

## 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.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

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

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

Sec. 1. Short title; table of contents.  
 Sec. 2. Definitions.

#### TITLE I—INTELLIGENCE ACTIVITIES

Sec. 101. Authorization of appropriations.  
 Sec. 102. Classified Schedule of Authorizations.  
 Sec. 103. Personnel ceiling adjustments.  
 Sec. 104. Intelligence Community Management Account.

#### TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Sec. 201. Authorization of appropriations.

#### TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

Sec. 301. Restriction on conduct of intelligence activities.  
 Sec. 302. Increase in employee compensation and benefits authorized by law.  
 Sec. 303. Modification of special pay authority for science, technology, engineering, or mathematics positions and addition of special pay authority for cyber positions.  
 Sec. 304. Director of National Intelligence review of placement of positions within the intelligence community on the Executive Schedule.  
 Sec. 305. Modification of appointment of Chief Information Officer of the Intelligence Community.  
 Sec. 306. Supply Chain and Counterintelligence Risk Management Task Force.  
 Sec. 307. Inspector General of the Intelligence Community auditing authority.  
 Sec. 308. Inspectors General studies on classification.

#### 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.  
 Sec. 402. Information sharing with State election officials.  
 Sec. 403. Technical modification to the Executive Schedule.  
 Sec. 404. Modification to the designation of the program manager-information sharing environment.

##### Subtitle B—Central Intelligence Agency

Sec. 411. Repeal of foreign language proficiency requirement for certain senior level positions in the Central Intelligence Agency.

##### Subtitle C—Other Elements

Sec. 421. Designation of the Counterintelligence Directorate of the Defense Security Service as an element of the intelligence community.

#### TITLE V—SECURING ENERGY INFRASTRUCTURE

- Sec. 501. Short title.
- Sec. 502. Definitions.
- Sec. 503. Pilot program for securing energy infrastructure.
- Sec. 504. Working group to evaluate program standards and develop strategy.
- Sec. 505. Reports on the Program.
- Sec. 506. No new regulatory authority for Federal agencies.
- Sec. 507. Exemption from disclosure.
- Sec. 508. Protection from liability.
- Sec. 509. Authorization of appropriations.

#### TITLE VI—REPORTS AND OTHER MATTERS

- Sec. 601. Technical correction to Inspector General study.
- Sec. 602. Governance for security clearance, suitability and fitness for employment, and credentialing.
- Sec. 603. Process for security clearances.
- Sec. 604. Reports on the vulnerabilities equities policy and process of the Federal Government.
- Sec. 605. Bug bounty programs.
- Sec. 606. Report on cyber attacks by foreign governments against United States election infrastructure.
- Sec. 607. Review of intelligence community's posture to collect against and analyze Russian efforts to influence the presidential election.
- Sec. 608. Assessment of foreign intelligence threats to Federal elections.
- Sec. 609. Strategy for countering Russian cyber threats to United States elections.
- Sec. 610. Limitation relating to establishment or support of cyber security unit with the Government of Russia.
- Sec. 611. Report on returning Russian compounds.
- Sec. 612. Intelligence community assessment on threat of Russian money laundering to the United States.
- Sec. 613. Notification of an active measures campaign.
- Sec. 614. Notification of travel by accredited diplomatic and consular personnel of the Russian Federation in the United States.
- Sec. 615. Modification of certain reporting requirement on travel of foreign diplomats.
- Sec. 616. Semiannual report on referrals to Department of Justice by elements of the intelligence community regarding unauthorized disclosure of classified information.
- Sec. 617. Notifications of designation of an intelligence officer as a persona non grata.
- Sec. 618. Biennial report on foreign investment risks.
- Sec. 619. Report on surveillance by foreign governments against United States telecommunications networks.
- Sec. 620. Reports on authorities of the Chief Intelligence Officer of the Department of Homeland Security.
- Sec. 621. Report on geospatial commercial activities for basic and applied research and development.
- Sec. 622. Technical amendments related to the Department of Energy.
- Sec. 623. Sense of Congress on WikiLeaks.

## 1 SEC. 2. DEFINITIONS.

2 In this Act:

1 (1) CONGRESSIONAL INTELLIGENCE COMMIT-  
 2 TEES.—The term “congressional intelligence com-  
 3 mittees” means—

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

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

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

## 12 **TITLE I—INTELLIGENCE** 13 **ACTIVITIES**

### 14 **SEC. 101. AUTHORIZATION OF APPROPRIATIONS.**

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

19 (1) The Office of the Director of National Intel-  
 20 ligence.

21 (2) The Central Intelligence Agency.

22 (3) The Department of Defense.

23 (4) The Defense Intelligence Agency.

24 (5) The National Security Agency.

1           (6) The Department of the Army, the Depart-  
2           ment of the Navy, and the Department of the Air  
3           Force.

4           (7) The Coast Guard.

5           (8) The Department of State.

6           (9) The Department of the Treasury.

7           (10) The Department of Energy.

8           (11) The Department of Justice.

9           (12) The Federal Bureau of Investigation.

10          (13) The Drug Enforcement Administration.

11          (14) The National Reconnaissance Office.

12          (15) The National Geospatial-Intelligence Agen-  
13          cy.

14          (16) The Department of Homeland Security.

15   **SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.**

16          (a) SPECIFICATIONS OF AMOUNTS.—The amounts  
17          authorized to be appropriated under section 101 and, sub-  
18          ject to section 103, the authorized personnel ceilings as  
19          of September 30, 2018, for the conduct of the intelligence  
20          activities of the elements listed in paragraphs (1) through  
21          (16) of section 101, are those specified in the classified  
22          Schedule of Authorizations prepared to accompany this  
23          Act.

24          (b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AU-  
25          THORIZATIONS.—

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

6           (2) DISTRIBUTION BY THE PRESIDENT.—Sub-  
7       ject to paragraph (3), the President shall provide for  
8       suitable distribution of the classified Schedule of Au-  
9       thorizations referred to in subsection (a), or of ap-  
10      propriate portions of such Schedule, within the exec-  
11      utive branch.

12          (3) LIMITS ON DISCLOSURE.—The President  
13      shall not publicly disclose the classified Schedule of  
14      Authorizations or any portion of such Schedule ex-  
15      cept—

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

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

21            (C) as otherwise required by law.

22   **SEC. 103. PERSONNEL CEILING ADJUSTMENTS.**

23          (a) AUTHORITY FOR INCREASES.—The Director of  
24      National Intelligence may authorize employment of civil-  
25      ian personnel in excess of the number authorized for fiscal

1 year 2018 by the classified Schedule of Authorizations re-  
2 ferred to in section 102(a) if the Director of National In-  
3 telligence determines that such action is necessary to the  
4 performance of important intelligence functions, except  
5 that the number of personnel employed in excess of the  
6 number authorized under such section may not, for any  
7 element of the intelligence community, exceed—

8 (1) 3 percent of the number of civilian per-  
9 sonnel authorized under such schedule for such ele-  
10 ment; or

11 (2) 10 percent of the number of civilian per-  
12 sonnel authorized under such schedule for such ele-  
13 ment for the purposes of converting the performance  
14 of any function by contractors to performance by ci-  
15 vilian personnel.

16 (b) TREATMENT OF CERTAIN PERSONNEL.—The Di-  
17 rector of National Intelligence shall establish guidelines  
18 that govern, for each element of the intelligence commu-  
19 nity, the treatment under the personnel levels authorized  
20 under section 102(a), including any exemption from such  
21 personnel levels, of employment or assignment in—

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

24 (2) a reserve corps or as a reemployed annu-  
25 itant; or

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

3       (c) NOTICE TO CONGRESSIONAL INTELLIGENCE  
4 COMMITTEES.—Not later than 15 days prior to the exer-  
5 cise of an authority described in subsection (a), the Direc-  
6 tor of National Intelligence shall submit to the congres-  
7 sional intelligence committees—

8           (1) a written notice of the exercise of such au-  
9       thority; and

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

14 **SEC. 104. INTELLIGENCE COMMUNITY MANAGEMENT AC-**  
15 **COUNT.**

16       (a) AUTHORIZATION OF APPROPRIATIONS.—There is  
17 authorized to be appropriated for the Intelligence Commu-  
18 nity Management Account of the Director of National In-  
19 telligence for fiscal year 2018 the sum of \$550,200,000.  
20 Within such amount, funds identified in the classified  
21 Schedule of Authorizations referred to in section 102(a)  
22 for advanced research and development shall remain avail-  
23 able until September 30, 2019.

24       (b) AUTHORIZED PERSONNEL LEVELS.—The ele-  
25 ments within the Intelligence Community Management



1 Account of the Director of National Intelligence are au-  
2 thorized 797 positions as of September 30, 2018. Per-  
3 sonnel serving in such elements may be permanent em-  
4 ployees of the Office of the Director of National Intel-  
5 ligence or personnel detailed from other elements of the  
6 United States Government.

