnel of the United States Government from surveillance conducted by foreign governments.

SEC. 717. BIENNIAL REPORT ON FOREIGN INVESTMENT RISKS.

(a) INTELLIGENCE COMMUNITY INTERAGENCY WORKING GROUP.—

(1) REQUIREMENT TO ESTABLISH.—The Director of National Intelligence shall establish an intelligence community interagency working group to prepare the biennial reports required by subsection (b).

(2) CHAIRPERSON.—The Director of National Intelligence shall serve as the chairperson of such interagency working group.

(3) MEMBERSHIP.—Such interagency working group shall be composed of representatives of each element of the intelligence community that the Director of National Intelligence determines appropriate.

(b) BIENNIAL REPORT ON FOREIGN INVESTMENT RISKS.—

(1) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on foreign investment risks prepared by the interagency working group established under subsection (a).

(2) ELEMENTS.—Each report required by paragraph (1) shall include identification, analysis, and explanation of the following:

(A) Any current or projected major threats to the national security of the United States with respect to foreign investment.

(B) Any strategy used by a foreign country that such interagency working group has identified to be a country of special concern to use foreign 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. 718. MODIFICATION OF CERTAIN REPORTING REQUIREMENT ON TRAVEL OF FOREIGN DIPLOMATS.

Section 502(d)(2) of the Intelligence Authorization Act for Fiscal Year 2017 (Public Law 115–31) is amended by striking ''the number'' and inserting ''a best estimate''.

SEC. 719. 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 congres-

sional 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. 720. CONGRESSIONAL NOTIFICATION OF DESIGNATION OF COVERED INTELLIGENCE OFFICER AS PERSONA NON GRATA.

(a) COVERED INTELLIGENCE OFFICER DEFINED.—In this section, the term ''covered intelligence officer'' means—

(1) a United States intelligence officer serving in a post in a foreign country; or

(2) a known or suspected foreign intelligence officer serving in a United States post.

(b) REQUIREMENT FOR REPORTS.—Not later than 72 hours after a covered intelligence officer is designated as a persona non grata, the Director of National Intelligence, in consultation with the Secretary of State, shall submit to the congressional intelligence committees, the Committee on Foreign Relations of the Senate, and the Committee on Foreign Affairs of the House of Representatives a notification of that designation. Each such notification shall include—

(1) the date of the designation;

(2) the basis for the designation; and

(3) a justification for the expulsion.

SEC. 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 congressional intelligence committees a written report describing—

(A) with respect to each element of the intelligence community—

(i) the title of the official or officials responsible for determining whether, pursuant to criteria contained in the Vulnerabilities Equities Policy and Process document or any successor document, a vulnerability must be submitted for review under the Vulnerabilities Equities Process; and

(ii) the process used by such element to make such determination; and

(B) the roles or responsibilities of that element during a review of a vulnerability submitted to the Vulnerabilities Equities Process.

(2) CHANGES TO PROCESS OR CRITERIA.—Not later than 30 days after any significant change is made to the process and criteria used by any element of the intelligence community for determining whether to submit a vulnerability for review under the Vulnerabilities Equities Process, such element shall submit to the congressional intelligence committees a report describing such change.

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

(c) ANNUAL REPORTS.—

(1) IN GENERAL.—Not less frequently than once each calendar year, the Director of National Intelligence shall submit to the congressional intelligence committees a classified report containing, with respect to the previous year—

(A) the number of vulnerabilities submitted for review under the Vulnerabilities Equities Process;

(B) the number of vulnerabilities described in subparagraph (A) disclosed to each vendor responsible for correcting the vulnerability, or to the public, pursuant to the Vulnerabilities Equities Process; and

(C) the aggregate number, by category, of the vulnerabilities excluded from review under the Vulnerabilities Equities Process, as described in paragraph 5.4 of the Vulnerabilities Equities Policy and Process document.

(2) UNCLASSIFIED INFORMATION.—Each report submitted under paragraph (1) shall include an unclassified appendix that contains—

(A) the aggregate number of vulnerabilities disclosed to vendors or the public pursuant to the Vulnerabilities Equities Process; and

(B) the aggregate number of vulnerabilities disclosed to vendors or the public pursuant to the Vulnerabilities Equities Process known to have been patched.

