Calendar No. 207

115TH CONGRESS
1ST SESSION

S. 1761

To authorize appropriations for fiscal year 2018 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 18, 2017

Mr. BURR, from the Select Committee on Intelligence of the Senate, reported, under authority of the order of the Senate of August 3, 2017, the following original bill; which was read twice and placed on the calendar

---

A BILL

To authorize appropriations for fiscal year 2018 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Intelligence Authorization Act for Fiscal Year 2018''.

(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'' means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

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

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2018 for the conduct of the intelligence and intelligence-related activities of the following elements of the United States Government:

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

(2) The Central Intelligence Agency.

(3) The Department of Defense.

(4) The Defense Intelligence Agency.

(5) The National Security Agency.

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

(7) The Coast Guard.

(8) The Department of State.

(9) The Department of the Treasury.

(10) The Department of Energy.

(11) The Department of Justice.

(12) The Federal Bureau of Investigation.

(13) The Drug Enforcement Administration.

(14) The National Reconnaissance Office.

(15) The National Geospatial-Intelligence Agency.

(16) The Department of Homeland Security.

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) SPECIFICATIONS OF AMOUNTS.—The amounts authorized to be appropriated under section 101 and, subject to section 103, the authorized personnel ceilings as of September 30, 2018, for the conduct of the intelligence activities of the elements listed in paragraphs (1) through (16) of section 101, are those specified in the classified Schedule of Authorizations 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 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. PERSONNEL CEILING ADJUSTMENTS.

(a) AUTHORITY FOR INCREASES.—The Director of National Intelligence may authorize employment of civilian personnel in excess of the number authorized for fiscal

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

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

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

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

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

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

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

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

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

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

SEC. 104. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2018 the sum of $550,200,000. Within such amount, funds identified in the classified Schedule of Authorizations referred to in section 102(a) for advanced research and development shall remain available until September 30, 2019.

(b) AUTHORIZED PERSONNEL LEVELS.—The elements within the Intelligence Community Management

Account of the Director of National Intelligence are authorized 797 positions as of September 30, 2018. Personnel serving in such elements may be permanent employees of the Office of the Director of National Intelligence or personnel detailed from other elements of the United States Government.

(c) CLASSIFIED AUTHORIZATIONS.—

(1) AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2018 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a). Such additional amounts made available for advanced research and development shall remain available until September 30, 2019.

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

specified in the classified Schedule of Authorizations referred to in section 102(a).

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund for fiscal year 2018 the sum of $514,000,000.

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.

(a) IN GENERAL.—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 (STEM)—

''(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 striking subsection (f);

(3) by redesignating subsections (b) through (e) as subsections (c) through (f), respectively;

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

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

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

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

is for positions that perform functions that execute the cyber mission of the Agency; or

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

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

''(A) any allowance, differential, bonus, award, or other similar cash payment in addition to basic pay that is authorized under title 10, United States Code, (or any other applicable law in addition to title 5 of such Code, excluding the Fair Labor Standards Act) 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).''; and

(5) in subsection (c), as redesignated by paragraph (3), by striking ''A minimum'' and inserting ''Except as provided in subsection (b), a minimum''.

(b) SPECIAL RATES FOR CYBER EMPLOYEES UNDER TITLE 5.—Section 5305 of title 5, United States Code, is amended—

(1) in subsection (g)(1), by striking ''subsection (h)'' and inserting ''subsections (h) and (k)''; and

(2) by adding at the end the following subsections:

''(k)(1) Notwithstanding the rate limitations set forth in subsections (a)(1) and (g)(2), the Office of Personnel Management may establish under this section a rate of pay that does not exceed the rate of basic pay payable for level II of the Executive Schedule under section 5313 for employees in positions that perform functions that execute a cyber mission and who are certified to have specified skills and competencies.

''(2) Payments under subsection (g)(1) may not be made to an employee receiving a rate of pay established under this section and described in paragraph (1) of this subsection if, or to the extent that, when added to basic pay otherwise payable, such payments would cause the total to exceed the rate of basic pay payable for level II of the Executive Schedule under section 5313.

''(l) An employee who is subject to a reduction or termination of a special rate of pay established under this section due to not maintaining a required skill or competency certification, or due to not obtaining a revised skill or competency certification, shall not be entitled to pay retention under section 5363 based on any resulting reduction in pay.''.

SEC. 304. DIRECTOR OF NATIONAL INTELLIGENCE REVIEW OF PLACEMENT OF POSITIONS WITHIN THE INTELLIGENCE COMMUNITY ON THE EXECUTIVE SCHEDULE.