7 (c) CLASSIFIED AUTHORIZATIONS.—

8 (1) AUTHORIZATION OF APPROPRIATIONS.—In  
9 addition to amounts authorized to be appropriated  
10 for the Intelligence Community Management Ac-  
11 count by subsection (a), there are authorized to be  
12 appropriated for the Intelligence Community Man-  
13 agement Account for fiscal year 2018 such addi-  
14 tional amounts as are specified in the classified  
15 Schedule of Authorizations referred to in section  
16 102(a). Such additional amounts made available for  
17 advanced research and development shall remain  
18 available until September 30, 2019.

19 (2) AUTHORIZATION OF PERSONNEL.—In addi-  
20 tion to the personnel authorized by subsection (b)  
21 for elements of the Intelligence Community Manage-  
22 ment Account as of September 30, 2018, there are  
23 authorized such additional personnel for the Com-  
24 munity Management Account as of that date as are

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

3 **TITLE II—CENTRAL INTEL-**  
4 **LIGENCE AGENCY RETIRE-**  
5 **MENT AND DISABILITY SYS-**  
6 **TEM**

7 **SEC. 201. AUTHORIZATION OF APPROPRIATIONS.**

8 There is authorized to be appropriated for the Cen-  
9 tral Intelligence Agency Retirement and Disability Fund  
10 for fiscal year 2018 the sum of \$514,000,000.

11 **TITLE III—GENERAL INTEL-**  
12 **LIGENCE COMMUNITY MAT-**  
13 **TERS**

14 **SEC. 301. RESTRICTION ON CONDUCT OF INTELLIGENCE**  
15 **ACTIVITIES.**

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

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

22 Appropriations authorized by this Act for salary, pay,  
23 retirement, and other benefits for Federal employees may  
24 be increased by such additional or supplemental amounts

1 as may be necessary for increases in such compensation  
 2 or benefits authorized by law.

3 **SEC. 303. MODIFICATION OF SPECIAL PAY AUTHORITY FOR**  
 4 **SCIENCE, TECHNOLOGY, ENGINEERING, OR**  
 5 **MATHEMATICS POSITIONS AND ADDITION OF**  
 6 **SPECIAL PAY AUTHORITY FOR CYBER POSI-**  
 7 **TIONS.**

8 (a) IN GENERAL.—Section 113B of the National Se-  
 9 curity Act of 1947 (50 U.S.C. 3049a) is amended—

10 (1) by amending subsection (a) to read as fol-  
 11 lows:

12 “(a) SPECIAL RATES OF PAY FOR POSITIONS RE-  
 13 QUIRING EXPERTISE IN SCIENCE, TECHNOLOGY, ENGI-  
 14 NEERING, OR MATHEMATICS.—

15 “(1) IN GENERAL.—Notwithstanding part III  
 16 of title 5, United States Code, the head of each ele-  
 17 ment of the intelligence community may, for 1 or  
 18 more categories of positions in such element that re-  
 19 quire expertise in science, technology, engineering,  
 20 or mathematics (STEM)—

21 “(A) establish higher minimum rates of  
 22 pay; and

23 “(B) make corresponding increases in all  
 24 rates of pay of the pay range for each grade or

1 level, subject to subsection (b) or (c), as appli-  
 2 cable.

3 “(2) TREATMENT.—The special rate supple-  
 4 ments resulting from the establishment of higher  
 5 rates under paragraph (1) shall be basic pay for the  
 6 same or similar purposes as those specified in sec-  
 7 tion 5305(j) of title 5, United States Code.”;

8 (2) by striking subsection (f);

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

11 (4) by inserting after subsection (a) the fol-  
 12 lowing:

13 “(b) SPECIAL RATES OF PAY FOR CYBER POSI-  
 14 TIONS.—

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

18 “(A) not to exceed the rate of basic pay  
 19 payable for level II of the Executive Schedule  
 20 under section 5313 of title 5, United States  
 21 Code, if the Director certifies to the Under Sec-  
 22 retary of Defense for Intelligence, in consulta-  
 23 tion with the Under Secretary of Defense for  
 24 Personnel and Readiness, that the rate of pay

1 is for positions that perform functions that exe-  
2 cute the cyber mission of the Agency; or

3 “(B) not to exceed the rate of basic pay  
4 payable for the Vice President of the United  
5 States under section 104 of title 3, United  
6 States Code, if the Director certifies to the Sec-  
7 retary of Defense, by name, individuals that  
8 have advanced skills and competencies and that  
9 perform critical functions that execute the cyber  
10 mission of the Agency.

11 “(2) PAY LIMITATION.—Employees receiving a  
12 special rate under paragraph (1) shall be subject to  
13 an aggregate pay limitation that parallels the limita-  
14 tion established in section 5307 of title 5, United  
15 States Code, except that—

16 “(A) any allowance, differential, bonus,  
17 award, or other similar cash payment in addi-  
18 tion to basic pay that is authorized under title  
19 10, United States Code, (or any other applica-  
20 ble law in addition to title 5 of such Code, ex-  
21 cluding the Fair Labor Standards Act) shall  
22 also be counted as part of aggregate compensa-  
23 tion; and

24 “(B) aggregate compensation may not ex-  
25 ceed the rate established for the Vice President

1 of the United States under section 104 of title  
2 3, United States Code.

3 “(3) LIMITATION ON NUMBER OF RECIPI-  
4 ENTS.—The number of individuals who receive basic  
5 pay established under paragraph (1)(B) may not ex-  
6 ceed 100 at any time.

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

16 (5) in subsection (c), as redesignated by para-  
17 graph (3), by striking “A minimum” and inserting  
18 “Except as provided in subsection (b), a minimum”.

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

22 (1) in subsection (g)(1), by striking “subsection  
23 (h)” and inserting “subsections (h) and (k)”; and

24 (2) by adding at the end the following sub-  
25 sections:

1       “(k)(1) Notwithstanding the rate limitations set forth  
2 in subsections (a)(1) and (g)(2), the Office of Personnel  
3 Management may establish under this section a rate of  
4 pay that does not exceed the rate of basic pay payable  
5 for level II of the Executive Schedule under section 5313  
6 for employees in positions that perform functions that exe-  
7 cute a cyber mission and who are certified to have speci-  
8 fied skills and competencies.

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

16       “(l) An employee who is subject to a reduction or ter-  
17 mination of a special rate of pay established under this  
18 section due to not maintaining a required skill or com-  
19 petency certification, or due to not obtaining a revised skill  
20 or competency certification, shall not be entitled to pay  
21 retention under section 5363 based on any resulting re-  
22 duction in pay.”.

1 **SEC. 304. DIRECTOR OF NATIONAL INTELLIGENCE REVIEW**  
 2 **OF PLACEMENT OF POSITIONS WITHIN THE**  
 3 **INTELLIGENCE COMMUNITY ON THE EXECU-**  
 4 **TIVE SCHEDULE.**

5 The Director of National Intelligence shall conduct  
 6 a review of positions within the intelligence community re-  
 7 garding the placement of such positions on the Executive  
 8 Schedule under subchapter II of chapter 53 of title 5,  
 9 United States Code. In carrying out such review, the Di-  
 10 rector shall determine—

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

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

16 **SEC. 305. MODIFICATION OF APPOINTMENT OF CHIEF IN-**  
 17 **FORMATION OFFICER OF THE INTELLIGENCE**  
 18 **COMMUNITY.**

19 Section 103G(a) of the National Security Act of 1947  
 20 (50 U.S.C. 3032(a)) is amended by striking “President”  
 21 and inserting “Director”.

22 **SEC. 306. SUPPLY CHAIN AND COUNTERINTELLIGENCE**  
 23 **RISK MANAGEMENT TASK FORCE.**

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



1 standardize information sharing between the intelligence  
2 community and the acquisition community of the Govern-  
3 ment of the United States with respect to the supply chain  
4 and counterintelligence risks.

5 (b) MEMBERS.—The Supply Chain and Counterintel-  
6 ligence Risk Management Task Force shall be composed  
7 of—

8 (1) a representative of the Defense Security  
9 Service;

10 (2) a representative of the General Services Ad-  
11 ministration;

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

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

17 (c) SECURITY CLEARANCES.—Each member of the  
18 Supply Chain and Counterintelligence Risk Management  
19 Task Force shall have a security clearance at the Top Se-  
20 cret and Sensitive Compartmented Information level.

21 (d) ANNUAL REPORT.—The Supply Chain and Coun-  
22 terintelligence Risk Management Task Force shall submit  
23 to the congressional intelligence committees an annual re-  
24 port that describes the activities of the Task Force during  
25 the previous year, including identification of the supply

1 chain and counterintelligence risks shared with the acqui-  
 2 sition community of the Government of the United States  
 3 by the intelligence community.

