

## Calendar No. 494

115TH CONGRESS  
2D SESSION**S. 3153**

To authorize appropriations for fiscal years 2018 and 2019 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

JUNE 28, 2018

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

---

**A BILL**

To authorize appropriations for fiscal years 2018 and 2019 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

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       “Matthew Young Pollard Intelligence Authorization Act  
6       for Fiscal Years 2018 and 2019”.

- 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 Schedules 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.  
 Sec. 202. Computation of annuities for employees of the Central Intelligence Agency.

#### 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. Modification of appointment of Chief Information Officer of the Intelligence Community.  
 Sec. 305. Director of National Intelligence review of placement of positions within the intelligence community on the Executive Schedule.  
 Sec. 306. Supply Chain and Counterintelligence Risk Management Task Force.  
 Sec. 307. Consideration of adversarial telecommunications and cybersecurity infrastructure when sharing intelligence with foreign governments and entities.  
 Sec. 308. Cyber protection support for the personnel of the intelligence community in positions highly vulnerable to cyber attack.  
 Sec. 309. Modification of authority relating to management of supply-chain risk.  
 Sec. 310. Limitations on determinations regarding certain security classifications.

#### TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

##### Subtitle A—Office of the Director of National Intelligence

Sec. 401. Authority for protection of current and former employees of the Office of the Director of National Intelligence.  
 Sec. 402. Designation of the program manager-information sharing environment.  
 Sec. 403. Modification to the executive schedule.

##### Subtitle B—Other Elements

- Sec. 411. Repeal of foreign language proficiency requirement for certain senior level positions in the Central Intelligence Agency.
- Sec. 412. Plan for designation of counterintelligence component of Defense Security Service as an element of intelligence community.
- Sec. 413. Notice not required for private entities.

#### TITLE V—ELECTION MATTERS

- Sec. 501. Report on cyber attacks by foreign governments against United States election infrastructure.
- Sec. 502. Review of intelligence community's posture to collect against and analyze Russian efforts to influence the Presidential election.
- Sec. 503. Assessment of foreign intelligence threats to Federal elections.
- Sec. 504. Strategy for countering Russian cyber threats to United States elections.
- Sec. 505. Information sharing with State election officials.
- Sec. 506. Designation of counterintelligence officer to lead election security matters.

#### TITLE VI—SECURITY CLEARANCES

- Sec. 601. Definitions.
- Sec. 602. Reports and plans relating to security clearances and background investigations.
- Sec. 603. Improving the process for security clearances.
- Sec. 604. Goals for promptness of determinations regarding security clearances.
- Sec. 605. Security Executive Agent.
- Sec. 606. Report on unified, simplified, governmentwide standards for positions of trust and security clearances.
- Sec. 607. Report on clearance in person concept.
- Sec. 608. Budget request documentation on funding for clearances.
- Sec. 609. Reports on reciprocity for security clearances inside of departments and agencies.
- Sec. 610. Intelligence community reports on security clearances.
- Sec. 611. Periodic report on positions in the intelligence community which can be conducted without access to classified information, networks, or facilities.
- Sec. 612. Information sharing program for positions of trust.
- Sec. 613. Report on protections for confidentiality of whistleblower-related communications.

#### TITLE VII—REPORTS AND OTHER MATTERS

##### Subtitle A—Matters Relating to Russia and Other Foreign Powers

- Sec. 701. Limitation relating to establishment or support of cybersecurity unit with the Government of Russia.
- Sec. 702. Report on returning Russian compounds.
- Sec. 703. Assessment of threat finance relating to Russia.
- Sec. 704. Notification of an active measures campaign.
- Sec. 705. Notification of travel by accredited diplomatic and consular personnel of the Russian Federation in the United States.

##### Subtitle B—Reports

- Sec. 711. Technical correction to Inspector General study.

- Sec. 712. Reports on authorities of the Chief Intelligence Officer of the Department of Homeland Security.
- Sec. 713. Report on cyber exchange program.
- Sec. 714. Report on role of Director of National Intelligence with respect to certain foreign investments.
- Sec. 715. Report on surveillance by foreign governments against United States telecommunications networks.
- Sec. 716. Biennial report on foreign investment risks.
- Sec. 717. Modification of certain reporting requirement on travel of foreign diplomats.
- Sec. 718. Semiannual reports on investigations of unauthorized disclosures of classified information.
- Sec. 719. Congressional notification of designation of covered intelligence officer as persona non grata.
- Sec. 720. Inspectors General reports on classification.
- Sec. 721. Reports on intelligence community participation in vulnerabilities equities process of Federal Government.
- Sec. 722. Reports on global water insecurity and national security implications.
- Sec. 723. Annual report on memoranda of understanding between elements of intelligence community and other entities of the United States Government regarding significant operational activities or policy.
- Sec. 724. Repeal of report requirement for inspectors general of certain elements of intelligence community.
- Sec. 725. Repeal of requirement for annual personnel level assessments for the intelligence community.
- Sec. 726. Report on outreach strategy addressing threats from United States adversaries to the United States technology sector.
- Sec. 727. Study on the feasibility of encrypting unclassified wireline and wireless telephone calls.
- Sec. 728. Modification of requirement for annual report on hiring and retention of minority employees.

#### Subtitle C—Other Matters

- Sec. 731. Technical amendments related to the Department of Energy.
- Sec. 732. Securing energy infrastructure.
- Sec. 733. Sense of Congress on WikiLeaks.
- Sec. 734. Bug bounty programs.
- Sec. 735. Sense of Congress on consideration of espionage activities when considering whether or not to provide visas to foreign individuals to be accredited to a United Nations mission in the United States.
- Sec. 736. Public Interest Declassification Board.
- Sec. 737. Modification of authorities relating to the National Intelligence University.