The Director of National Intelligence 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 shall determine—

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

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

SEC. 305. 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. 306. SUPPLY CHAIN AND COUNTERINTELLIGENCE RISK MANAGEMENT TASK FORCE.

(a) REQUIREMENT TO ESTABLISH.—The Director of National Intelligence shall establish a Supply Chain and Counterintelligence Risk Management Task Force to

standardize information sharing between the intelligence community and the acquisition community of the Government of the United States with respect to the supply chain and counterintelligence risks.

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

(1) a representative of the Defense Security Service;

(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; and

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

(c) SECURITY CLEARANCES.—Each member of the Supply Chain and Counterintelligence Risk Management Task Force shall have a security clearance at the Top Secret and Sensitive Compartmented Information level.

(d) ANNUAL REPORT.—The Supply Chain and Counterintelligence Risk Management Task Force shall submit to the congressional intelligence 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 Government of the United States by the intelligence community.

SEC. 307. INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY AUDITING AUTHORITY.

Section 103H(j)(2)(A) of the National Security Act of 1947 (50 U.S.C. 3033(j)(2)(A)) is amended—

(1) by striking ''law and the policies of the Director of National Intelligence,'' and inserting ''law,''; and

(2) by striking ''General.'' and inserting ''General and is authorized to obtain the temporary or intermittent services of experts or consultants or an organization thereof.''.

SEC. 308. INSPECTORS GENERAL STUDIES ON CLASSIFICATION.

(a) REQUIREMENT FOR STUDY.—Not later than October 1, 2019, each Inspector General listed in subsection (b) shall carry out and submit to the congressional intelligence committees a report on the following:

(1) A study of the application of classification and handling markers on a representative sample of finished reports, including compartments.

(2) A study analyzing compliance with declassification procedures.

(3) A study on reviewing processes for identifying topics of public or historical importance that merit prioritization for a declassification review.

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

(1) The Inspector General of the Intelligence Community.

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

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

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

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

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

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

SEC. 401. AUTHORITY FOR THE 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. INFORMATION SHARING WITH STATE ELECTION OFFICIALS.

(a) SECURITY CLEARANCES.—

(1) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall sponsor a security clearance up to the top secret level for each eligible chief election official of a State or the District of Co-

lumbia, and up to one eligible designee of such an election official, at the time that he or she assumes such position.

(2) DETERMINATION OF LEVELS.—

(A) IN GENERAL.—The Director shall determine the level of clearances for the positions described in paragraph (1).

(B) INTERIM CLEARANCES.—The Director 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 one designee of such official under such paragraph.

(b) INFORMATION SHARING.—

(1) IN GENERAL.—The Director shall share appropriate classified information related to threats to election systems and to the integrity of the election process with chief election officials and such designees who have received a security clearance under subsection (a).

(2) REPORTS.—The Director shall transmit reports on such information sharing to the respective affected Secretary of State or States.

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

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

SEC. 403. TECHNICAL MODIFICATION TO THE EXECUTIVE SCHEDULE.

Section 5313 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. MODIFICATION TO THE 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) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(f)) 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 Intelligence Authorization Act for Fiscal Year 2018, each individual designated as the program manager shall be appointed by the Director of National Intelligence.".

Subtitle B—Central Intelligence Agency

SEC. 411. REPEAL OF FOREIGN LANGUAGE PROFICIENCY REQUIREMENT FOR CERTAIN SENIOR LEVEL POSITIONS IN THE CENTRAL INTELLIGENCE AGENCY.

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

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

Subtitle C—Other Elements

SEC. 421. DESIGNATION OF THE COUNTERINTELLIGENCE DIRECTORATE OF THE DEFENSE SECURITY SERVICE AS AN ELEMENT OF THE INTELLIGENCE COMMUNITY.

(a) DESIGNATION.—Paragraph (4) of section 3 of the National Security Act of 1947 (50 U.S.C. 3003(4)) is amended—

(1) by redesignating subparagraphs (H) through (L) as subparagraphs (I) through (M), respectively; and

(2) by inserting after subparagraph (G) the following:

''(H) The Counterintelligence Directorate of the Defense Security Service of the Department of Defense.''.

(b) APPLICATION OF LAWS, REGULATIONS, RULES, AND POLICIES.—Beginning on the date of the enactment of this Act, any law, regulation, rule, or policy that applies to the elements of the intelligence community, as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3303), shall apply to the Counterintelligence Directorate of the Defense Security Service of the Department of Defense.

TITLE V—SECURING ENERGY INFRASTRUCTURE

SEC. 501. SHORT TITLE.

This title may be cited as the ''Securing Energy Infrastructure Act of 2017''.

SEC. 502. DEFINITIONS.

In this title:

(1) 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.