4 **SEC. 307. INSPECTOR GENERAL OF THE INTELLIGENCE**  
 5 **COMMUNITY AUDITING AUTHORITY.**

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

8 (1) by striking “law and the policies of the Di-  
 9 rector of National Intelligence,” and inserting  
 10 “law,”; and

11 (2) by striking “General.” and inserting “Gen-  
 12 eral and is authorized to obtain the temporary or  
 13 intermittent services of experts or consultants or an  
 14 organization thereof.”.

15 **SEC. 308. INSPECTORS GENERAL STUDIES ON CLASSIFICA-**  
 16 **TION.**

17 (a) REQUIREMENT FOR STUDY.—Not later than Oc-  
 18 tober 1, 2019, each Inspector General listed in subsection  
 19 (b) shall carry out and submit to the congressional intel-  
 20 ligence committees a report on the following:

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

24 (2) A study analyzing compliance with declas-  
 25 sification procedures.

1           (3) A study on reviewing processes for identi-  
2       fying topics of public or historical importance that  
3       merit prioritization for a declassification review.

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

6           (1) The Inspector General of the Intelligence  
7       Community.

8           (2) The Inspector General of the Central Intel-  
9       ligence Agency.

10          (3) The Inspector General of the National Se-  
11       curity Agency.

12          (4) The Inspector General of the Defense Intel-  
13       ligence Agency.

14          (5) The Inspector General of the National Re-  
15       connaissance Office.

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

1 **TITLE IV—MATTERS RELATING**  
 2 **TO ELEMENTS OF THE INTEL-**  
 3 **LIGENCE COMMUNITY**

4 **Subtitle A—Office of the Director**  
 5 **of National Intelligence**

6 **SEC. 401. AUTHORITY FOR THE PROTECTION OF CURRENT**  
 7 **AND FORMER EMPLOYEES OF THE OFFICE**  
 8 **OF THE DIRECTOR OF NATIONAL INTEL-**  
 9 **LIGENCE.**

10 Section 5(a)(4) of the Central Intelligence Agency  
 11 Act of 1949 (50 U.S.C. 3506(a)(4)) is amended by strik-  
 12 ing “such personnel of the Office of the Director of Na-  
 13 tional Intelligence as the Director of National Intelligence  
 14 may designate;” and inserting “current and former per-  
 15 sonnel of the Office of the Director of National Intel-  
 16 ligence and their immediate families as the Director of Na-  
 17 tional Intelligence may designate;”.

18 **SEC. 402. INFORMATION SHARING WITH STATE ELECTION**  
 19 **OFFICIALS.**

20 (a) SECURITY CLEARANCES.—

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

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

4 (2) DETERMINATION OF LEVELS.—

5 (A) IN GENERAL.—The Director shall de-  
6 termine the level of clearances for the positions  
7 described in paragraph (1).

8 (B) INTERIM CLEARANCES.—The Director  
9 may issue interim clearances, for a period to be  
10 determined by the Director, to a chief election  
11 official as described in paragraph (1) and up to  
12 one designee of such official under such para-  
13 graph.

14 (b) INFORMATION SHARING.—

15 (1) IN GENERAL.—The Director shall share ap-  
16 propriate classified information related to threats to  
17 election systems and to the integrity of the election  
18 process with chief election officials and such des-  
19 ignees who have received a security clearance under  
20 subsection (a).

21 (2) REPORTS.—The Director shall transmit re-  
22 ports on such information sharing to the respective  
23 affected Secretary of State or States.

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

1 triet of Columbia, the Commonwealth of Puerto Rico, and  
2 any territory or possession of the United States.

3 **SEC. 403. TECHNICAL MODIFICATION TO THE EXECUTIVE**  
4 **SCHEDULE.**

5 Section 5313 of title 5, United States Code, is  
6 amended by adding at the end the following:

7 “Director of the National Counterintelligence  
8 and Security Center.”.

9 **SEC. 404. MODIFICATION TO THE DESIGNATION OF THE**  
10 **PROGRAM MANAGER-INFORMATION SHARING**  
11 **ENVIRONMENT.**

12 (a) INFORMATION SHARING ENVIRONMENT.—Sec-  
13 tion 1016(b) of the Intelligence Reform and Terrorism  
14 Prevention Act of 2004 (6 U.S.C. 485(b)) is amended—

15 (1) in paragraph (1), by striking “President”  
16 and inserting “Director of National Intelligence”;  
17 and

18 (2) in paragraph (2), by striking “President”  
19 both places that term appears and inserting “Direc-  
20 tor of National Intelligence”.

21 (b) PROGRAM MANAGER.—Section 1016(f) of the In-  
22 telligence Reform and Terrorism Prevention Act of 2004  
23 (6 U.S.C. 485(f)) is amended by striking “The individual  
24 designated as the program manager shall serve as pro-  
25 gram manager until removed from service or replaced by

1 the President (at the President’s sole discretion).” and in-  
 2 serting “Beginning on the date of the enactment of the  
 3 Intelligence Authorization Act for Fiscal Year 2018, each  
 4 individual designated as the program manager shall be ap-  
 5 pointed by the Director of National Intelligence.”.

## 6       **Subtitle B—Central Intelligence** 7                                   **Agency**

### 8       **SEC. 411. REPEAL OF FOREIGN LANGUAGE PROFICIENCY** 9                                   **REQUIREMENT FOR CERTAIN SENIOR LEVEL** 10                                  **POSITIONS IN THE CENTRAL INTELLIGENCE** 11                                  **AGENCY.**

12       (a) REPEAL OF FOREIGN LANGUAGE PROFICIENCY  
 13 REQUIREMENT.—Section 104A of the National Security  
 14 Act of 1947 (50 U.S.C. 3036) is amended by striking sub-  
 15 section (g).

16       (b) CONFORMING REPEAL OF REPORT REQUIRE-  
 17 MENT.—Section 611 of the Intelligence Authorization Act  
 18 for Fiscal Year 2005 (Public Law 108–487) is amended  
 19 by striking subsection (c).

1           **Subtitle C—Other Elements**

2   **SEC. 421. DESIGNATION OF THE COUNTERINTELLIGENCE**  
3                   **DIRECTORATE OF THE DEFENSE SECURITY**  
4                   **SERVICE AS AN ELEMENT OF THE INTEL-**  
5                   **LIGENCE COMMUNITY.**

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

9                   (1) by redesignating subparagraphs (H)  
10           through (L) as subparagraphs (I) through (M), re-  
11           spectively; and

12                   (2) by inserting after subparagraph (G) the fol-  
13           lowing:

14                           “(H) The Counterintelligence Directorate  
15                   of the Defense Security Service of the Depart-  
16                   ment of Defense.”.

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



1       **TITLE V—SECURING ENERGY**  
2                   **INFRASTRUCTURE**

3   **SEC. 501. SHORT TITLE.**

4       This title may be cited as the “Securing Energy In-  
5   frastructure Act of 2017”.

6   **SEC. 502. DEFINITIONS.**

7       In this title:

8           (1) COVERED ENTITY.—The term “covered en-  
9       tity” means an entity identified pursuant to section  
10      9(a) of Executive Order 13636 of February 12,  
11      2013 (78 Fed. Reg. 11742) relating to identification  
12      of critical infrastructure where a cybersecurity inci-  
13      dent could reasonably result in catastrophic regional  
14      or national effects on public health or safety, eco-  
15      nomic security, or national security.

16          (2) DIRECTOR.—Except as otherwise specifi-  
17       cally provided, the term “Director” means the Direc-  
18       tor of Intelligence and Counterintelligence of the De-  
19       partment of Energy.

20          (3) EXPLOIT.—The term “exploit” means a  
21       software tool designed to take advantage of a secu-  
22       rity vulnerability.

23          (4) INDUSTRIAL CONTROL SYSTEM.—

24            (A) IN GENERAL.—The term “industrial  
25       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 INFRA-  
STRUCTURE.**

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-

1       turers in the supply chain) that voluntarily partici-  
 2       pate in the Program to identify new classes of secu-  
 3       rity vulnerabilities of the covered entities; and

4               (2) researching, developing, testing, and imple-  
 5       menting technology platforms and standards, in  
 6       partnership with covered entities, to isolate and de-  
 7       fend industrial control systems of covered entities  
 8       from security vulnerabilities and exploits in the most  
 9       critical systems of the covered entities, including—

10               (A) analog and nondigital control systems;

11               (B) purpose-built control systems; and

12               (C) physical controls.

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

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

17               (1) to evaluate the technology platforms and  
 18       standards used in the Program under section  
 19       503(2); and

20               (2) to develop a national cyber-informed engi-  
 21       neering strategy to isolate and defend covered enti-  
 22       ties from security vulnerabilities and exploits in the  
 23       most critical systems of the covered entities.

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

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

3 (1) The Department of Energy.

4 (2) The energy industry, including electric utili-  
5 ties and manufacturers recommended by the Energy  
6 Sector coordinating councils.