## 1 **SEC. 2. DEFINITIONS.**

2       In this Act:

3               (1) CONGRESSIONAL INTELLIGENCE COMMIT-

4       TEES.—The term “congressional intelligence com-

1       mittees” has the meaning given such term in section  
 2       3 of the National Security Act of 1947 (50 U.S.C.  
 3       3003).

4               (2) INTELLIGENCE COMMUNITY.—The term  
 5       “intelligence community” has the meaning given  
 6       such term in such section.

## 7               **TITLE I—INTELLIGENCE** 8               **ACTIVITIES**

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

10       (a) IN GENERAL.—Funds are hereby authorized to  
 11       be appropriated for fiscal years 2018 and 2019 for the  
 12       conduct of the intelligence and intelligence-related activi-  
 13       ties of the following elements of the United States Govern-  
 14       ment:

15               (1) The Office of the Director of National Intel-  
 16       ligence.

17               (2) The Central Intelligence Agency.

18               (3) The Department of Defense.

19               (4) The Defense Intelligence Agency.

20               (5) The National Security Agency.

21               (6) The Department of the Army, the Depart-  
 22       ment of the Navy, and the Department of the Air  
 23       Force.

24               (7) The Coast Guard.

25               (8) The Department of State.

1 (9) The Department of the Treasury.

2 (10) The Department of Energy.

3 (11) The Department of Justice.

4 (12) The Federal Bureau of Investigation.

5 (13) The Drug Enforcement Administration.

6 (14) The National Reconnaissance Office.

7 (15) The National Geospatial-Intelligence Agen-  
8 cy.

9 (16) The Department of Homeland Security.

10 (b) CERTAIN SPECIFIC AUTHORIZATION.—Funds ap-  
11 propriated by the Department of Defense Missile Defeat  
12 and Defense Enhancements Appropriations Act, 2018 (di-  
13 vision B of Public Law 115–96) for intelligence or intel-  
14 ligence-related activities are specifically authorized by  
15 Congress for purposes of section 504 of the National Secu-  
16 rity Act of 1947 (50 U.S.C. 3094), as specified in the clas-  
17 sified Schedule of Authorizations pursuant to section 102,  
18 and are subject to such section 504.

19 (c) LIMITATION ON CERTAIN WAIVERS FROM LIM-  
20 ITATIONS ON FUNDING OF INTELLIGENCE ACTIVITIES.—

21 (1) WAIVERS FOR COVERT ACTIONS.—Section  
22 504 of the National Security Act of 1947 (50 U.S.C.  
23 3094) is amended—

24 (A) by redesignating subsection (e) as sub-  
25 section (f); and

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

3 “(e) This section cannot be waived for any covert ac-  
 4 tion (as defined in section 503(e)) unless and until the  
 5 Director of National Intelligence notifies the congressional  
 6 intelligence committees that the action is urgent for na-  
 7 tional security purposes.”.

8 (2) WAIVERS FOR MAJOR SYSTEMS ACQUISI-  
 9 TIONS.—Such section, as amended by paragraph (1),  
 10 is further amended—

11 (A) by redesignating subsection (f) as sub-  
 12 section (g); and

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

15 “(f) This section cannot be waived for any major sys-  
 16 tem (as defined in section 506A(e)) acquisition unless and  
 17 until the Director of National Intelligence notifies the con-  
 18 gressional intelligence committees that the action is urgent  
 19 for national security purposes.”.

20 **SEC. 102. CLASSIFIED SCHEDULES OF AUTHORIZATIONS.**

21 (a) SPECIFICATIONS OF AMOUNTS AND PERSONNEL  
 22 LEVELS.—

23 (1) FISCAL YEAR 2018.—The amounts author-  
 24 ized to be appropriated under section 101 and, sub-  
 25 ject to section 103, the authorized personnel ceilings

1 as of September 30, 2018, for the conduct of the in-  
2 telligence activities of the elements listed in para-  
3 graphs (1) through (16) of section 101, are those  
4 specified in the classified Schedule of Authorizations  
5 for fiscal year 2018 prepared to accompany this Act.

6 (2) FISCAL YEAR 2019.—The amounts author-  
7 ized to be appropriated under section 101 and, sub-  
8 ject to section 103, the authorized personnel ceilings  
9 as of September 30, 2019, for the conduct of the in-  
10 telligence activities of the elements listed in para-  
11 graphs (1) through (16) of section 101, are those  
12 specified in the classified Schedule of Authorizations  
13 for fiscal year 2019 prepared to accompany this Act.

14 (b) AVAILABILITY OF CLASSIFIED SCHEDULES OF  
15 AUTHORIZATIONS.—

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

21 (2) DISTRIBUTION BY THE PRESIDENT.—Sub-  
22 ject to paragraph (3), the President shall provide for  
23 suitable distribution of the classified Schedules of  
24 Authorizations referred to in subsection (a), or of



1 appropriate portions of such Schedule, within the ex-  
2 ecutive branch.

3 (3) LIMITS ON DISCLOSURE.—The President  
4 shall not publicly disclose the classified Schedules of  
5 Authorizations or any portion of such Schedule ex-  
6 cept—

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

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

12 (C) as otherwise required by law.

13 **SEC. 103. PERSONNEL CEILING ADJUSTMENTS.**

14 (a) AUTHORITY FOR INCREASES.—The Director of  
15 National Intelligence may authorize employment of civil-  
16 ian personnel in excess of the number authorized for fiscal  
17 year 2018 by the classified Schedules of Authorizations  
18 referred to in section 102(a) if the Director of National  
19 Intelligence determines that such action is necessary to  
20 the performance of important intelligence functions, ex-  
21 cept that the number of personnel employed in excess of  
22 the number authorized under such section may not, for  
23 any element of the intelligence community, exceed—

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

4           (2) 10 percent of the number of civilian per-  
5           sonnel authorized under such schedule for such ele-  
6           ment for the purposes of converting the performance  
7           of any function by contractors to performance by ci-  
8           vilian personnel.