(2) DIRECTOR.—Except as otherwise specifically provided, the term ''Director'' means the Director of Intelligence and Counterintelligence of the Department of Energy.

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

(4) INDUSTRIAL CONTROL SYSTEM.—

(A) IN GENERAL.—The term ''industrial control system'' means an operational tech-

nology used to measure, control, or manage industrial functions.

(B) INCLUSIONS.—The term ''industrial control system'' 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 section 503.

(7) 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.

SEC. 503. PILOT PROGRAM FOR SECURING ENERGY INFRASTRUCTURE.

Not later than 180 days after the date of enactment of this title, the Director 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 manufac-

turers in the supply chain) that voluntarily participate in the Program to identify new classes of security vulnerabilities of the covered entities; and

(2) researching, developing, testing, and implementing technology platforms 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.

SEC. 504. WORKING GROUP TO EVALUATE PROGRAM STANDARDS AND DEVELOP STRATEGY.

(a) ESTABLISHMENT.—The Director shall establish a working group—

(1) to evaluate the technology platforms and standards used in the Program under section 503(2); and

(2) 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.

(b) MEMBERSHIP.—The working group established under subsection (a) shall be composed of not fewer than

10 members, to be appointed by the Director, at least 1 member of which shall represent each of the following:

(1) The Department of Energy.

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

(3)(A) The Department of Homeland Security; or

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

(4) The North American Electric Reliability Corporation.

(5) The Nuclear Regulatory Commission.

(6)(A) The Office of the Director of National Intelligence; or

(B) the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).

(7)(A) The Department of Defense; or

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

(8) A State or regional energy agency.

(9) A national research body or academic institution.

(10) The National Laboratories.

SEC. 505. REPORTS ON THE PROGRAM.

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

(1) describes the results of the Program;

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

(3) describes the results of the evaluations conducted by the working group established under section 504(a).

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

(1) describes the results of the Program;

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

(3) describes the results of the evaluations conducted by the working group established under section 504(a).

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

(1) the congressional intelligence committees;

(2) the Committee on Energy and Natural Resources of the Senate; and

(3) the Committee on Energy and Commerce of the House of Representatives.

SEC. 506. NO NEW REGULATORY AUTHORITY FOR FEDERAL AGENCIES.

Nothing in this title authorizes the Director or the head of any other Federal agency to issue new regulations.

SEC. 507. EXEMPTION FROM DISCLOSURE.

Information shared by or with the Federal Government or a State, tribal, or local government under this title shall be—

(1) deemed to be voluntarily shared information; and

(2) exempt from disclosure under any provision of Federal, 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.

SEC. 508. PROTECTION FROM LIABILITY.

(a) IN GENERAL.—A cause of action against a covered entity for engaging in the voluntary activities authorized under section 503—

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

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

(b) VOLUNTARY ACTIVITIES.—Nothing in this title subjects any covered entity to liability for not engaging in the voluntary activities authorized under section 503.

SEC. 509. AUTHORIZATION OF APPROPRIATIONS.

(a) PILOT PROGRAM.—There is authorized to be appropriated $10,000,000 to carry out section 503.

(b) WORKING GROUP AND REPORT.—There is authorized to be appropriated $1,500,000 to carry out sections 504 and 505.

(c) AVAILABILITY.—Amounts made available under subsections (a) and (b) shall remain available until expended.

TITLE VI—REPORTS AND OTHER MATTERS

SEC. 601. 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. 602. GOVERNANCE FOR SECURITY CLEARANCE, SUITABILITY AND FITNESS FOR EMPLOYMENT, AND CREDENTIALING.

(a) GOVERNANCE COUNCIL FOR SUITABILITY, CREDENTIALING, AND SECURITY.—

(1) ESTABLISHMENT.—There is an interagency Security, Suitability, and Credentialing Council (in this section the ''Council''). The Council shall be accountable to the President and to Congress to achieve the goals of the executive branch vetting enterprise.

(2) MEMBERSHIP.—

(A) COMPOSITION.—The Council shall be composed for the following:

(i) One individual who shall be appointed by the Director of the Office of Management and Budget.

(ii) The individual serving as the Suitability Executive Agent and the Credentialing Executive Agent pursuant to subsections (b) and (c), respectively.

(iii) The individual serving as the Security Executive Agent pursuant to subsection (d)(1).

(iv) The Under Secretary of Defense for Intelligence.

(v) The Director of the National Background Investigations Bureau.

(B) CHAIRPERSON.—The Chairperson of the Council shall be the individual appointed under subparagraph (A)(i). The Chairperson shall have authority, direction, and control over the functions of the Council.