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

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

11 (4) The North American Electric Reliability  
12 Corporation.

13 (5) The Nuclear Regulatory Commission.

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

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

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

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

22 (8) A State or regional energy agency.

23 (9) A national research body or academic insti-  
24 tution.

25 (10) The National Laboratories.

1 **SEC. 505. REPORTS ON THE PROGRAM.**

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

6 (1) describes the results of the Program;

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

9 (3) describes the results of the evaluations con-  
10 ducted by the working group established under sec-  
11 tion 504(a).

12 (b) FINAL REPORT.—Not later than 2 years after the  
13 date on which funds are first disbursed under the Pro-  
14 gram, the Director shall submit to the appropriate com-  
15 mittees of Congress a final report that—

16 (1) describes the results of the Program;

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

19 (3) describes the results of the evaluations con-  
20 ducted by the working group established under sec-  
21 tion 504(a).

22 (c) APPROPRIATE COMMITTEES OF CONGRESS DE-  
23 FINED.—In this section, the term “appropriate commit-  
24 tees of Congress” means—

25 (1) the congressional intelligence committees;

1           (2) the Committee on Energy and Natural Re-  
2           sources of the Senate; and

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

5   **SEC. 506. NO NEW REGULATORY AUTHORITY FOR FEDERAL**  
6                           **AGENCIES.**

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

9   **SEC. 507. EXEMPTION FROM DISCLOSURE.**

10          Information shared by or with the Federal Govern-  
11          ment or a State, tribal, or local government under this  
12          title shall be—

13               (1) deemed to be voluntarily shared informa-  
14               tion; and

15               (2) exempt from disclosure under any provision  
16               of Federal, State, tribal, or local freedom of infor-  
17               mation law, open government law, open meetings  
18               law, open records law, sunshine law, or similar law  
19               requiring the disclosure of information or records.

20   **SEC. 508. PROTECTION FROM LIABILITY.**

21          (a) IN GENERAL.—A cause of action against a cov-  
22          ered entity for engaging in the voluntary activities author-  
23          ized under section 503—

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

1           (2) shall be promptly dismissed by the applica-  
2       ble court.

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

6       **SEC. 509. AUTHORIZATION OF APPROPRIATIONS.**

7       (a) PILOT PROGRAM.—There is authorized to be ap-  
8       propriated \$10,000,000 to carry out section 503.

9       (b) WORKING GROUP AND REPORT.—There is au-  
10      thorized to be appropriated \$1,500,000 to carry out sec-  
11      tions 504 and 505.

12      (c) AVAILABILITY.—Amounts made available under  
13      subsections (a) and (b) shall remain available until ex-  
14      pended.

15      **TITLE VI—REPORTS AND OTHER**  
16                                   **MATTERS**

17      **SEC. 601. TECHNICAL CORRECTION TO INSPECTOR GEN-**  
18                                   **ERAL STUDY.**

19      Section 11001(d) of title 5, United States Code, is  
20      amended—

21           (1) in the subsection heading, by striking  
22      “AUDIT” and inserting “REVIEW”;

23           (2) in paragraph (1), by striking “audit” and  
24      inserting “review”; and

1           (3) in paragraph (2), by striking “audit” and  
2           inserting “review”.

3 **SEC. 602. GOVERNANCE FOR SECURITY CLEARANCE, SUIT-**  
4 **ABILITY AND FITNESS FOR EMPLOYMENT,**  
5 **AND CREDENTIALING.**

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

8           (1) ESTABLISHMENT.—There is an interagency  
9 Security, Suitability, and Credentialing Council (in  
10 this section the “Council”). The Council shall be ac-  
11 countable to the President and to Congress to  
12 achieve the goals of the executive branch vetting en-  
13 terprise.

14           (2) MEMBERSHIP.—

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

17                   (i) One individual who shall be ap-  
18 pointed by the Director of the Office of  
19 Management and Budget.

20                   (ii) The individual serving as the Suit-  
21 ability Executive Agent and the  
22 Credentialing Executive Agent pursuant to  
23 subsections (b) and (c), respectively.



1 (iii) The individual serving as the Se-  
2 curity Executive Agent pursuant to sub-  
3 section (d)(1).

4 (iv) The Under Secretary of Defense  
5 for Intelligence.

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

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

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

15 (A) Ensuring enterprise-wide alignment of  
16 suitability, security, credentialing, and as ap-  
17 propriate, fitness processes.

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

21 (C) Defining requirements for enterprise-  
22 wide reciprocity management information tech-  
23 nology, and develop standards for enterprise-  
24 wide information technology.

25 (D) Working with agencies—

1 (i) to implement continuous perform-  
2 ance improvement programs, policies, and  
3 procedures;

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

6 (iii) to prepare annual reports on re-  
7 sults.

8 (E) Ensuring and overseeing the develop-  
9 ment of tools and techniques for enhancing  
10 background investigations and adjudications.

11 (F) Enabling discussion and consensus res-  
12 olution of differences in processes, policies, and  
13 procedures among the members of the Council,  
14 and other agencies as appropriate.

15 (G) Sharing best practices.

16 (H) Advise the Suitability Executive  
17 Agent, the Credentialing Executive Agent, and  
18 the Security Executive Agent on policies affect-  
19 ing the alignment of investigations and adju-  
20 dications.

21 (I) Working with agencies to develop agen-  
22 cy policies and procedures to enable sharing of  
23 vetting information consistent with the law and  
24 the protection of privacy and civil liberties and

1 to the extent necessary for enterprise-wide effi-  
2 ciency, effectiveness, and security.

3 (J) Monitoring performance to identify and  
4 drive enterprise-level process enhancements,  
5 and make recommendations for changes to ex-  
6 ecutive branch-wide guidance and authorities to  
7 resolve overlaps or close policy gaps where they  
8 may exist.

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

11 (L) Developing and continuously reevaluating and revising outcome-based metrics that  
12 measure the quality, efficiency and effectiveness  
13 of the vetting enterprise.  
14

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

19 (b) SUITABILITY EXECUTIVE AGENT.—

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

23 (2) DUTIES.—The duties of the Suitability Ex-  
24 ecutive Agent are as follows:

1 (A) Pursuant to sections 1103 and 1104 of  
2 title 5, United States Code, and the Civil Serv-  
3 ice Rules, to be responsible for suitability and  
4 fitness by—

5 (i) prescribing suitability standards  
6 and minimum standards of fitness for em-  
7 ployment;

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

11 (iii) prescribing applicable investiga-  
12 tive standards, policies, and procedures for  
13 suitability and fitness;

14 (iv) prescribing suitability and fitness  
15 reciprocity standards;

16 (v) making suitability determinations;  
17 and

18 (vi) taking suitability actions.

19 (B) To issue regulations, guidance, and  
20 standards to fulfill the Director's responsibil-  
21 ities related to suitability and fitness under Ex-  
22 ecutive Order 13488 of January 16, 2009, as  
23 amended.

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

1 agencies, including acting as the final authority  
2 to arbitrate and resolve disputes among the  
3 agencies involving the reciprocity of investiga-  
4 tions and adjudications of suitability and fit-  
5 ness.

6 (D) To continue to initially approve, and  
7 periodically review for renewal, agencies' re-  
8 quests to administer polygraphs in connection  
9 with appointment in the competitive service, in  
10 consultation with the Security Executive Agent  
11 as appropriate.

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

16 (F) Shall, pursuant to section 1104 of title  
17 5, United States Code, prescribe performance  
18 standards and a system of oversight for any  
19 suitability or fitness function delegated by the  
20 Director to the head of another agency, includ-  
21 ing uniform and consistent policies and proce-  
22 dures to ensure the effective, efficient, timely,  
23 and secure completion of delegated functions.

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

1 instructions to the heads of agencies to promote ap-  
2 propriate uniformity, centralization, efficiency, effec-  
3 tiveness, reciprocity, timeliness, and security in proc-  
4 esses relating to determining suitability or fitness.

5 (c) CREDENTIALING EXECUTIVE AGENT.—

6 (1) IN GENERAL.—In addition to serving as the  
7 Suitability Executive Agent, the Director of the Of-  
8 fice of Personnel Management shall also serve as the  
9 Credentialing Executive Agent.

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

12 (A) To develop standards for investiga-  
13 tions, reinvestigations, and continuous vetting  
14 for a covered individual's eligibility for a PIV  
15 credential.

16 (B) To develop adjudicative guidelines for  
17 a covered individual's eligibility for a PIV cre-  
18 dential.

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

22 (D) To develop standards for unfavorable  
23 determinations of eligibility for a PIV creden-  
24 tial, including procedures for denying and re-  
25 voking the eligibility for a PIV credential, for

1 reconsideration of unfavorable determinations,  
2 and for rendering the PIV credential inoper-  
3 able.