9           (b) TREATMENT OF CERTAIN PERSONNEL.—The Di-  
10          rector of National Intelligence shall establish guidelines  
11          that govern, for each element of the intelligence commu-  
12          nity, the treatment under the personnel levels authorized  
13          under section 102(a), including any exemption from such  
14          personnel levels, of employment or assignment in—

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

17               (2) a reserve corps or as a reemployed annu-  
18               itant; or

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

21          (c) NOTICE TO CONGRESSIONAL INTELLIGENCE  
22          COMMITTEES.—Not later than 15 days prior to the exer-  
23          cise of an authority described in subsection (a), the Direc-  
24          tor of National Intelligence shall submit to the congres-  
25          sional intelligence committees—

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

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

7 **SEC. 104. INTELLIGENCE COMMUNITY MANAGEMENT AC-**  
 8 **COUNT.**

9 (a) AUTHORIZATION OF APPROPRIATIONS.—

10 (1) FISCAL YEAR 2018.—There is authorized to  
 11 be appropriated for the Intelligence Community  
 12 Management Account of the Director of National In-  
 13 telligence for fiscal year 2018 the sum of  
 14 \$546,900,000. Within such amount, funds identified  
 15 in the classified Schedule of Authorizations referred  
 16 to in section 102(a) for advanced research and de-  
 17 velopment shall remain available until September 30,  
 18 2019.

19 (2) FISCAL YEAR 2019.—There is authorized to  
 20 be appropriated for the Intelligence Community  
 21 Management Account of the Director of National In-  
 22 telligence for fiscal year 2019 the sum of  
 23 \$539,624,000. Within such amount, funds identified  
 24 in the classified Schedule of Authorizations referred  
 25 to in section 102(a) for advanced research and de-

1        velopment shall remain available until September 30,  
2        2020.

3        (b) AUTHORIZED PERSONNEL LEVELS.—The ele-  
4        ments within the Intelligence Community Management  
5        Account of the Director of National Intelligence are au-  
6        thorized 797 positions as of September 30, 2018. Per-  
7        sonnel serving in such elements may be permanent em-  
8        ployees of the Office of the Director of National Intel-  
9        ligence or personnel detailed from other elements of the  
10      United States Government.

11      (c) CLASSIFIED AUTHORIZATIONS.—

12            (1) AUTHORIZATION OF APPROPRIATIONS.—

13            (A) FISCAL YEAR 2018.—In addition to  
14            amounts authorized to be appropriated for the  
15            Intelligence Community Management Account  
16            by subsection (a), there are authorized to be ap-  
17            propriated for the Intelligence Community Man-  
18            agement Account for fiscal year 2018 such ad-  
19            ditional amounts as are specified in the classi-  
20            fied Schedule of Authorizations referred to in  
21            section 102(a). Such additional amounts made  
22            available for advanced research and develop-  
23            ment shall remain available until September 30,  
24            2019.

1           (B) FISCAL YEAR 2019.—In addition to  
2           amounts authorized to be appropriated for the  
3           Intelligence Community Management Account  
4           by subsection (a), there are authorized to be ap-  
5           propriated for the Intelligence Community Man-  
6           agement Account for fiscal year 2019 such ad-  
7           ditional amounts as are specified in the classi-  
8           fied Schedule of Authorizations referred to in  
9           section 102(a). Such additional amounts made  
10          available for advanced research and develop-  
11          ment shall remain available until September 30,  
12          2020.

13          (2) AUTHORIZATION OF PERSONNEL.—In addi-  
14          tion to the personnel authorized by subsection (b)  
15          for elements of the Intelligence Community Manage-  
16          ment Account as of September 30, 2018, there are  
17          authorized such additional personnel for the Com-  
18          munity Management Account as of that date as are  
19          specified in the classified Schedule of Authorizations  
20          referred to in section 102(a).

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

5 **SEC. 201. AUTHORIZATION OF APPROPRIATIONS.**

6 There is authorized to be appropriated for the Cen-  
 7 tral Intelligence Agency Retirement and Disability Fund  
 8 \$514,000,000 for each of fiscal years 2018 and 2019.

9 **SEC. 202. COMPUTATION OF ANNUITIES FOR EMPLOYEES**  
 10 **OF THE CENTRAL INTELLIGENCE AGENCY.**

11 (a) COMPUTATION OF ANNUITIES.—

12 (1) IN GENERAL.—Section 221 of the Central  
 13 Intelligence Agency Retirement Act (50 U.S.C.  
 14 2031) is amended—

15 (A) in subsection (a)(3)(B), by striking the  
 16 period at the end and inserting “, as deter-  
 17 mined by using the annual rate of basic pay  
 18 that would be payable for full-time service in  
 19 that position.”;

20 (B) in subsection (b)(1)(C)(i), by striking  
 21 “12-month” and inserting “2-year”;

22 (C) in subsection (f)(2), by striking “one  
 23 year” and inserting “two years”;

1 (D) in subsection (g)(2), by striking “one  
 2 year” each place such term appears and insert-  
 3 ing “two years”;

4 (E) by redesignating subsections (h), (i),  
 5 (j), (k), and (l) as subsections (i), (j), (k), (l),  
 6 and (m), respectively; and

7 (F) by inserting after subsection (g) the  
 8 following:

9 “(h) CONDITIONAL ELECTION OF INSURABLE INTER-  
 10 EST SURVIVOR ANNUITY BY PARTICIPANTS MARRIED AT  
 11 THE TIME OF RETIREMENT.—

12 “(1) AUTHORITY TO MAKE DESIGNATION.—  
 13 Subject to the rights of former spouses under sub-  
 14 section (b) and section 222, at the time of retire-  
 15 ment a married participant found by the Director to  
 16 be in good health may elect to receive an annuity re-  
 17 duced in accordance with subsection (f)(1)(B) and  
 18 designate in writing an individual having an insur-  
 19 able interest in the participant to receive an annuity  
 20 under the system after the participant’s death, ex-  
 21 cept that any such election to provide an insurable  
 22 interest survivor annuity to the participant’s spouse  
 23 shall only be effective if the participant’s spouse  
 24 waives the spousal right to a survivor annuity under

1       this Act. The amount of the annuity shall be equal  
2       to 55 percent of the participant's reduced annuity.