(3) FUNCTIONS.—The functions of the Council are as follows:

(A) Ensuring enterprise-wide alignment of suitability, security, credentialing, and as appropriate, fitness processes.

(B) Holding agencies accountable for the implementation of suitability, security, fitness, and credentialing processes and procedures.

(C) Defining requirements for enterprise-wide reciprocity management information technology, and develop standards for enterprise-wide information technology.

(D) Working with agencies—

(i) to implement continuous performance improvement programs, policies, and procedures;

(ii) to establish annual goals and progress metrics; and

(iii) to prepare annual reports on results.

(E) Ensuring and overseeing the development of tools and techniques for enhancing background investigations and adjudications.

(F) Enabling discussion and consensus resolution of differences in processes, policies, and procedures among the members of the Council, and other agencies as appropriate.

(G) Sharing best practices.

(H) Advise the Suitability Executive Agent, the Credentialing Executive Agent, and the Security Executive Agent on policies affecting the alignment of investigations and adjudications.

(I) Working with agencies to develop agency policies and procedures to enable sharing of vetting information consistent with the law and the protection of privacy and civil liberties and

to the extent necessary for enterprise-wide efficiency, effectiveness, and security.

(J) Monitoring performance to identify and drive enterprise-level process enhancements, and make recommendations for changes to executive branch-wide guidance and authorities to resolve overlaps or close policy gaps where they may exist.

(K) Promoting data-driven, transparent, and expeditious policy-making processes.

(L) Developing and continuously reevaluating and revising outcome-based metrics that measure the quality, efficiency and effectiveness of the vetting enterprise.

(4) SUBORDINATE BODIES.—The Chairperson may establish subordinate entities, mechanisms, and policies to support and assist the Council in carrying out the functions of the Council.

(b) SUITABILITY EXECUTIVE AGENT.—

(1) IN GENERAL.—The Director of the Office of Personnel Management shall serve as the Suitability Executive Agent.

(2) DUTIES.—The duties of the Suitability Executive Agent are as follows:

(A) Pursuant to sections 1103 and 1104 of title 5, United States Code, and the Civil Service Rules, to be responsible for suitability and fitness by—

(i) prescribing suitability standards and minimum standards of fitness for employment;

(ii) prescribing position designation requirements with regard to the risk to the efficiency and integrity of the service;

(iii) prescribing applicable investigative standards, policies, and procedures for suitability and fitness;

(iv) prescribing suitability and fitness reciprocity standards;

(v) making suitability determinations; and

(vi) taking suitability actions.

(B) To issue regulations, guidance, and standards to fulfill the Director's responsibilities related to suitability and fitness under Executive Order 13488 of January 16, 2009, as amended.

(C) To promote reciprocal recognition of suitability or fitness determinations among the

agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and adjudications of suitability and fitness.

(D) To continue to initially approve, and periodically review for renewal, agencies' requests to administer polygraphs in connection with appointment in the competitive service, in consultation with the Security Executive Agent as appropriate.

(E) To make a continuing review of agency programs for suitability and fitness vetting to determine whether they are being implemented according to this section.

(F) Shall, pursuant to section 1104 of title 5, United States Code, prescribe performance standards and a system of oversight for any suitability or fitness function delegated by the Director to the head of another agency, including uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of delegated functions.

(3) GUIDELINES AND INSTRUCTIONS.—The Suitability Executive Agent may issue guidelines and

instructions to the heads of agencies to promote appropriate uniformity, centralization, efficiency, effectiveness, reciprocity, timeliness, and security in processes relating to determining suitability or fitness.

(c) CREDENTIALING EXECUTIVE AGENT.—

(1) IN GENERAL.—In addition to serving as the Suitability Executive Agent, the Director of the Office of Personnel Management shall also serve as the Credentialing Executive Agent.

(2) DUTIES.—The duties of the Credentialing Executive Agent are as follows:

(A) To develop standards for investigations, reinvestigations, and continuous vetting for a covered individual's eligibility for a PIV credential.

(B) To develop adjudicative guidelines for a covered individual's eligibility for a PIV credential.

(C) To develop guidelines on reporting and recording determinations of eligibility for a PIV credential.

(D) To develop standards for unfavorable determinations of eligibility for a PIV credential, including procedures for denying and revoking the eligibility for a PIV credential, for

reconsideration of unfavorable determinations, and for rendering the PIV credential inoperable.

(E) To develop standards and procedures for suspending eligibility for a PIV credential when there is a reasonable basis to believe there may be an unacceptable risk pending an inquiry or investigation, including special standards and procedures for imminent risk.

(F) To develop uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations and adjudications relating to eligibility for a PIV credential.