(3) NON-DUPLICATION.—The Director of National Intelligence may forgo submission of an an-

nual 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. INSPECTORS GENERAL REPORTS ON CLASSIFICATION.

(a) REPORTS REQUIRED.—Not later than October 1, 2019, each Inspector General listed in subsection (b) shall submit to the congressional intelligence committees a report that includes, with respect to the department or agency of the Inspector General, analyses of the following:

(1) The accuracy of the application of classification and handling markers on a representative sample of finished reports, including such reports that are compartmented.

(2) Compliance with declassification procedures.

(3) The effectiveness of processes for identifying topics of public or historical importance that merit prioritization for a declassification review.

(b) INSPECTORS GENERAL LISTED.—The Inspectors General listed in this subsection are as follows:

(1) The Inspector General of the Intelligence Community.

(2) The Inspector General of the Central Intelligence Agency.

(3) The Inspector General of the National Security Agency.

(4) The Inspector General of the Defense Intelligence Agency.

(5) The Inspector General of the National Reconnaissance Office.

(6) The Inspector General of the National Geospatial-Intelligence Agency.

SEC. 723. REPORTS ON GLOBAL WATER INSECURITY AND NATIONAL SECURITY IMPLICATIONS AND BRIEFING ON EMERGING INFECTIOUS DISEASE AND PANDEMICS.

(a) REPORTS ON GLOBAL WATER INSECURITY AND NATIONAL SECURITY IMPLICATIONS.—

(1) REPORTS REQUIRED.—Not later than 180 days after the date of the enactment of this Act and not less frequently than once every 5 years thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a

report on the implications of water insecurity on the national security interest of the United States, including consideration of social, economic, agricultural, and environmental factors.

(2) ASSESSMENT SCOPE AND FOCUS.—Each report submitted under paragraph (1) shall include an assessment of water insecurity described in such subsection with a global scope, but focus on areas of the world—

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

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

(ii) where challenges relating to water insecurity are likely to emerge and become significant during the 5-year or the 20-year period beginning on the date of the report; and

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

(3) CONSULTATION.—In researching a report required by paragraph (1), the Director shall consult with—

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

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

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

(b) BRIEFING ON EMERGING INFECTIOUS DISEASE AND PANDEMICS.—

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

(A) the congressional intelligence committees;

(B) the Committee on Foreign Affairs, the Committee on Armed Services, and the Committee on Appropriations of the House of Representatives; and

(C) the Committee on Foreign Relations, the Committee on Armed Services, and the Committee on Appropriations of the Senate.

(2) BRIEFING.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall provide to the appropriate congressional committees a briefing on the anticipated geopolitical effects of emerging infectious disease (including deliberate, accidental, and naturally occurring infectious disease threats) and pandemics, and their implications on the national security of the United States.

(3) CONTENT.—The briefing under paragraph (2) shall include an assessment of—

(A) the economic, social, political, and security risks, costs, and impacts of emerging infectious diseases on the United States and the international political and economic system;

(B) the economic, social, political, and security risks, costs, and impacts of a major transnational pandemic on the United States and the international political and economic system; and

(C) contributing trends and factors to the matters assessed under subparagraphs (A) and (B).

(4) EXAMINATION OF RESPONSE CAPACITY.—In examining the risks, costs, and impacts of emerging infectious disease and a possible transnational pandemic under paragraph (3), the Director of National Intelligence shall also examine in the briefing under paragraph (2) the response capacity within affected countries and the international system. In considering response capacity, the Director shall include—

(A) the ability of affected nations to effectively detect and manage emerging infectious diseases and a possible transnational pandemic;

(B) the role and capacity of international organizations and nongovernmental organizations to respond to emerging infectious disease and a possible pandemic, and their ability to coordinate with affected and donor nations; and

(C) the effectiveness of current international frameworks, agreements, and health systems to respond to emerging infectious diseases and a possible transnational pandemic.

(5) FORM.—The briefing under paragraph (2) may be classified.

SEC. 724. 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. 725. 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. 726. MODIFICATION OF REQUIREMENT FOR ANNUAL REPORT ON HIRING AND RETENTION OF MINORITY EMPLOYEES.

(a) EXPANSION OF PERIOD OF REPORT.—Subsection (a) of section 114 of the National Security Act of 1947

(50 U.S.C. 3050) is amended by inserting ''and the preceding 5 fiscal years'' after ''fiscal year''.