3               “(2) REDUCTION IN PARTICIPANT’S ANNUITY.—

4       The annuity payable to the participant making such  
5       election shall be reduced by 10 percent of an annuity  
6       computed under subsection (a) and by an additional  
7       5 percent for each full 5 years the designated indi-  
8       vidual is younger than the participant. The total re-  
9       duction under this subparagraph may not exceed 40  
10      percent.

11              “(3) COMMENCEMENT OF SURVIVOR ANNU-

12      ITY.—The annuity payable to the designated indi-  
13      vidual shall begin on the day after the day that the  
14      retired participant dies and terminate on the last  
15      day of the month before the designated individual  
16      dies.

17              “(4) RECOMPUTATION OF PARTICIPANT’S AN-

18      NUITY ON DEATH OF DESIGNATED INDIVIDUAL.—An  
19      annuity that is reduced under this subsection shall,  
20      effective the first day of the month following the  
21      death of the designated individual, be recomputed  
22      and paid as if the annuity had not been so re-  
23      duced.”.

24              (2) CONFORMING AMENDMENTS.—



1 (A) CENTRAL INTELLIGENCE AGENCY RE-  
 2 TIREMENT ACT.—The Central Intelligence  
 3 Agency Retirement Act (50 U.S.C. 2001 et  
 4 seq.) is amended—

5 (i) in section 232(b)(1) (50 U.S.C.  
 6 2052(b)(1)), by striking “221(h),” and in-  
 7 serting “221(i),”; and

8 (ii) in section 252(h)(4) (50 U.S.C.  
 9 2082(h)(4)), by striking “221(k)” and in-  
 10 serting “221(l)”.

11 (B) CENTRAL INTELLIGENCE AGENCY ACT  
 12 OF 1949.—Subsection (a) of section 14 of the  
 13 Central Intelligence Agency Act of 1949 (50  
 14 U.S.C. 3514(a)) is amended by striking  
 15 “221(h)(2), 221(i), 221(l),” and inserting  
 16 “221(i)(2), 221(j), 221(m),”.

17 (b) ANNUITIES FOR FORMER SPOUSES.—Subpara-  
 18 graph (B) of section 222(b)(5) of the Central Intelligence  
 19 Agency Retirement Act (50 U.S.C. 2032(b)(5)(B)) is  
 20 amended by striking “one year” and inserting “two  
 21 years”.

22 (c) PRIOR SERVICE CREDIT.—Subparagraph (A) of  
 23 section 252(b)(3) of the Central Intelligence Agency Re-  
 24 tirement Act (50 U.S.C. 2082(b)(3)(A)) is amended by

1 striking “October 1, 1990” both places that term appears  
 2 and inserting “March 31, 1991”.

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

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

8 (2) by inserting after subsection (a) the fol-  
 9 lowing:

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

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

19 **TITLE III—GENERAL INTEL-**  
 20 **LIGENCE COMMUNITY MAT-**  
 21 **TERS**

22 **SEC. 301. RESTRICTION ON CONDUCT OF INTELLIGENCE**  
 23 **ACTIVITIES.**

24 The authorization of appropriations by this Act shall  
 25 not be deemed to constitute authority for the conduct of

1 any intelligence activity that is not otherwise authorized  
 2 by the Constitution or the laws of the United States.

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

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

10 **SEC. 303. MODIFICATION OF SPECIAL PAY AUTHORITY FOR**  
 11 **SCIENCE, TECHNOLOGY, ENGINEERING, OR**  
 12 **MATHEMATICS POSITIONS AND ADDITION OF**  
 13 **SPECIAL PAY AUTHORITY FOR CYBER POSI-**  
 14 **TIONS.**

15 Section 113B of the National Security Act of 1947  
 16 (50 U.S.C. 3049a) is amended—

17 (1) by amending subsection (a) to read as fol-  
 18 lows:

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

22 “(1) IN GENERAL.—Notwithstanding part III  
 23 of title 5, United States Code, the head of each ele-  
 24 ment of the intelligence community may, for 1 or  
 25 more categories of positions in such element that re-

1       quire expertise in science, technology, engineering,  
2       or mathematics—

3               “(A) establish higher minimum rates of  
4       pay; and

5               “(B) make corresponding increases in all  
6       rates of pay of the pay range for each grade or  
7       level, subject to subsection (b) or (c), as appli-  
8       cable.

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

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

16              (3) by inserting after subsection (a) the fol-  
17      lowing:

18              “(b) SPECIAL RATES OF PAY FOR CYBER POSI-  
19      TIONS.—

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

23              “(A) not to exceed the rate of basic pay  
24              payable for level II of the Executive Schedule  
25              under section 5313 of title 5, United States

1 Code, if the Director certifies to the Under Sec-  
2 retary of Defense for Intelligence, in consulta-  
3 tion with the Under Secretary of Defense for  
4 Personnel and Readiness, that the rate of pay  
5 is for positions that perform functions that exe-  
6 cute the cyber mission of the Agency; or

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

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

20 “(A) any allowance, differential, bonus,  
21 award, or other similar cash payment in addi-  
22 tion to basic pay that is authorized under title  
23 10, United States Code (or any other applicable  
24 law in addition to title 5 of such Code, exclud-  
25 ing the Fair Labor Standards Act of 1938 (29

1 U.S.C. 201 et seq.)) shall also be counted as  
 2 part of aggregate compensation; and

3 “(B) aggregate compensation may not ex-  
 4 ceed the rate established for the Vice President  
 5 of the United States under section 104 of title  
 6 3, United States Code.