(G) To monitor and make a continuing review of agency programs for determining eligibility for a PIV credential to determine whether they are being implemented according to this section.

(H) To consult to the extent practicable with other agencies with responsibilities related to PIV credentials to ensure that policies and procedures are consistent with law.

(3) GUIDELINES AND INSTRUCTIONS.—The Credentialing Executive Agent may develop guide-

lines and instructions to the heads of agencies as necessary to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to eligibility for a PIV credential.

(4) PIV CREDENTIAL DEFINED.—In this subsection, the term ''PIV credential'' means a personal identity verification credential permitting logical and physical access to Federally controlled facilities and Federally controlled information systems.

(d) SECURITY EXECUTIVE AGENT.—

(1) IN GENERAL.—The Director of National Intelligence shall serve as the Security Executive Agent.

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

(A) 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 agency.

(B) To make a continuing review of agencies' national security background investigation and adjudication programs to determine whether they are being implemented according to this section.

(C) To develop and issue uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations, polygraphs, and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position.

(D) To serve as the final authority to designate an agency or agencies, to the extent that it is not practicable to use the National Background Investigations Bureau, 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.

(E) To serve as the final authority to designate an agency or agencies to determine eligibility for access to classified information or eligibility to hold a sensitive position in accordance with Executive Order 12968 of August 2, 1995, as amended.

(F) To ensure reciprocal recognition of eligibility for access to classified information or

eligibility to hold a sensitive position among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and adjudications of eligibility.

(3) AUTHORITIES.—The Security Executive Agent may—

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

(B) if consistent with the national security, authorize exceptions to or waivers of national security investigative requirements, and may issue implementing or clarifying guidance as necessary;

(C) assign, in whole or in part, to the head of any agency (solely or jointly) any of the duties of the Security Executive Agent under paragraph (2) or the authorities in subpara-

graphs (A) and (B) of this paragraph, with the agency's exercise of such assigned duties or authorities to be subject to the Security Executive Agent's oversight and with such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate; and

(D) define and set standards for continuous evaluation for continued access to classified information.

(e) PRESERVATION OF AUTHORITY.—Nothing in this section shall be construed to limit the authorities of the Director of the Office of Personnel Management, the Director of National Intelligence, or the Secretary of Defense under any provision of law.

SEC. 603. PROCESS FOR SECURITY CLEARANCES.

(a) REVIEWS.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, acting as the Security Executive Agent in accordance with subsection (d) of section 602, in coordination with the Suitability Executive Agent and the Credentialing Executive Agent who are serving in accordance with subsections (b) and (c) of such section, shall submit to the congressional intelligence committees a report that includes the following:

(1) REVIEW AND ASSESSMENT OF STANDARDS.—

(A) IN GENERAL.—A review of the relationship among the information requested by the Questionnaire for National Security Positions (Standard Form 86), the application of the Federal Investigative Standards prescribed by the Office of Personnel Management and the Office of the Director of National Intelligence, and the application of the adjudicative guidelines under Security Executive Agent Directive 4 (''National Security Adjudicative Guidelines'').

(B) ASSESSMENT.—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.

(2) RECOMMENDATIONS TO IMPROVE BACKGROUND INVESTIGATIONS.—Recommendations to improve the background investigation process, including recommendations—

(A) to simplify the Questionnaire for National Security Positions (Standard Form 86)

and increase customer support to applicants completing such Questionnaire;

(B) to use remote and virtual techniques and centralized locations during field investigation work;

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

(D) to build the capacity of the background investigation labor sector.

(3) REVIEW OF SCHEDULES.—A review of whether the schedule for processing security clearances included in section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341) should be modified.

(4) EVALUATION OF SPLITTING THE BACKGROUND INVESTIGATION FUNCTION.—

(A) IN GENERAL.—An evaluation of the impact on costs, quality, and timeliness of security clearance background investigations associated with transferring to the Secretary of Defense responsibility for conducting background investigations for—

(i) personnel of the Department of Defense; or

(ii) all contractors to and personnel of the United States Government.

(B) ANALYSIS.—An analysis of—

(i) the time required for the Secretary of Defense to gain sufficient institutional capacity and capability to perform the investigations described in clauses (i) and (ii) of subparagraph (A);

(ii) past experience with agencies and departments of the United States having responsibility for conducting background investigations, including the transfer to the Office of Personnel Management of background investigations for personnel of the Department of Defense during 2003, 2004, and 2005; and

(iii) the mobility of the workforce who perform background investigations between government agencies and contractors.

(b) POLICY, STRATEGY, AND IMPLEMENTATION.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, acting as the Security Executive Agent in accordance with section 602(d), shall establish the following:

(1) POLICY AND IMPLEMENTATION PLAN FOR INTERIM SECURITY CLEARANCES.—A policy and implementation plan for the issuance of interim security clearances.