(b) CLARIFICATION ON DISAGGREGATION OF DATA.—Subsection (b) of such section is amended, in the matter before paragraph (1), by striking ''disaggregated data by category of covered person from each element of the intelligence community'' and inserting ''data, disaggregated by category of covered person and by element of the intelligence community,''.

SEC. 727. REPORTS ON INTELLIGENCE COMMUNITY LOAN REPAYMENT AND RELATED PROGRAMS.

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

(1) there should be established, through the issuing of an Intelligence Community Directive or otherwise, an intelligence community-wide program for student loan repayment, student loan forgiveness, financial counseling, and related matters, for employees of the intelligence community;

(2) creating such a program would enhance the ability of the elements of the intelligence community to recruit, hire, and retain highly qualified personnel, including with respect to mission-critical and hard-to-fill positions;

(3) such a program, including with respect to eligibility requirements, should be designed so as to maximize the ability of the elements of the intelligence community to recruit, hire, and retain highly qualified personnel, including with respect to mission-critical and hard-to-fill positions; and

(4) to the extent possible, such a program should be uniform throughout the intelligence community and publicly promoted by each element of the intelligence community to both current employees of the element as well as to prospective employees of the element.

(b) REPORT ON POTENTIAL INTELLIGENCE COMMUNITY-WIDE PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in cooperation with the heads of the elements of the intelligence community and the heads of any other appropriate department or agency of the Federal Government, shall submit to the congressional intelligence committees a report on potentially establishing and carrying out an intelligence community-wide program for student loan repayment, student loan forgiveness, financial

counseling, and related matters, as described in subsection (a).

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

(A) A description of the financial resources that the elements of the intelligence community would require to establish and initially carry out the program specified in paragraph (1).

(B) A description of the practical steps to establish and carry out such a program.

(C) The identification of any legislative action the Director determines necessary to establish and carry out such a program.

(c) ANNUAL REPORTS ON ESTABLISHED PROGRAMS.—

(1) COVERED PROGRAMS DEFINED.—In this subsection, the term ''covered programs'' means any loan repayment program, loan forgiveness program, financial counseling program, or similar program, established pursuant to title X of the National Security Act of 1947 (50 U.S.C. 3191 et seq.) or any other provision of law that may be administered or used by an element of the intelligence community.

(2) ANNUAL REPORTS REQUIRED.—Not less frequently than once each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the covered programs. Each such report shall include, with respect to the period covered by the report, the following:

(A) The number of personnel from each element of the intelligence community who used each covered program.

(B) The total amount of funds each element expended for each such program.

(C) A description of the efforts made by each element to promote each covered program pursuant to both the personnel of the element of the intelligence community and to prospective personnel.

SEC. 728. REPEAL OF CERTAIN REPORTING REQUIREMENTS.

(a) CORRECTING LONG-STANDING MATERIAL WEAKNESSES.—Section 368 of the Intelligence Authorization Act for Fiscal Year 2010 (Public Law 110–259; 50 U.S.C. 3051 note) is hereby repealed.

(b) INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP.—Section 210D of the Homeland Security Act of 2002 (6 U.S.C. 124k) is amended—

(1) by striking subsection (c);

(2) by redesignating subsections (d) through (i) as subsections (c) through (h), respectively; and

(3) in subsection (c), as so redesignated—

(A) in paragraph (8), by striking ''; and'' and inserting a period; and

(B) by striking paragraph (9).

(c) INSPECTOR GENERAL REPORT.—Section 8H of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

(1) by striking subsection (g); and

(2) by redesignating subsections (h) and (i) as subsections (g) and (h), respectively.

SEC. 729. INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY REPORT ON SENIOR EXECUTIVES OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.

(a) SENIOR EXECUTIVE SERVICE POSITION DEFINED.—In this section, the term ''Senior Executive Service position'' has the meaning given that term in section 3132(a)(2) of title 5, United States Code, and includes any position above the GS–15, step 10, level of the General Schedule under section 5332 of such title.

(b) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Inspector General of the

Intelligence Community shall submit to the congressional intelligence committees a report on the number of Senior Executive Service positions in the Office of the Director of National Intelligence.

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

(1) The number of required Senior Executive Service positions for the Office of the Director of National Intelligence.

(2) Whether such requirements are reasonably based on the mission of the Office.