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

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

20 (4) in subsection (c), as redesignated by para-  
 21 graph (2), by striking “A minimum” and inserting  
 22 “Except as provided in subsection (b), a minimum”;

23 (5) in subsection (d), as redesignated by para-  
 24 graph (2), by inserting “or (b)” after “by subsection  
 25 (a)”; and

1 (6) in subsection (g), as redesignated by para-  
 2 graph (2)—

3 (A) in paragraph (1), by striking “Not  
 4 later than 90 days after the date of the enact-  
 5 ment of the Intelligence Authorization Act for  
 6 Fiscal Year 2017” and inserting “Not later  
 7 than 90 days after the date of the enactment of  
 8 the Matthew Young Pollard Intelligence Au-  
 9 thorization Act for Fiscal Years 2018 and  
 10 2019”; and

11 (B) in paragraph (2)(A), by inserting “or  
 12 (b)” after “subsection (a)”.

13 **SEC. 304. MODIFICATION OF APPOINTMENT OF CHIEF IN-**  
 14 **FORMATION OFFICER OF THE INTELLIGENCE**  
 15 **COMMUNITY.**

16 Section 103G(a) of the National Security Act of 1947  
 17 (50 U.S.C. 3032(a)) is amended by striking “President”  
 18 and inserting “Director”.

19 **SEC. 305. DIRECTOR OF NATIONAL INTELLIGENCE REVIEW**  
 20 **OF PLACEMENT OF POSITIONS WITHIN THE**  
 21 **INTELLIGENCE COMMUNITY ON THE EXECU-**  
 22 **TIVE SCHEDULE.**

23 (a) REVIEW.—The Director of National Intelligence,  
 24 in coordination with the Director of the Office of Per-  
 25 sonnel Management, shall conduct a review of positions

1 within the intelligence community regarding the placement  
2 of such positions on the Executive Schedule under sub-  
3 chapter II of chapter 53 of title 5, United States Code.  
4 In carrying out such review, the Director of National In-  
5 telligence, in coordination with the Director of the Office  
6 of Personnel Management, shall determine—

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

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

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

14      (b) REPORT.—Not later than 60 days after the date  
15 on which the review under subsection (a) is completed, the  
16 Director of National Intelligence shall submit to the con-  
17 gressional intelligence committees, the Committee on  
18 Homeland Security and Governmental Affairs of the Sen-  
19 ate, and the Committee on Oversight and Government Re-  
20 form of the House of Representatives an unredacted re-  
21 port describing the standards by which the review was con-  
22 ducted and the outcome of the review.



1 **SEC. 306. SUPPLY CHAIN AND COUNTERINTELLIGENCE**  
2 **RISK MANAGEMENT TASK FORCE.**

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

10 (b) MEMBERS.—The Supply Chain and Counterintel-  
11 ligence Risk Management Task Force established under  
12 subsection (a) shall be composed of—

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

15 (2) a representative of the General Services Ad-  
16 ministration;

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

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

22 (5) the Director of the National Counterintel-  
23 ligence and Security Center; and

24 (6) such other members as the Director of Na-  
25 tional Intelligence determines appropriate.

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

6       (d) ANNUAL REPORT.—

7           (1) IN GENERAL.—Not less frequently than  
8 once each year, the Supply Chain and Counterintel-  
9 ligence Risk Management Task Force established  
10 under subsection (a) shall submit to the appropriate  
11 congressional committees a report that describes the  
12 activities of the Task Force during the previous  
13 year, including identification of the supply chain and  
14 counterintelligence risks shared with the acquisition  
15 community of the United States Government by the  
16 intelligence community.

17           (2) APPROPRIATE CONGRESSIONAL COMMIT-  
18 TEES DEFINED.—In this subsection, the term “ap-  
19 propriate congressional committees” means the fol-  
20 lowing:

21           (A) The congressional intelligence commit-  
22 tees.

23           (B) The Committee on Armed Services and  
24 the Committee on Homeland Security and Gov-  
25 ernmental Affairs of the Senate.

1 (C) The Committee on Armed Services, the  
2 Committee on Homeland Security, and the  
3 Committee on Oversight and Government Re-  
4 form of the House of Representatives.

5 **SEC. 307. CONSIDERATION OF ADVERSARIAL TELE-**  
6 **COMMUNICATIONS AND CYBERSECURITY IN-**  
7 **FRASTRUCTURE WHEN SHARING INTEL-**  
8 **LIGENCE WITH FOREIGN GOVERNMENTS AND**  
9 **ENTITIES.**

10 Whenever the head of an element of the intelligence  
11 community enters into an intelligence sharing agreement  
12 with a foreign government or any other foreign entity, the  
13 head of the element shall consider the pervasiveness of  
14 telecommunications and cybersecurity infrastructure,  
15 equipment, and services provided by adversaries of the  
16 United States, particularly China and Russia, or entities  
17 of such adversaries in the country or region of the foreign  
18 government or other foreign entity entering into the agree-  
19 ment.