(2) POLICY ON CONSISTENT TREATMENT OF GOVERNMENT AND CONTRACTOR PERSONNEL.—A policy and implementation plan to ensure contractors are treated consistently in the security clearance process across agencies and departments of the United States and as compared to employees of such agencies and departments. Such policy shall address—

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

(B) standardization of how requests for clearance sponsorship are issued;

(C) digitization of background investigation-related forms;

(D) use of the polygraph;

(E) the application of the adjudicative guidelines under Security Executive Agent Directive 4 (''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; and

(H) reporting on security incidents and performance.

(3) STRATEGY AND IMPLEMENTATION FOR PERIODIC REINVESTIGATIONS.—

(A) STRATEGY AND IMPLEMENTATION PLAN.—A strategy and implementation plan to conduct periodic reinvestigations as part of a security clearance determination exclusively on an as-needed, risk-based basis. Such plan shall include actions to assess the extent to which automated records checks and other continuous evaluation methods may be used to expedite or focus reinvestigations.

(B) EXCEPTION.—The Security Executive Agent may provide justification if certain populations are determined to require periodic reinvestigations at regular intervals.

(4) POLICY FOR AUTOMATED RECORDS CHECKS.—A policy and implementation plan for agencies and departments of the United States Government, 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) POLICY AND IMPLEMENTATION FOR SHARING OF BACKGROUND INVESTIGATION DATA.—A policy and implementation plan for sharing information between and among agencies or departments of the United States and private entities that is relevant to decisions about granting or renewing security clearances. Such information shall—

(A) pertain to security and human resources matters; and

(B) be treated in a manner consistent with privacy concerns.

SEC. 604. REPORTS ON THE VULNERABILITIES EQUITIES POLICY AND PROCESS OF THE FEDERAL GOVERNMENT.

(a) REPORT POLICY AND PROCESS.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act and not later than 30 days after any substantive change in policy,

the head of each element of the intelligence community shall submit to the congressional intelligence committees a report detailing the process and criteria the head uses for determining whether to submit a vulnerability for review under the vulnerabilities equities policy and process of the Federal Government.

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

(b) ANNUAL REPORT ON VULNERABILITIES.—

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

(A) how many vulnerabilities the intelligence community has submitted for review during the previous calendar year;

(B) how many of such vulnerabilities were ultimately disclosed to the vendor responsible for correcting the vulnerability during the previous calendar year; and

(C) vulnerabilities disclosed since the previous report that have either—

(i) been patched or mitigated by the responsible vendor; or

(ii) have not been patched or mitigated by the responsible vendor and more than 180 days have elapsed since the vulnerability was disclosed.

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

(A) The date the vulnerability was disclosed to the responsible vendor.

(B) The date the patch or mitigation for the vulnerability was made publicly available by the responsible vendor.

(C) An unclassified appendix that includes—

(i) a top-line summary of the aggregate number of vulnerabilities disclosed to vendors, how many have been patched, and the average time between disclosure of the vulnerability and the patching of the vulnerability; and

(ii) the aggregate number of vulnerabilities disclosed to each responsible vendor, delineated by the amount of time required to patch or mitigate the vulner-

ability, as defined by thirty day increments.

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

(c) VULNERABILITIES EQUITIES POLICY AND PROCESS OF THE FEDERAL GOVERNMENT DEFINED.—In this section, the term ''vulnerabilities equities policy and process of the Federal Government'' means the policy and process established by the National Security Council for the Federal Government, or successor set of policies and processes, establishing policy and responsibilities for disseminating information about vulnerabilities discovered by the Federal Government or its contractors, or disclosed to the Federal Government by the private sector in government off-the-shelf (GOTS), commercial off-the-shelf (COTS), or other commercial information technology or industrial control products or systems (including both hardware and software).

SEC. 605. BUG BOUNTY PROGRAMS.

(a) DEFINITIONS.—In this section:

(1) 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 re-

port vulnerabilities within an information system in exchange for payment.

(2) 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 Under Secretary for Intelligence and Analysis of the Department of Homeland Security shall submit to the congressional intelligence committees a strategic plan to implement bug bounty programs at appropriate agencies and departments of the United States.

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

(A) an assessment of—

(i) the effectiveness of 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. 606. REPORT ON CYBER ATTACKS BY FOREIGN GOVERNMENTS AGAINST UNITED STATES ELECTION INFRASTRUCTURE.

(a) 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 congressional intelligence 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.

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

(c) DEFINITIONS.—In this section:

(1) 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.

(2) 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.