(3) A discussion of how the number of the Senior Executive Service positions in the Office compare to the number of senior positions at comparable organizations.

(d) COOPERATION.—The Director of National Intelligence shall provide to the Inspector General of the Intelligence Community any information requested by the Inspector General of the Intelligence Community that is necessary to carry out this section by not later than 14 calendar days after the date on which the Inspector General of the Intelligence Community makes such request.

SEC. 730. BRIEFING ON FEDERAL BUREAU OF INVESTIGATION OFFERING PERMANENT RESIDENCE TO SOURCES AND COOPERATORS.

Not later than 30 days after the date of the enactment of this Act, the Director of the Federal Bureau of Investigation shall provide to the congressional intelligence committees a briefing on the ability of the Federal Bureau of Investigation to offer, as an inducement to assisting the Bureau, permanent residence within the United States to foreign individuals who are sources or cooperators in counterintelligence or other national security-related investigations. The briefing shall address the following:

(1) The extent to which the Bureau may make such offers, whether independently or in conjunction with other agencies and departments of the United States Government, including a discussion of the authorities provided by section 101(a)(15)(S) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)(S)), section 7 of the Central Intelligence Agency Act (50 U.S.C. 3508), and any other provision of law under which the Bureau may make such offers.

(2) An overview of the policies and operational practices of the Bureau with respect to making such offers.

(3) The sufficiency of such policies and practices with respect to inducing individuals to cooperate with, serve as sources for such investigations, or both.

(4) Whether the Director recommends any legislative actions to improve such policies and practices, particularly with respect to the counterintelligence efforts of the Bureau.

SEC. 731. INTELLIGENCE ASSESSMENT OF NORTH KOREA REVENUE SOURCES.

(a) ASSESSMENT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Assistant Secretary of State for Intelligence and Research and the Assistant Secretary of the Treasury for Intelligence and Analysis, shall produce an intelligence assessment of the revenue sources of the North Korean regime. Such assessment shall include revenue from the following sources:

(1) Trade in coal, iron, and iron ore.

(2) The provision of fishing rights to North Korean territorial waters.

(3) Trade in gold, titanium ore, vanadium ore, copper, silver, nickel, zinc, or rare earth minerals, and other stores of value.

(4) Trade in textiles.

(5) Sales of conventional defense articles and services.

(6) Sales of controlled goods, ballistic missiles, and other associated items.

(7) Other types of manufacturing for export, as the Director of National Intelligence considers appropriate.

(8) The exportation of workers from North Korea in a manner intended to generate significant revenue, directly or indirectly, for use by the government of North Korea.

(9) The provision of nonhumanitarian goods (such as food, medicine, and medical devices) and services by other countries.

(10) The provision of services, including banking and other support, including by entities located in the Russian Federation, China, and Iran.

(11) Online commercial activities of the Government of North Korea, including online gambling.

(12) Criminal activities, including cyber-enabled crime and counterfeit goods.

(b) ELEMENTS.—The assessment required under subsection (a) shall include an identification of each of the following:

(1) The sources of North Korea's funding.

(2) Financial and non-financial networks, including supply chain management, transportation, and facilitation, through which North Korea accesses the United States and international financial systems and repatriates and exports capital, goods, and services.

(3) The global financial institutions, money services business, and payment systems that assist North Korea with financial transactions.

(c) SUBMITTAL TO CONGRESS.—Upon completion of the assessment required under subsection (a), the Director of National Intelligence shall submit to the congressional intelligence committees a copy of such assessment.

SEC. 732. REPORT ON POSSIBLE EXPLOITATION OF VIRTUAL CURRENCIES BY TERRORIST ACTORS.

(a) SHORT TITLE.—This section may be cited as the ''Stop Terrorist Use of Virtual Currencies Act''.

(b) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Secretary of the Treasury, shall submit to Congress a report on the possible exploitation of virtual currencies by terrorist actors. Such report shall include the following elements:

(1) An assessment of the means and methods by which international terrorist organizations and State sponsors of terrorism use virtual currencies.

(2) An assessment of the use by terrorist organizations and State sponsors of terrorism of virtual currencies compared to the use by such organizations and States of other forms of financing to support operations, including an assessment of the collection posture of the intelligence community on the use of virtual currencies by such organizations and States.