20 **SEC. 308. CYBER PROTECTION SUPPORT FOR THE PER-**  
21 **SONNEL OF THE INTELLIGENCE COMMUNITY**  
22 **IN POSITIONS HIGHLY VULNERABLE TO**  
23 **CYBER ATTACK.**

24 (a) DEFINITIONS.—In this section:

1           (1) PERSONAL ACCOUNTS.—The term “personal  
2       accounts” means accounts for online and tele-  
3       communications services, including telephone, resi-  
4       dential Internet access, email, text and multimedia  
5       messaging, cloud computing, social media, health  
6       care, and financial services, used by personnel of the  
7       intelligence community outside of the scope of their  
8       employment with elements of the intelligence com-  
9       munity.

10          (2) PERSONAL TECHNOLOGY DEVICES.—The  
11       term “personal technology devices” means tech-  
12       nology devices used by personnel of the intelligence  
13       community outside of the scope of their employment  
14       with elements of the intelligence community, includ-  
15       ing networks to which such devices connect.

16       (b) AUTHORITY TO PROVIDE CYBER PROTECTION  
17       SUPPORT.—

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

23           (2) AT-RISK PERSONNEL.—The personnel de-  
24       scribed in this paragraph are personnel of the intel-  
25       ligence community—

1           (A) who the Director determines to be  
2           highly vulnerable to cyber attacks and hostile  
3           information collection activities because of the  
4           positions occupied by such personnel in the in-  
5           telligence community; and

6           (B) whose personal technology devices or  
7           personal accounts are highly vulnerable to cyber  
8           attacks and hostile information collection activi-  
9           ties.

10       (c) NATURE OF CYBER PROTECTION SUPPORT.—

11   Subject to the availability of resources, the cyber protec-  
12   tion support provided to personnel under subsection (a)  
13   may include training, advice, assistance, and other services  
14   relating to cyber attacks and hostile information collection  
15   activities.

16       (d) LIMITATION ON SUPPORT.—Nothing in this sec-  
17   tion shall be construed—

18           (1) to encourage personnel of the intelligence  
19           community to use personal technology devices for of-  
20           ficial business; or

21           (2) to authorize cyber protection support for  
22           senior intelligence community personnel using per-  
23           sonal devices, networks, and personal accounts in an  
24           official capacity.

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

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

8 (2) guidance for the use of cyber protection  
 9 support and tracking of support requests for per-  
 10 sonnel receiving cyber protection support under sub-  
 11 section (a).

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

14 (a) MODIFICATION OF EFFECTIVE DATE.—Sub-  
 15 section (f) of section 309 of the Intelligence Authorization  
 16 Act for Fiscal Year 2012 (Public Law 112-87; 50 U.S.C.  
 17 3329 note) is amended by striking “the date that is 180  
 18 days after”.

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

22 (c) REPORTS.—Such section is amended—

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

1           (2) by inserting after subsection (e) the fol-  
 2       lowing:

3       “(f) ANNUAL REPORTS.—

4           “(1) IN GENERAL.—Except as provided in para-  
 5       graph (2), not later than 180 days after the date of  
 6       the enactment of the Matthew Young Pollard Intel-  
 7       ligence Authorization Act for Fiscal Years 2018 and  
 8       2019 and not less frequently than once each cal-  
 9       endar year thereafter, the Director of National Intel-  
 10      ligence shall, in consultation with each head of a  
 11      covered agency, submit to the congressional intel-  
 12      ligence committees (as defined in section 3 of the  
 13      National Security Act of 1947 (50 U.S.C. 3003)), a  
 14      report that details the determinations and notifica-  
 15      tions made under subsection (c) during the most re-  
 16      cently completed calendar year.

17           “(2) INITIAL REPORT.—The first report sub-  
 18      mitted under paragraph (1) shall detail all the deter-  
 19      minations and notifications made under subsection  
 20      (c) before the date of the submittal of the report.”.

21   **SEC. 310. LIMITATIONS ON DETERMINATIONS REGARDING**  
 22                           **CERTAIN SECURITY CLASSIFICATIONS.**

23           (a) PROHIBITION.—An officer of an element of the  
 24      intelligence community who has been nominated by the  
 25      President for a position that requires the advice and con-

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

3 (b) CLASSIFICATION DETERMINATIONS.—

4 (1) IN GENERAL.—Except as provided in para-  
5 graph (2), in a case in which an officer described in  
6 subsection (a) has been nominated as described in  
7 such subsection and classification authority rests  
8 with the officer or another officer who reports di-  
9 rectly to such officer, a classification decision with  
10 respect to information relating to the officer shall be  
11 made by the Director of National Intelligence.

12 (2) NOMINATIONS OF DIRECTOR OF NATIONAL  
13 INTELLIGENCE.—In a case described in paragraph  
14 (1) in which the officer nominated is the Director of  
15 National Intelligence, the classification decision shall  
16 be made by the Principal Deputy Director of Na-  
17 tional Intelligence.

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



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 PROTECTION OF CURRENT AND**  
 7 **FORMER EMPLOYEES OF THE OFFICE OF THE**  
 8 **DIRECTOR OF NATIONAL INTELLIGENCE.**

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

17 **SEC. 402. DESIGNATION OF THE PROGRAM MANAGER-IN-**  
 18 **FORMATION SHARING ENVIRONMENT.**

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

22 (1) in paragraph (1), by striking “President”  
 23 and inserting “Director of National Intelligence”;  
 24 and

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

4       (b) PROGRAM MANAGER.—Section 1016(f)(1) of the  
5       Intelligence Reform and Terrorism Prevention Act of  
6       2004 (6 U.S.C. 485(f)(1)) is amended by striking “The  
7       individual designated as the program manager shall serve  
8       as program manager until removed from service or re-  
9       placed by the President (at the President’s sole discre-  
10      tion).” and inserting “Beginning on the date of the enact-  
11      ment of the Matthew Young Pollard Intelligence Author-  
12      ization Act for Fiscal Years 2018 and 2019, each indi-  
13      vidual designated as the program manager shall be ap-  
14      pointed by the Director of National Intelligence.”.