SEC. 607. REVIEW OF INTELLIGENCE COMMUNITY'S POSTURE TO COLLECT AGAINST AND ANALYZE RUSSIAN EFFORTS TO INFLUENCE THE PRESIDENTIAL ELECTION.

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

(1) complete an after action review of the intelligence community's posture 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. 608. ASSESSMENT OF FOREIGN INTELLIGENCE THREATS TO FEDERAL ELECTIONS.

(a) 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 and complete not later than 180 days before such election, an assessment of security vulnerabilities of State election systems; and

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

(A) congressional leadership; and

(B) the congressional intelligence committees.

(b) UPDATE.—Not later than 90 days before any regularly scheduled Federal election, the Director of National Intelligence shall—

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

(2) submit the updated assessment to—

(A) congressional leadership; and

(B) the congressional intelligence committees.

(c) DEFINITIONS.—In this section:

(1) 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.

(2) 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).

SEC. 609. STRATEGY FOR COUNTERING RUSSIAN CYBER THREATS TO UNITED STATES ELECTIONS.

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

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

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

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

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

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

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

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

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

(8) Public education and communication efforts.

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

(c) REPORT TO CONGRESS.—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 brief the congressional intelligence committees on the strategy developed under subsection (a).

SEC. 610. LIMITATION RELATING TO ESTABLISHMENT OR SUPPORT OF CYBER SECURITY UNIT WITH THE GOVERNMENT OF RUSSIA.

(a) LIMITATION.—No amount may be expended by the Federal Government to establish or support a cyber security unit or other cyber agreement that is jointly established or otherwise implemented by the Government of the United States and the Government of Russia unless, at least 30 days prior to the establishment of such agreement, the Director of National Intelligence submits to the congressional intelligence committees a report on such agreement that includes the elements required by subsection (b).

(b) REPORT ELEMENTS.—If the Director submits a report under subsection (a), 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.

SEC. 611. REPORT ON RETURNING RUSSIAN COMPOUNDS.

(a) COVERED COMPOUNDS DEFINED.—In this section, the term ''covered compounds'' means the real property in New York and the real property in Maryland that were under the control of the Government of Russia in 2016 and were removed from such control in response to various transgressions by the Government of Russia, including the interference by the Government of Russia in the 2016 election in the United States.

(b) REQUIREMENT FOR REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the intelligence risks of returning the covered compounds to Russian control.

(c) FORM OF REPORT.—The report required by subsection (b) shall be submitted in classified and unclassified forms.

SEC. 612. INTELLIGENCE COMMUNITY ASSESSMENT ON THREAT OF RUSSIAN MONEY LAUNDERING TO THE UNITED STATES.

(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 Secretary of the Treasury, shall submit to the congressional intelligence committees an intelligence community assessment on the threat of Russian money laundering to the United States. The assessment shall be based on all-source intelligence, including from the intelligence community and from all elements of the Department of the Treasury under the Office of Terrorism and Financial Intelligence.

(b) ELEMENTS.—The assessment required by subsection (a) shall cover the following:

(1) Money laundering in the Russian Federation, global nodes of money laundering used by Russian and associated entities, and the entry points of money laundering by Russian and associated entities into the United States.

(2) Vulnerabilities to money laundering in the United States financial and legal system, including specific sectors, and ways in which Russian money laundering has exploited those vulnerabilities.

(3) Any connections between Russian oligarchs and elements of Russian organized crime involved in money laundering and the Government of Russia.

(4) The counterintelligence threat posed by Russian money laundering as well as the threat to the United States financial system and United States efforts to enforce sanctions and combat organized crime.

SEC. 613. NOTIFICATION OF AN ACTIVE MEASURES CAMPAIGN.

(a) 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 Chairman and Vice Chairman or Ranking Member of each of the congressional intelligence 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.

(b) CONTENT OF NOTIFICATION.—Each notification required by subsection (a) shall include information con-

cerning actions taken by the United States to expose or halt an attempt referred to in subsection (a).

SEC. 614. 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), 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 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. 615. 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. 616. SEMIANNUAL REPORT ON REFERRALS TO DEPARTMENT OF JUSTICE BY ELEMENTS OF THE INTELLIGENCE COMMUNITY REGARDING UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION.

(a) REPORTS REQUIRED.—Not less frequently than once every 6 months, the Assistant Attorney General for National Security of the Department of Justice, in consultation with the Director of the Federal Bureau of Investigation, shall submit to the congressional intelligence committees 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.

(b) CONTENTS.—Each report submitted under subsection (a) shall include, for each referral covered by the report, at a minimum, the following:

(1) The date the referral was received.