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

10 (F) To develop uniform and consistent  
11 policies and procedures to ensure the effective,  
12 efficient, timely, and secure completion of inves-  
13 tigations and adjudications relating to eligibility  
14 for a PIV credential.

15 (G) To monitor and make a continuing re-  
16 view of agency programs for determining eligi-  
17 bility for a PIV credential to determine whether  
18 they are being implemented according to this  
19 section.

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

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

1 lines and instructions to the heads of agencies as  
2 necessary to ensure appropriate uniformity, cen-  
3 tralization, efficiency, effectiveness, and timeliness in  
4 processes relating to eligibility for a PIV credential.

5 (4) PIV CREDENTIAL DEFINED.—In this sub-  
6 section, the term “PIV credential” means a personal  
7 identity verification credential permitting logical and  
8 physical access to Federally controlled facilities and  
9 Federally controlled information systems.

10 (d) SECURITY EXECUTIVE AGENT.—

11 (1) IN GENERAL.—The Director of National In-  
12 telligence shall serve as the Security Executive  
13 Agent.

14 (2) DUTIES.—The duties of the Security Exec-  
15 utive Agent are as follows:

16 (A) To direct the oversight of investiga-  
17 tions, reinvestigations, adjudications, and, as  
18 applicable, polygraphs for eligibility for access  
19 to classified information or eligibility to hold a  
20 sensitive position made by any agency.

21 (B) To make a continuing review of agen-  
22 cies’ national security background investigation  
23 and adjudication programs to determine wheth-  
24 er they are being implemented according to this  
25 section.



1           (C) To develop and issue uniform and con-  
2           sistent policies and procedures to ensure the ef-  
3           fective, efficient, timely, and secure completion  
4           of investigations, polygraphs, and adjudications  
5           relating to determinations of eligibility for ac-  
6           cess to classified information or eligibility to  
7           hold a sensitive position.

8           (D) To serve as the final authority to des-  
9           ignate an agency or agencies, to the extent that  
10          it is not practicable to use the National Back-  
11          ground Investigations Bureau, to conduct inves-  
12          tigations of persons who are proposed for access  
13          to classified information or for eligibility to hold  
14          a sensitive position to ascertain whether such  
15          persons satisfy the criteria for obtaining and re-  
16          taining access to classified information or eligi-  
17          bility to hold a sensitive position.

18          (E) To serve as the final authority to des-  
19          ignate an agency or agencies to determine eligi-  
20          bility for access to classified information or eli-  
21          gibility to hold a sensitive position in accord-  
22          ance with Executive Order 12968 of August 2,  
23          1995, as amended.

24          (F) To ensure reciprocal recognition of eli-  
25          gibility for access to classified information or

1 eligibility to hold a sensitive position among the  
2 agencies, including acting as the final authority  
3 to arbitrate and resolve disputes among the  
4 agencies involving the reciprocity of investiga-  
5 tions and adjudications of eligibility.

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

8 (A) issue guidelines and instructions to the  
9 heads of agencies to ensure appropriate uni-  
10 formity, centralization, efficiency, effectiveness,  
11 timeliness, and security in processes relating to  
12 determinations by agencies of eligibility for ac-  
13 cess to classified information or eligibility to  
14 hold a sensitive position, including such matters  
15 as investigations, polygraphs, adjudications, and  
16 reciprocity;

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

22 (C) assign, in whole or in part, to the head  
23 of any agency (solely or jointly) any of the du-  
24 ties of the Security Executive Agent under  
25 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           (1) REVIEW AND ASSESSMENT OF STAND-  
2 ARDS.—

3           (A) IN GENERAL.—A review of the rela-  
4 tionship among the information requested by  
5 the Questionnaire for National Security Posi-  
6 tions (Standard Form 86), the application of  
7 the Federal Investigative Standards prescribed  
8 by the Office of Personnel Management and the  
9 Office of the Director of National Intelligence,  
10 and the application of the adjudicative guide-  
11 lines under Security Executive Agent Directive  
12 4 (“National Security Adjudicative Guide-  
13 lines”).

14           (B) ASSESSMENT.—An assessment of  
15 whether such Questionnaire, Standards, and  
16 guidelines should be revised to account for the  
17 prospect of a holder of a security clearance be-  
18 coming an insider threat.

19           (2) RECOMMENDATIONS TO IMPROVE BACK-  
20 GROUND INVESTIGATIONS.—Recommendations to  
21 improve the background investigation process, in-  
22 cluding recommendations—

23           (A) to simplify the Questionnaire for Na-  
24 tional Security Positions (Standard Form 86)

1 and increase customer support to applicants  
2 completing such Questionnaire;

3 (B) to use remote and virtual techniques  
4 and centralized locations during field investiga-  
5 tion work;

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

9 (D) to build the capacity of the back-  
10 ground investigation labor sector.

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

16 (4) EVALUATION OF SPLITTING THE BACK-  
17 GROUND INVESTIGATION FUNCTION.—

18 (A) IN GENERAL.—An evaluation of the  
19 impact on costs, quality, and timeliness of secu-  
20 rity clearance background investigations associ-  
21 ated with transferring to the Secretary of De-  
22 fense responsibility for conducting background  
23 investigations for—

24 (i) personnel of the Department of  
25 Defense; or

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

3 (B) ANALYSIS.—An analysis of—

4 (i) the time required for the Secretary  
5 of Defense to gain sufficient institutional  
6 capacity and capability to perform the in-  
7 vestigations described in clauses (i) and (ii)  
8 of subparagraph (A);

9 (ii) past experience with agencies and  
10 departments of the United States having  
11 responsibility for conducting background  
12 investigations, including the transfer to the  
13 Office of Personnel Management of back-  
14 ground investigations for personnel of the  
15 Department of Defense during 2003,  
16 2004, and 2005; and

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

20 (b) POLICY, STRATEGY, AND IMPLEMENTATION.—

21 Not later than 90 days after the date of the enactment  
22 of this Act, the Director of National Intelligence, acting  
23 as the Security Executive Agent in accordance with section  
24 602(d), shall establish the following:

1           (1) POLICY AND IMPLEMENTATION PLAN FOR  
2 INTERIM SECURITY CLEARANCES.—A policy and im-  
3 plementation plan for the issuance of interim secu-  
4 rity clearances.

5           (2) POLICY ON CONSISTENT TREATMENT OF  
6 GOVERNMENT AND CONTRACTOR PERSONNEL.—A  
7 policy and implementation plan to ensure contrac-  
8 tors are treated consistently in the security clearance  
9 process across agencies and departments of the  
10 United States and as compared to employees of such  
11 agencies and departments. Such policy shall ad-  
12 dress—

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

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

18               (C) digitization of background investiga-  
19 tion-related forms;

20               (D) use of the polygraph;

21               (E) the application of the adjudicative  
22 guidelines under Security Executive Agent Di-  
23 rective 4 (“National Security Adjudicative  
24 Guidelines”);

1 (F) reciprocal recognition of clearances  
2 across agencies and departments of the United  
3 States, regardless of status of periodic reinves-  
4 tigation;

5 (G) tracking of clearance files as individ-  
6 uals move from employment with an agency or  
7 department of the United States to employment  
8 in the private sector; and

9 (H) reporting on security incidents and  
10 performance.

11 (3) STRATEGY AND IMPLEMENTATION FOR  
12 PERIODIC REINVESTIGATIONS.—

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

22 (B) EXCEPTION.—The Security Executive  
23 Agent may provide justification if certain popu-  
24 lations are determined to require periodic re-  
25 investigations at regular intervals.



1           (4) POLICY FOR AUTOMATED RECORDS  
 2 CHECKS.—A policy and implementation plan for  
 3 agencies and departments of the United States Gov-  
 4 ernment, as a part of the security clearance process,  
 5 to accept automated records checks generated pursu-  
 6 ant to a security clearance applicant’s employment  
 7 with a prior employer.

8           (5) POLICY AND IMPLEMENTATION FOR SHAR-  
 9 ING OF BACKGROUND INVESTIGATION DATA.—A pol-  
 10 icy and implementation plan for sharing information  
 11 between and among agencies or departments of the  
 12 United States and private entities that is relevant to  
 13 decisions about granting or renewing security clear-  
 14 ances. Such information shall—

15                   (A) pertain to security and human re-  
 16 sources matters; and

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

19 **SEC. 604. REPORTS ON THE VULNERABILITIES EQUITIES**  
 20 **POLICY AND PROCESS OF THE FEDERAL GOV-**  
 21 **ERNMENT.**

22 (a) REPORT POLICY AND PROCESS.—

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

1 the head of each element of the intelligence commu-  
2 nity shall submit to the congressional intelligence  
3 committees a report detailing the process and cri-  
4 teria the head uses for determining whether to sub-  
5 mit a vulnerability for review under the  
6 vulnerabilities equities policy and process of the Fed-  
7 eral Government.