(3) A description of any existing legal impediments that inhibit or prevent the intelligence community from collecting information on or helping prevent the use of virtual currencies by international terrorist organizations and State sponsors of terrorism and an identification of any gaps in existing law that could be exploited for illicit funding by such organizations and States.

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

SEC. 733. INCLUSION OF DISCIPLINARY ACTIONS IN ANNUAL REPORT RELATING TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 707(b)(1)(G)(ii) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881f(b)(1)(G)(ii)) is amended by inserting before the semicolon the following: ", including whether disciplinary actions were taken as a result of such an incident of noncompliance and the extent of such disciplinary actions".

Subtitle C—Other Matters

SEC. 741. PUBLIC INTEREST DECLASSIFICATION BOARD.

Section 710(b) of the Public Interest Declassification Act of 2000 (Public Law 106–567; 50 U.S.C. 3161 note) is amended by striking "December 31, 2018" and inserting "December 31, 2028".

SEC. 742. 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.—Except as otherwise specifically provided, 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 (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(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. 743. 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 Armed Services and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Armed Services and the Committee on Homeland Security 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 that 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 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. 744. 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 full-time 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) PILOT PROGRAM ON ADMISSION OF PRIVATE SECTOR CIVILIANS TO RECEIVE INSTRUCTION.—

(1) PILOT PROGRAM REQUIRED.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall commence

carrying out a pilot program to assess the feasability and advisability of permitting eligible private sector employees who work in organizations relevant to national security to receive instruction at the National Intelligence University.

(B) DURATION.—The Secretary shall carry out the pilot program during the 3-year period beginning on the date of the commencement of the pilot program.

(C) EXISTING PROGRAM.—The Secretary shall carry out the pilot program in a manner that is consistent with section 2167 of title 10, United States Code.

(D) NUMBER OF PARTICIPANTS.—No more than the equivalent of 35 full-time student positions may be filled at any one time by private sector employees enrolled under the pilot program.

(E) DIPLOMAS AND DEGREES.—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 title 10, United States Code.

(2) ELIGIBLE PRIVATE SECTOR EMPLOYEES.—

(A) IN GENERAL.—For purposes of this subsection, 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.

(B) LIMITATION.—Under this subsection, 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.

(3) ANNUAL CERTIFICATION BY SECRETARY OF DEFENSE.—Under the pilot program, 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.

(4) PILOT PROGRAM REQUIREMENTS.—The Secretary of Defense shall ensure that—

(A) the curriculum in which private sector employees may be enrolled under the pilot program is not readily available through other schools and concentrates on national security-relevant issues; and

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

(5) TUITION.—The President of the National Intelligence University shall charge students enrolled under the pilot program a rate that—

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

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

(6) STANDARDS OF CONDUCT.—While receiving instruction at the National Intelligence University, students enrolled under the pilot program, 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.

(7) USE OF FUNDS.—

(A) IN GENERAL.—Amounts received by the National Intelligence University for instruction of students enrolled under the pilot program shall be retained by the university to defray the costs of such instruction.

(B) RECORDS.—The source, and the disposition, of such funds shall be specifically identified in records of the university.

(8) REPORTS.—

(A) ANNUAL REPORTS.—Each academic year in which the pilot program is carried out, the Secretary 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 report on the number of eligible

private sector employees participating in the pilot program.

(B) FINAL REPORT.—Not later than 90 days after the date of the conclusion of the pilot program, the Secretary 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 report on the findings of the Secretary with respect to the pilot program. Such report shall include—

(i) the findings of the Secretary with respect to the feasability and advisability of permitting eligible private sector employees who work in organizations relevant to national security to receive instruction at the National Intelligence University; and

(ii) a recommendation as to whether the pilot program should be extended.

SEC. 745. TECHNICAL AND CLERICAL AMENDMENTS TO THE NATIONAL SECURITY ACT OF 1947.

(a) TABLE OF CONTENTS.—The table of contents at the beginning of the National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended—

(1) by inserting after the item relating to section 2 the following new item:

"Sec. 3. Definitions.";

(2) by striking the item relating to section 107;

(3) by striking the item relating to section 113B and inserting the following new item:

"Sec. 113B. Special pay authority for science, technology, engineering, or mathematics positions.";

(4) by striking the items relating to sections 202, 203, 204, 208, 209, 210, 211, 212, 213, and 214; and

(5) by inserting after the item relating to section 311 the following new item:

"Sec. 312. Repealing and saving provisions.".