15   **SEC. 403. MODIFICATION TO THE EXECUTIVE SCHEDULE.**

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

18       “Director of the National Counterintelligence and Se-  
19      curity Center.”.

1           **Subtitle B—Other Elements**

2   **SEC. 411. REPEAL OF FOREIGN LANGUAGE PROFICIENCY**  
3                   **REQUIREMENT FOR CERTAIN SENIOR LEVEL**  
4                   **POSITIONS IN THE CENTRAL INTELLIGENCE**  
5                   **AGENCY.**

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

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

14   **SEC. 412. PLAN FOR DESIGNATION OF COUNTERINTEL-**  
15                   **LIGENCE COMPONENT OF DEFENSE SECU-**  
16                   **RITY SERVICE AS AN ELEMENT OF INTEL-**  
17                   **LIGENCE COMMUNITY.**

18          Not later than 90 days after the date of the enact-  
19 ment of this Act, the Director of National Intelligence and  
20 Under Secretary of Defense for Intelligence, in coordina-  
21 tion with the Director of the National Counterintelligence  
22 and Security Center, shall submit to the congressional in-  
23 telligence committees, the Committee on Armed Services  
24 of the Senate, and the Committee on Armed Services of  
25 the House of Representatives a plan to designate the coun-

1 terintelligence component of the Defense Security Service  
2 of the Department of Defense as an element of the intel-  
3 ligence community by not later than January 1, 2020.

4 Such plan shall—

5           (1) address the implications of such designation  
6           on the authorities, governance, personnel, resources,  
7           information technology, collection, analytic products,  
8           information sharing, and business processes of the  
9           Defense Security Service and the intelligence com-  
10          munity; and

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

13 **SEC. 413. NOTICE NOT REQUIRED FOR PRIVATE ENTITIES.**

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

16           (1) by redesignating subsection (j) as sub-  
17          section (k); and

18           (2) by inserting after subsection (i) the fol-  
19          lowing:

20          “(j) **RULE OF CONSTRUCTION.**—Nothing in this sec-  
21          tion shall be construed to require the Secretary to provide  
22          notice to any private entity before the Secretary issues a  
23          binding operational directive under subsection (b)(2).”.

# 1     **TITLE V—ELECTION MATTERS**

## 2     **SEC. 501. REPORT ON CYBER ATTACKS BY FOREIGN GOV-** 3                   **ERNMENTS AGAINST UNITED STATES ELEC-** 4                   **TION INFRASTRUCTURE.**

5           (a) DEFINITIONS.—In this section:

6                 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
7           TEES.—The term “appropriate congressional com-  
8           mittees” means—

9                         (A) the congressional intelligence commit-  
10           tees;

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

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

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

17                         (A) The majority leader of the Senate.

18                         (B) The minority leader of the Senate.

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

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

23                 (3) STATE.—The term “State” means any  
24           State of the United States, the District of Columbia,

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

3 (b) REPORT REQUIRED.—Not later than 60 days  
4 after the date of the enactment of this Act, the Under  
5 Secretary of Homeland Security for Intelligence and Anal-  
6 ysis shall submit to congressional leadership and the ap-  
7 propriate congressional committees a report on cyber at-  
8 tacks and attempted cyber attacks by foreign governments  
9 on United States election infrastructure in States and lo-  
10 calities in connection with the Presidential election in the  
11 United States and such cyber attacks (or attempted cyber  
12 attacks) as the Under Secretary anticipates against such  
13 infrastructure. Such report shall identify the States and  
14 localities affected and shall include cyber attacks and at-  
15 tempted cyber attacks against voter registration data-  
16 bases, voting machines, voting-related computer networks,  
17 and the networks of Secretaries of State and other election  
18 officials of the various States.

19 (c) FORM.—The report submitted under subsection  
20 (b) shall be submitted in unclassified form, but may in-  
21 clude a classified annex.

1 **SEC. 502. REVIEW OF INTELLIGENCE COMMUNITY'S POS-**  
2 **TURE TO COLLECT AGAINST AND ANALYZE**  
3 **RUSSIAN EFFORTS TO INFLUENCE THE PRES-**  
4 **IDENTIAL ELECTION.**

5 (a) REVIEW REQUIRED.—Not later than 1 year after  
6 the date of the enactment of this Act, the Director of Na-  
7 tional Intelligence shall—

8 (1) complete an after action review of the pos-  
9 ture of the intelligence community to collect against  
10 and analyze efforts of the Government of Russia to  
11 interfere in the 2016 Presidential election in the  
12 United States; and

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

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

20 (1) An assessment of whether the resources of  
21 the intelligence community were properly aligned to  
22 detect and respond to the efforts described in sub-  
23 section (a)(1).

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

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

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

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

9           (6) A review of the use of alternative and pre-  
10          dictive analysis.

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

14      **SEC. 503. ASSESSMENT OF FOREIGN INTELLIGENCE**  
15                              **THREATS TO FEDERAL ELECTIONS.**

16          (a) DEFINITIONS.—In this section:

17               (1) APPROPRIATE CONGRESSIONAL COMMIT-  
18               TEES.—The term “appropriate congressional com-  
19               mittees” means—

20                       (A) the congressional intelligence commit-  
21                       tees;

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

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



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

3                   (A) The majority leader of the Senate.

4                   (B) The minority leader of the Senate.

5                   (C) The Speaker of the House of Rep-  
6           resentatives.

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

9           (3) SECURITY VULNERABILITY.—The term “se-  
10          curity vulnerability” has the meaning given such  
11          term in section 102 of the Cybersecurity Information  
12          Sharing Act of 2015 (6 U.S.C. 1501).