(2) A statement indicating whether the alleged unauthorized disclosure described in the referral was substantiated by the Department of Justice.

(3) A statement indicating the highest level of classification of the information that was revealed in the unauthorized disclosure.

(4) A statement indicating whether an open criminal investigation related to the referral is active.

(5) A statement indicating whether any criminal charges have been filed related to the referral.

(6) A statement indicating whether the Department of Justice has been able to attribute the unauthorized disclosure to a particular entity or individual.

(c) FORM OF REPORT.—Each report submitted under subsection (a) shall be submitted in unclassified form, but may have a classified annex.

SEC. 617. NOTIFICATIONS OF DESIGNATION OF AN INTELLIGENCE OFFICER AS A PERSONA NON GRATA.

(a) REQUIREMENT FOR REPORTS.—Not later than 72 hours after an intelligence officer is designated as a persona non grata, the Director of National Intelligence, in consultation with the Secretary of State, shall submit

to the congressional intelligence committees a notification of that designation. Each such notification shall include—

(1) the date of the designation;

(2) the basis for the designation; and

(3) a justification for the expulsion.

(b) INTELLIGENCE OFFICER DEFINED.—In this section, the term ''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.

SEC. 618. 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) REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, and biennially thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees a report on foreign investment risks prepared by the interagency working group established under subsection (a).

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

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

(B) Any macro trends in foreign investment of a country that such interagency working group has identified to be a country of special concern.

(C) Any strategy used by such a country to exploit a vulnerability identified under subparagraph (A) through the acquisition of crit-

ical technologies, critical materials, or critical infrastructure.

(D) Any market distortion or unfair competition by a foreign country in the form of market barriers, nonreciprocal investment treatment, subsidies, government corruption, compulsory technology transfer, or theft of intellectual property.

SEC. 619. REPORT ON SURVEILLANCE BY FOREIGN GOVERNMENTS AGAINST UNITED STATES TELECOMMUNICATIONS NETWORKS.

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 congressional intelligence committees a report describing—

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

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

SEC. 620. REPORTS ON AUTHORITIES OF THE CHIEF INTELLIGENCE OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) DEFINITIONS.—In this section:

(1) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(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.

(3) OFFICE.—The term ''Office'' means the Office of Intelligence and Analysis of the Department.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(5) UNDER SECRETARY.—The term ''Under Secretary'' means the Under Secretary for Intelligence and Analysis of the Department.

(b) REQUIREMENT FOR REPORT.—Not later than 120 days after the date of the enactment of this Act, the

Secretary, in consultation with the Under Secretary, shall submit to the congressional intelligence committees a report on the authorities of the Under Secretary.

(c) CONTENTS.—The report required by subsection (b) shall include 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 and the Homeland Security Intelligence Council, over which the Chief Intelligence Officer chairs; 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—

(A) to coordinate intelligence programs; and

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

SEC. 621. REPORT ON GEOSPATIAL COMMERCIAL ACTIVITIES FOR BASIC AND APPLIED RESEARCH AND DEVELOPMENT.

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

(1) rapid technology change and a significant increase in data collection by the intelligence community has outpaced the ability of the intelligence community to exploit vast quantities of intelligence data;

(2) the data collection capabilities of the intelligence community and the Department of Defense have outpaced their ability to exploit vast quantities of data;

(3) furthermore, international competitors may be catching up, and in some cases leading, in key technology areas;

(4) many United States companies have talent and technological capabilities that the Federal Government could harness; and

(5) these companies would be able to more effectively develop automation, artificial intelligence, and associated algorithms if given access to data of

the National Geospatial-Intelligence Agency, consistent with the protection of sources and methods.

(b) REPORT.—Not later than 30 days after the date of the enactment of this Act, the Director of the National Geospatial-Intelligence Agency shall submit to the appropriate congressional committees a report on the authorities necessary to conduct commercial activities relating to geospatial intelligence that the Director determines necessary to engage in basic research, applied research, data transfers, and development projects, with respect to automation, artificial intelligence, and associated algorithms, including how the Director would use such authorities, consistent with applicable laws and procedures relating to the protection of sources and methods.

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

(1) the Committee on Armed Services and the Select Committee on Intelligence of the Senate; and

(2) the Committee on Armed Services and the Permanent Select Committee on Intelligence of the House of Representatives.

SEC. 622. 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 (I), by realigning the margin of such subparagraph 2 ems to the left.

SEC. 623. SENSE OF CONGRESS ON WIKILEAKS.

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

Calendar No. 207

115TH CONGRESS
1ST SESSION

S. 1761

A BILL

To authorize appropriations for fiscal year 2018 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

AUGUST 18, 2017

Read twice and placed on the calendar