8 (2) FORM.—Each report submitted under para-  
9 graph (1) shall be submitted in unclassified form,  
10 but may include a classified annex.

11 (b) ANNUAL REPORT ON VULNERABILITIES.—

12 (1) IN GENERAL.—Not less frequently than  
13 once each year, the Director of National Intelligence  
14 shall submit to the congressional intelligence com-  
15 mittees a report on—

16 (A) how many vulnerabilities the intel-  
17 ligence community has submitted for review  
18 during the previous calendar year;

19 (B) how many of such vulnerabilities were  
20 ultimately disclosed to the vendor responsible  
21 for correcting the vulnerability during the pre-  
22 vious calendar year; and

23 (C) vulnerabilities disclosed since the pre-  
24 vious report that have either—

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

3 (ii) have not been patched or miti-  
4 gated by the responsible vendor and more  
5 than 180 days have elapsed since the vul-  
6 nerability was disclosed.

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

9 (A) The date the vulnerability was dis-  
10 closed to the responsible vendor.

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

14 (C) An unclassified appendix that in-  
15 cludes—

16 (i) a top-line summary of the aggre-  
17 gate number of vulnerabilities disclosed to  
18 vendors, how many have been patched, and  
19 the average time between disclosure of the  
20 vulnerability and the patching of the vul-  
21 nerability; and

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

1 ability, as defined by thirty day incre-  
 2 ments.

3 (3) FORM.—Each report submitted under para-  
 4 graph (1) shall be in classified form.

5 (c) VULNERABILITIES EQUITIES POLICY AND PROC-  
 6 ESS OF THE FEDERAL GOVERNMENT DEFINED.—In this  
 7 section, the term “vulnerabilities equities policy and proc-  
 8 ess of the Federal Government” means the policy and  
 9 process established by the National Security Council for  
 10 the Federal Government, or successor set of policies and  
 11 processes, establishing policy and responsibilities for dis-  
 12 seminating information about vulnerabilities discovered by  
 13 the Federal Government or its contractors, or disclosed  
 14 to the Federal Government by the private sector in govern-  
 15 ment off-the-shelf (GOTS), commercial off-the-shelf  
 16 (COTS), or other commercial information technology or  
 17 industrial control products or systems (including both  
 18 hardware and software).

19 **SEC. 605. BUG BOUNTY PROGRAMS.**

20 (a) DEFINITIONS.—In this section:

21 (1) BUG BOUNTY PROGRAM.—The term “bug  
 22 bounty program” means a program under which an  
 23 approved computer security specialist or security re-  
 24 searcher is temporarily authorized to identify and re-

1 port vulnerabilities within an information system in  
2 exchange for payment.

3 (2) INFORMATION SYSTEM.—The term “infor-  
4 mation system” has the meaning given that term in  
5 section 3502 of title 44, United States Code.

6 (b) BUG BOUNTY PROGRAM PLAN.—

7 (1) REQUIREMENT.—Not later than 180 days  
8 after the date of the enactment of this Act, the  
9 Under Secretary for Intelligence and Analysis of the  
10 Department of Homeland Security shall submit to  
11 the congressional intelligence committees a strategic  
12 plan to implement bug bounty programs at appro-  
13 priate agencies and departments of the United  
14 States.

15 (2) CONTENTS.—The plan required by para-  
16 graph (1) shall include—

17 (A) an assessment of—

18 (i) the effectiveness of the “Hack the  
19 Pentagon” pilot program carried out by  
20 the Department of Defense in 2016 and  
21 subsequent bug bounty programs in identi-  
22 fying and reporting vulnerabilities within  
23 the information systems of the Department  
24 of Defense; and

1 (ii) private sector bug bounty pro-  
 2 grams, including such programs imple-  
 3 mented by leading technology companies in  
 4 the United States; and

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

8 **SEC. 606. REPORT ON CYBER ATTACKS BY FOREIGN GOV-**  
 9 **ERNMENTS AGAINST UNITED STATES ELEC-**  
 10 **TION INFRASTRUCTURE.**

11 (a) REPORT REQUIRED.—Not later than 60 days  
 12 after the date of the enactment of this Act, the Under  
 13 Secretary of Homeland Security for Intelligence and Anal-  
 14 ysis shall submit to congressional leadership and the con-  
 15 gressional intelligence committees a report on cyber at-  
 16 tacks and attempted cyber attacks by foreign governments  
 17 on United States election infrastructure in States and lo-  
 18 calities in connection with the 2016 presidential election  
 19 in the United States and such cyber attacks or attempted  
 20 cyber attacks as the Under Secretary anticipates against  
 21 such infrastructure. Such report shall identify the States  
 22 and localities affected and shall include cyber attacks and  
 23 attempted cyber attacks against voter registration data-  
 24 bases, voting machines, voting-related computer networks,

1 and the networks of secretaries of State and other election  
2 officials.

3 (b) FORM.—The report submitted under subsection  
4 (a) shall be submitted in unclassified form, but may in-  
5 clude a classified annex.

6 (c) DEFINITIONS.—In this section:

7 (1) CONGRESSIONAL LEADERSHIP.—The term  
8 “congressional leadership” includes the following:

9 (A) The majority leader of the Senate.

10 (B) The minority leader of the Senate.

11 (C) The Speaker of the House of Rep-  
12 resentatives.

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

15 (2) STATE.—The term “State” means any  
16 State of the United States, the District of Columbia,  
17 the Commonwealth of Puerto Rico, and any territory  
18 or possession of the United States.

19 **SEC. 607. REVIEW OF INTELLIGENCE COMMUNITY’S POS-**  
20 **TURE TO COLLECT AGAINST AND ANALYZE**  
21 **RUSSIAN EFFORTS TO INFLUENCE THE PRES-**  
22 **IDENTIAL ELECTION.**

23 (a) ASSESSMENT REQUIRED.—Not later than one  
24 year after the date of the enactment of this Act, the Direc-  
25 tor of National Intelligence shall—

1           (1) complete an after action review of the intel-  
2       ligence community's posture to collect against and  
3       analyze efforts of the Government of Russia to inter-  
4       fere in the 2016 presidential election in the United  
5       States; and

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

9       (b) ELEMENTS.—The review required by subsection  
10   (a) shall include, with respect to the posture and efforts  
11   described in paragraph (1) of such subsection, the fol-  
12   lowing:

13           (1) An assessment of whether the resources of  
14       the intelligence community were properly aligned to  
15       detect and respond to the efforts described in sub-  
16       section (a)(1).

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

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

23           (4) An assessment of applicable authorities nec-  
24       essary to collect on any such efforts and any defi-  
25       ciencies in those authorities.



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

3           (6) A review of the use of alternative and pre-  
4           dictive analysis.

5           (c) FORM OF REPORT.—The report required by sub-  
6           section (a)(2) shall be submitted to the congressional intel-  
7           ligence committees in a classified form.

8   **SEC. 608. ASSESSMENT OF FOREIGN INTELLIGENCE**  
9                           **THREATS TO FEDERAL ELECTIONS.**

10          (a) IN GENERAL.—The Director of National Intel-  
11          ligence, in coordination with the Director of the Central  
12          Intelligence Agency, the Director of the National Security  
13          Agency, the Director of the Federal Bureau of Investiga-  
14          tion, the Secretary of Homeland Security, and the heads  
15          of other relevant elements of the intelligence community,  
16          shall—

17                (1) commence not later than 1 year before any  
18                regularly scheduled Federal election and complete  
19                not later than 180 days before such election, an as-  
20                sessment of security vulnerabilities of State election  
21                systems; and

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

1 (A) congressional leadership; and

2 (B) the congressional intelligence commit-  
3 tees.

4 (b) UPDATE.—Not later than 90 days before any reg-  
5 ularly scheduled Federal election, the Director of National  
6 Intelligence shall—

7 (1) update the assessment of foreign intel-  
8 ligence threats to that election; and

9 (2) submit the updated assessment to—

10 (A) congressional leadership; and

11 (B) the congressional intelligence commit-  
12 tees.

13 (c) DEFINITIONS.—In this section:

14 (1) CONGRESSIONAL LEADERSHIP.—The term  
15 “congressional leadership” includes the following:

16 (A) The majority leader of the Senate.

17 (B) The minority leader of the Senate.

18 (C) The Speaker of the House of Rep-  
19 resentatives.

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

22 (2) SECURITY VULNERABILITY.—The term “se-  
23 curity vulnerability” has the meaning given such  
24 term in section 102 of the Cybersecurity Information  
25 Sharing Act of 2015 (6 U.S.C. 1501).