(b) OTHER TECHNICAL CORRECTIONS.—Such Act is further amended—

(1) in section 102A—

(A) in subparagraph (G) of paragraph (1) of subsection (g), by moving the margins of such subparagraph 2 ems to the left; and

(B) in paragraph (3) of subsection (v), by moving the margins of such paragraph 2 ems to the left;

(2) in section 106—

(A) by inserting "**SEC. 106.**" before "(a)"; and

(B) in subparagraph (I) of paragraph (2) of subsection (b), by moving the margins of such subparagraph 2 ems to the left;

(3) by striking section 107;

(4) in section 108(c), by striking ''in both a classified and an unclassified form'' and inserting ''to Congress in classified form, but may include an unclassified summary'';

(5) in section 112(c)(1), by striking ''section 103(c)(7)'' and inserting ''section 102A(i)'';

(6) by amending section 201 to read as follows:

''SEC. 201. DEPARTMENT OF DEFENSE.

''Except to the extent inconsistent with the provisions of this Act or other provisions of law, the provisions of title 5, United States Code, shall be applicable to the Department of Defense.'';

(7) in section 205, by redesignating subsections (b) and (c) as subsections (a) and (b), respectively;

(8) in section 206, by striking ''(a)'';

(9) in section 207, by striking ''(c)'';

(10) in section 308(a), by striking ''this Act'' and inserting ''sections 2, 101, 102, 103, and 303 of this Act'';

(11) by redesignating section 411 as section 312;

(12) in section 503—

(A) in paragraph (5) of subsection (c)—

(i) by moving the margins of such paragraph 2 ems to the left; and

(ii) by moving the margins of subparagraph (B) of such paragraph 2 ems to the left; and

(B) in paragraph (2) of subsection (d), by moving the margins of such paragraph 2 ems to the left; and

(13) in subparagraph (B) of paragraph (3) of subsection (a) of section 504, by moving the margins of such subparagraph 2 ems to the right.

SEC. 746. 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. 747. SENSE OF CONGRESS ON NOTIFICATION OF CERTAIN DISCLOSURES OF CLASSIFIED INFORMATION.

(a) DEFINITIONS.—In this section:

(1) ADVERSARY FOREIGN GOVERNMENT.—The term ''adversary foreign government'' means the government of any of the following foreign countries:

(A) North Korea.

(B) Iran.

(C) China.

(D) Russia.

(E) Cuba.

(2) COVERED CLASSIFIED INFORMATION.—The term ''covered classified information'' means classified information that was—

(A) collected by an element of the intelligence community; or

(B) provided by the intelligence service or military of a foreign country to an element of the intelligence community.

(3) ESTABLISHED INTELLIGENCE CHANNELS.—The term ''established intelligence channels'' means

methods to exchange intelligence to coordinate foreign intelligence relationships, as established pursuant to law by the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the National Security Agency, or other head of an element of the intelligence community.

(4) INDIVIDUAL IN THE EXECUTIVE BRANCH.—The term ''individual in the executive branch'' means any officer or employee of the executive branch, including individuals—

(A) occupying a position specified in article II of the Constitution;

(B) appointed to a position by an individual described in subparagraph (A); or

(C) serving in the civil service or the Senior Executive Service (or similar service for senior executives of particular departments or agencies).

(b) FINDINGS.—Congress finds that section 502 of the National Security Act of 1947 (50 U.S.C. 3092) requires elements of the intelligence community to keep the congressional intelligence committees ''fully and currently informed'' about all ''intelligence activities'' of the United States, and to ''furnish to the congressional intelligence committees any information or material concerning intel-

ligence activities * * * which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.''.

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

(1) section 502 of the National Security Act of 1947 (50 U.S.C. 3092), together with other intelligence community authorities, obligates an element of the intelligence community to submit to the congressional intelligence committees written notification, by not later than 7 days after becoming aware, that an individual in the executive branch has disclosed covered classified information to an official of an adversary foreign government using methods other than established intelligence channels; and

(2) each such notification should include—

(A) the date and place of the disclosure of classified information covered by the notification;

(B) a description of such classified information;

(C) identification of the individual who made such disclosure and the individual to whom such disclosure was made; and

(D) a summary of the circumstances of such disclosure.

SEC. 748. 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. 749. 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.

○