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

3 (a) REQUIREMENT FOR A STRATEGY.—Not later  
4 than 90 days after the date of the enactment of this Act,  
5 the Director of National Intelligence, in coordination with  
6 the Secretary of Homeland Security, the Director of the  
7 Federal Bureau of Investigation, the Director of the Cen-  
8 tral Intelligence Agency, the Secretary of State, the Sec-  
9 retary of Defense, and the Secretary of the Treasury, shall  
10 develop a whole-of-government strategy for countering the  
11 threat of Russian cyber attacks and attempted cyber at-  
12 tacks against electoral systems and processes in the  
13 United States, including Federal, State, and local election  
14 systems, voter registration databases, voting tabulation  
15 equipment, and equipment and processes for the secure  
16 transmission of election results.

17 (b) ELEMENTS OF THE STRATEGY.—The strategy re-  
18 quired by subsection (a) shall include the following ele-  
19 ments:

20 (1) A whole-of-government approach to pro-  
21 tecting United States electoral systems and proc-  
22 esses that includes the agencies and departments in-  
23 dicated in subsection (a) as well as any other agen-  
24 cies and departments of the United States, as deter-  
25 mined appropriate by the Director of National Intel-  
26 ligence and the Secretary of Homeland Security.

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

4           (3) Technical security measures, including  
5           auditable paper trails for voting machines, securing  
6           wireless and Internet connections, and other tech-  
7           nical safeguards.

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

11          (5) Improvements in the identification and at-  
12          tribution of Russian government or nongovernment  
13          cyber threat actors.

14          (6) Deterrence, including actions and measures  
15          that could or should be undertaken against or com-  
16          municated to the Government of Russia or other en-  
17          tities to deter attacks against, or interference with,  
18          United States election systems and processes.

19          (7) Improvements in Federal Government com-  
20          munications with State and local election officials.

21          (8) Public education and communication ef-  
22          forts.

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

1 (c) REPORT TO CONGRESS.—Not later than 90 days  
2 after the date of the enactment of this Act, the Director  
3 of National Intelligence and the Secretary of Homeland  
4 Security shall brief the congressional intelligence commit-  
5 tees on the strategy developed under subsection (a).

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

9 (a) LIMITATION.—No amount may be expended by  
10 the Federal Government to establish or support a cyber  
11 security unit or other cyber agreement that is jointly es-  
12 tablished or otherwise implemented by the Government of  
13 the United States and the Government of Russia unless,  
14 at least 30 days prior to the establishment of such agree-  
15 ment, the Director of National Intelligence submits to the  
16 congressional intelligence committees a report on such  
17 agreement that includes the elements required by sub-  
18 section (b).

19 (b) REPORT ELEMENTS.—If the Director submits a  
20 report under subsection (a), such report shall include a  
21 description of each of the following:

22 (1) The purpose of the agreement.

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

1           (3) The expected value to national security re-  
2           sulting from the implementation of the agreement.

3           (4) Such counterintelligence concerns associated  
4           with the agreement as the Director may have and  
5           such measures as the Director expects to be taken  
6           to mitigate such concerns.

7   **SEC. 611. REPORT ON RETURNING RUSSIAN COMPOUNDS.**

8           (a) COVERED COMPOUNDS DEFINED.—In this sec-  
9           tion, the term “covered compounds” means the real prop-  
10          erty in New York and the real property in Maryland that  
11          were under the control of the Government of Russia in  
12          2016 and were removed from such control in response to  
13          various transgressions by the Government of Russia, in-  
14          cluding the interference by the Government of Russia in  
15          the 2016 election in the United States.

16          (b) REQUIREMENT FOR REPORT.—Not later than  
17          180 days after the date of the enactment of this Act, the  
18          Director of National Intelligence shall submit to the con-  
19          gressional intelligence committees a report on the intel-  
20          ligence risks of returning the covered compounds to Rus-  
21          sian control.

22          (c) FORM OF REPORT.—The report required by sub-  
23          section (b) shall be submitted in classified and unclassified  
24          forms.

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

4 (a) **ASSESSMENT REQUIRED.**—Not later than 180  
5 days after the date of the enactment of this Act, the Direc-  
6 tor of National Intelligence, in coordination with the Sec-  
7 retary of the Treasury, shall submit to the congressional  
8 intelligence committees an intelligence community assess-  
9 ment on the threat of Russian money laundering to the  
10 United States. The assessment shall be based on all-source  
11 intelligence, including from the intelligence community  
12 and from all elements of the Department of the Treasury  
13 under the Office of Terrorism and Financial Intelligence.

14 (b) **ELEMENTS.**—The assessment required by sub-  
15 section (a) shall cover the following:

16 (1) Money laundering in the Russian Federa-  
17 tion, global nodes of money laundering used by Rus-  
18 sian and associated entities, and the entry points of  
19 money laundering by Russian and associated entities  
20 into the United States.

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

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

4           (4) The counterintelligence threat posed by  
5           Russian money laundering as well as the threat to  
6           the United States financial system and United  
7           States efforts to enforce sanctions and combat orga-  
8           nized crime.

9   **SEC. 613. NOTIFICATION OF AN ACTIVE MEASURES CAM-**  
10                   **PAIGN.**

11       (a) REQUIREMENT FOR NOTIFICATION.—The Direc-  
12       tor of National Intelligence, in cooperation with the Direc-  
13       tor of the Federal Bureau of Investigation and the head  
14       of any other relevant agency, shall notify the Chairman  
15       and Vice Chairman or Ranking Member of each of the  
16       congressional intelligence committees, and of other rel-  
17       evant committees of jurisdiction, each time the Director  
18       of National Intelligence determines there is credible infor-  
19       mation that a foreign power has, is, or will attempt to  
20       employ a covert influence or active measures campaign  
21       with regard to the modernization, employment, doctrine,  
22       or force posture of the nuclear deterrent or missile de-  
23       fense.

24       (b) CONTENT OF NOTIFICATION.—Each notification  
25       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 DIP-  
LOMATIC 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 busi-  
ness days in advance of all travel by accredited dip-  
lomatic and consular personnel of the Russian Fed-  
eration in the United States, and take necessary ac-  
tion to secure full compliance by Russian personnel  
and address any noncompliance; and

(2) provide notice of travel described in para-  
graph (1) to the Director of National Intelligence  
and the Director of the Federal Bureau of Investiga-  
tion within 1 hour of receiving notice of such travel.

1 **SEC. 615. MODIFICATION OF CERTAIN REPORTING RE-**  
 2 **QUIREMENT ON TRAVEL OF FOREIGN DIP-**  
 3 **LOMATS.**

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

7 **SEC. 616. SEMIANNUAL REPORT ON REFERRALS TO DE-**  
 8 **PARTMENT OF JUSTICE BY ELEMENTS OF**  
 9 **THE INTELLIGENCE COMMUNITY REGARDING**  
 10 **UNAUTHORIZED DISCLOSURE OF CLASSIFIED**  
 11 **INFORMATION.**

12 (a) **REPORTS REQUIRED.**—Not less frequently than  
 13 once every 6 months, the Assistant Attorney General for  
 14 National Security of the Department of Justice, in con-  
 15 sultation with the Director of the Federal Bureau of In-  
 16 vestigation, shall submit to the congressional intelligence  
 17 committees a report on the status of each referral made  
 18 to the Department of Justice from any element of the in-  
 19 telligence community regarding an unauthorized disclo-  
 20 sure of classified information made during the most recent  
 21 365-day period or any referral that has not yet been  
 22 closed, regardless of the date the referral was made.

23 (b) **CONTENTS.**—Each report submitted under sub-  
 24 section (a) shall include, for each referral covered by the  
 25 report, at a minimum, the following:

26 (1) The date the referral was received.

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

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

7           (4) A statement indicating whether an open  
8           criminal investigation related to the referral is ac-  
9           tive.

10          (5) A statement indicating whether any crimi-  
11          nal charges have been filed related to the referral.

12          (6) A statement indicating whether the Depart-  
13          ment of Justice has been able to attribute the unau-  
14          thorized disclosure to a particular entity or indi-  
15          vidual.

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

19      **SEC. 617. NOTIFICATIONS OF DESIGNATION OF AN INTEL-**  
20                              **LIGENCE OFFICER AS A PERSONA NON**  
21                              **GRATA.**

22          (a) REQUIREMENT FOR REPORTS.—Not later than  
23          72 hours after an intelligence officer is designated as a  
24          persona non grata, the Director of National Intelligence,  
25          in consultation with the Secretary of State, shall submit

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

- 3 (1) the date of the designation;
- 4 (2) the basis for the designation; and
- 5 (3) a justification for the expulsion.

6 (b) INTELLIGENCE OFFICER DEFINED.—In this sec-  
 7 tion, the term “intelligence officer” means—

- 8 (1) a United States intelligence officer serving
- 9 in a post in a foreign country; or
- 10 (2) a known or suspected foreign intelligence of-
- 11 ficer serving in a United States post.

12 **SEC. 618. BIENNIAL REPORT ON FOREIGN INVESTMENT**  
 13 **RISKS.**

14 (a) INTELLIGENCE COMMUNITY INTERAGENCY  
 15 WORKING GROUP.—

16 (1) REQUIREMENT TO ESTABLISH.—The Direc-  
 17 tor of National Intelligence shall establish an intel-  
 18 ligence community interagency working group to  
 19 prepare the biennial reports required by subsection

20 (b).

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

24 (3) MEMBERSHIP.—Such interagency working  
 25 group shall be composed of representatives of each

1 element of the intelligence community that the Di-  
2 rector of National Intelligence determines appro-  
3 priate.

4 (b) BIENNIAL REPORT ON FOREIGN INVESTMENT  
5 RISKS.—

6 (1) REQUIREMENT.—Not later than 180 days  
7 after the date of the enactment of this Act, and bi-  
8 ennially thereafter, the Director of National Intel-  
9 ligence shall submit to the congressional intelligence  
10 committees a report on foreign investment risks pre-  
11 pared by the interagency working group established  
12 under subsection (a).

13 (2) CONTENT.—Each report required by para-  
14 graph (1) shall include an identification, analysis,  
15 and explanation of the following:

16 (A) Any current or projected major vulner-  
17 ability to the national security of the United  
18 States with respect to foreign investment.

19 (B) Any macro trends in foreign invest-  
20 ment of a country that such interagency work-  
21 ing group has identified to be a country of spe-  
22 cial concern.

23 (C) Any strategy used by such a country  
24 to exploit a vulnerability identified under sub-  
25 paragraph (A) through the acquisition of crit-

1            ical technologies, critical materials, or critical  
2            infrastructure.

3            (D) Any market distortion or unfair com-  
4            petition by a foreign country in the form of  
5            market barriers, nonreciprocal investment treat-  
6            ment, subsidies, government corruption, com-  
7            pulsory technology transfer, or theft of intellec-  
8            tual property.

9    **SEC. 619. REPORT ON SURVEILLANCE BY FOREIGN GOV-**  
10                    **ERNMENTS AGAINST UNITED STATES TELE-**  
11                    **COMMUNICATIONS NETWORKS.**

12           Not later than 180 days after the date of the enact-  
13           ment of this Act, the Director of National Intelligence  
14           shall, in coordination with the Director of the Central In-  
15           telligence Agency, the Director of the National Security  
16           Agency, the Director of the Federal Bureau of Investiga-  
17           tion, and the Secretary of Homeland Security, submit to  
18           the congressional intelligence committees a report describ-  
19           ing—

20           (1) any attempts known to the intelligence com-  
21           munity by foreign governments to exploit cybersecu-  
22           rity vulnerabilities in United States telecommuni-  
23           cations networks (including Signaling System No. 7)  
24           to target for surveillance of United States persons,  
25           including employees of the Federal Government; and

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

6 **SEC. 620. REPORTS ON AUTHORITIES OF THE CHIEF INTEL-**  
 7 **LIGENCE OFFICER OF THE DEPARTMENT OF**  
 8 **HOMELAND SECURITY.**

9           (a) DEFINITIONS.—In this section:

10           (1) DEPARTMENT.—The term “Department”  
 11           means the Department of Homeland Security.

12           (2) HOMELAND SECURITY INTELLIGENCE EN-  
 13           TERPRISE.—The term “Homeland Security Intel-  
 14           ligence Enterprise” has the meaning given such  
 15           term in Department of Homeland Security Instruc-  
 16           tion Number 264–01–001, or successor authority.

17           (3) OFFICE.—The term “Office” means the Of-  
 18           fice of Intelligence and Analysis of the Department.

19           (4) SECRETARY.—The term “Secretary” means  
 20           the Secretary of Homeland Security.

21           (5) UNDER SECRETARY.—The term “Under  
 22           Secretary” means the Under Secretary for Intel-  
 23           ligence and Analysis of the Department.

24           (b) REQUIREMENT FOR REPORT.—Not later than  
 25           120 days after the date of the enactment of this Act, the

1 Secretary, in consultation with the Under Secretary, shall  
2 submit to the congressional intelligence committees a re-  
3 port on the authorities of the Under Secretary.

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

6 (1) An analysis of whether the Under Secretary  
7 has the legal and policy authority necessary to orga-  
8 nize and lead the Homeland Security Intelligence  
9 Enterprise, with respect to intelligence, and, if not,  
10 a description of—

11 (A) the obstacles to exercising the authori-  
12 ties of the Chief Intelligence Officer and the  
13 Homeland Security Intelligence Council, over  
14 which the Chief Intelligence Officer chairs; and

15 (B) the legal and policy changes necessary  
16 to effectively coordinate, organize, and lead in-  
17 telligence activities of the Department of Home-  
18 land Security.

19 (2) A description of the actions that the Sec-  
20 retary has taken to address the inability of the  
21 Under Secretary to require components of the De-  
22 partment, other than the Office—

23 (A) to coordinate intelligence programs;  
24 and



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

3 **SEC. 621. REPORT ON GEOSPATIAL COMMERCIAL ACTIVI-**  
4 **TIES FOR BASIC AND APPLIED RESEARCH**  
5 **AND DEVELOPMENT.**

6 (a) SENSE OF CONGRESS.—It is the sense of Con-  
7 gress that—

8 (1) rapid technology change and a significant  
9 increase in data collection by the intelligence com-  
10 munity has outpaced the ability of the intelligence  
11 community to exploit vast quantities of intelligence  
12 data;

13 (2) the data collection capabilities of the intel-  
14 ligence community and the Department of Defense  
15 have outpaced their ability to exploit vast quantities  
16 of data;

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

20 (4) many United States companies have talent  
21 and technological capabilities that the Federal Gov-  
22 ernment could harness; and

23 (5) these companies would be able to more ef-  
24 fectively develop automation, artificial intelligence,  
25 and associated algorithms if given access to data of

1 the National Geospatial-Intelligence Agency, con-  
2 sistent with the protection of sources and methods.

3 (b) REPORT.—Not later than 30 days after the date  
4 of the enactment of this Act, the Director of the National  
5 Geospatial-Intelligence Agency shall submit to the appro-  
6 priate congressional committees a report on the authori-  
7 ties necessary to conduct commercial activities relating to  
8 geospatial intelligence that the Director determines nec-  
9 essary to engage in basic research, applied research, data  
10 transfers, and development projects, with respect to auto-  
11 mation, artificial intelligence, and associated algorithms,  
12 including how the Director would use such authorities,  
13 consistent with applicable laws and procedures relating to  
14 the protection of sources and methods.

15 (c) APPROPRIATE CONGRESSIONAL COMMITTEES DE-  
16 FINED.—In this section, the term “appropriate congres-  
17 sional committees” means—

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

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

1 **SEC. 622. TECHNICAL AMENDMENTS RELATED TO THE DE-**  
2 **PARTMENT OF ENERGY.**

3 (a) NATIONAL NUCLEAR SECURITY ADMINISTRATION  
4 ACT.—

5 (1) CLARIFICATION OF FUNCTIONS OF THE AD-  
6 MINISTRATOR FOR NUCLEAR SECURITY.—Subsection

7 (b) of section 3212 of the National Nuclear Security  
8 Administration Act (50 U.S.C. 2402(b)) is amend-  
9 ed—

10 (A) by striking paragraphs (11) and (12);  
11 and

12 (B) by redesignating paragraphs (13)  
13 through (19) as paragraphs (11) through (17),  
14 respectively.

15 (2) COUNTERINTELLIGENCE PROGRAMS.—Sec-  
16 tion 3233(b) of the National Nuclear Security Ad-  
17 ministration Act (50 U.S.C. 2423(b)) is amended—

18 (A) by striking “Administration” and in-  
19 serting “Department”; and

20 (B) by inserting “Intelligence and” after  
21 “the Office of”.

22 (b) ATOMIC ENERGY DEFENSE ACT.—Section  
23 4524(b)(2) of the Atomic Energy Defense Act (50 U.S.C.  
24 2674(b)(2)) is amended by inserting “Intelligence and”  
25 after “The Director of”.

1       (c) NATIONAL SECURITY ACT OF 1947.—Paragraph  
2 (2) of section 106(b) of the National Security Act of 1947  
3 (50 U.S.C. 3041(b)(2)) is amended—

4           (1) in subparagraph (E), by inserting “and  
5 Counterintelligence” after “Office of Intelligence”;

6           (2) by striking subparagraph (F);

7           (3) by redesignating subparagraphs (G), (H),  
8 and (I) as subparagraphs (F), (G), and (H), respec-  
9 tively; and

10          (4) in subparagraph (I), by realigning the mar-  
11 gin of such subparagraph 2 ems to the left.

12 **SEC. 623. SENSE OF CONGRESS ON WIKILEAKS.**

13       It is the sense of Congress that WikiLeaks and the  
14 senior leadership of WikiLeaks resemble a non-state hos-  
15 tile intelligence service often abetted by state actors and  
16 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