13          (b) ASSESSMENT AND REPORT.—The Director of Na-  
14          tional Intelligence, in coordination with the Director of the  
15          Central Intelligence Agency, the Director of the National  
16          Security Agency, the Director of the Federal Bureau of  
17          Investigation, the Secretary of Homeland Security, and  
18          the heads of other relevant elements of the intelligence  
19          community, shall—

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

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

5                   (A) congressional leadership; and

6                   (B) the appropriate congressional commit-  
 7           tees.

8           (c) UPDATE.—Not later than 90 days before any reg-  
 9           ularly scheduled Federal election, the Director of National  
 10          Intelligence shall—

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

13           (2) submit the updated assessment to—

14                   (A) congressional leadership; and

15                   (B) the appropriate congressional commit-  
 16          tees.

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

19           (a) REQUIREMENT FOR A STRATEGY.—Not later  
 20          than 90 days after the date of the enactment of this Act,  
 21          the Director of National Intelligence, in coordination with  
 22          the Secretary of Homeland Security, the Director of the  
 23          Federal Bureau of Investigation, the Director of the Cen-  
 24          tral Intelligence Agency, the Secretary of State, the Sec-  
 25          retary of Defense, and the Secretary of the Treasury, shall

1 develop a whole-of-government strategy for countering the  
2 threat of Russian cyber attacks and attempted cyber at-  
3 tacks against electoral systems and processes in the  
4 United States, including Federal, State, and local election  
5 systems, voter registration databases, voting tabulation  
6 equipment, and equipment and processes for the secure  
7 transmission of election results.

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

11 (1) A whole-of-government approach to pro-  
12 tecting United States electoral systems and proc-  
13 esses that includes the agencies and departments in-  
14 dicated in subsection (a) as well as any other agen-  
15 cies and departments of the United States, as deter-  
16 mined appropriate by the Director of National Intel-  
17 ligence and the Secretary of Homeland Security.

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

21 (3) Technical security measures, including  
22 auditable paper trails for voting machines, securing  
23 wireless and Internet connections, and other tech-  
24 nical safeguards.

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

4           (5) Improvement in the identification and attri-  
5           bution of Russian government or nongovernment  
6           cyber threat actors.

7           (6) Deterrence, including actions and measures  
8           that could or should be undertaken against or com-  
9           municated to the Government of Russia or other en-  
10          tities to deter attacks against, or interference with,  
11          United States election systems and processes.

12          (7) Improvement in Federal Government com-  
13          munications with State and local election officials.

14          (8) Public education and communication ef-  
15          forts.

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

19          (c) CONGRESSIONAL BRIEFING.—

20               (1) IN GENERAL.—Not later than 90 days after  
21               the date of the enactment of this Act, the Director  
22               of National Intelligence and the Secretary of Home-  
23               land Security shall jointly brief the appropriate con-  
24               gressional committees on the strategy developed  
25               under subsection (a).

1           (2) APPROPRIATE CONGRESSIONAL COMMIT-  
 2           TEES DEFINED.—In this subsection, the term “ap-  
 3           propriate congressional committees” means the fol-  
 4           lowing:

5                   (A) The congressional intelligence commit-  
 6           tees.

7                   (B) The Committee on Armed Services and  
 8           the Committee on Homeland Security and Gov-  
 9           ernmental Affairs of the Senate.

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

13 **SEC. 505. INFORMATION SHARING WITH STATE ELECTION**  
 14 **OFFICIALS.**

15           (a) SECURITY CLEARANCES.—

16                   (1) IN GENERAL.—Not later than 30 days after  
 17           the date of the enactment of this Act, the Director  
 18           of National Intelligence shall support the Under Sec-  
 19           retary of Homeland Security for Intelligence and  
 20           Analysis, and any other official of the Department  
 21           of Homeland Security designated by the Secretary of  
 22           Homeland Security, in sponsoring a security clear-  
 23           ance up to the top secret level for each eligible chief  
 24           election official of a State or the District of Colum-  
 25           bia, and additional eligible designees of such election

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

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

9 (b) INFORMATION SHARING.—

10 (1) IN GENERAL.—The Director of National In-  
11 telligence shall assist the Under Secretary of Home-  
12 land Security for Intelligence and Analysis with  
13 sharing any appropriate classified information re-  
14 lated to threats to election systems and to the integ-  
15 rity of the election process with chief election offi-  
16 cials and such designees who have received a secu-  
17 rity clearance under subsection (a).

18 (2) COORDINATION.—The Under Secretary of  
19 Homeland Security for Intelligence and Analysis  
20 shall coordinate with the Director of National Intel-  
21 ligence to facilitate the sharing of information to the  
22 affected Secretaries of State or States.

23 (c) STATE DEFINED.—In this section, the term  
24 “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. 506. DESIGNATION OF COUNTERINTELLIGENCE OFFI-**  
 4 **CER TO LEAD ELECTION SECURITY MATTERS.**

5 (a) IN GENERAL.—The Director of National Intel-  
 6 ligence shall designate a national counterintelligence offi-  
 7 cer within the National Counterintelligence and Security  
 8 Center to lead, manage, and coordinate counterintelligence  
 9 matters relating to election security.

10 (b) ADDITIONAL RESPONSIBILITIES.—The person  
 11 designated under subsection (a) shall also lead, manage,  
 12 and coordinate counterintelligence matters relating to  
 13 risks posed by interference from foreign powers (as de-  
 14 fined in section 101 of the Foreign Intelligence Surveil-  
 15 lance Act of 1978 (50 U.S.C. 1801)) to the following:

- 16 (1) The Federal Government election security
- 17 supply chain.
- 18 (2) Election voting systems and software.
- 19 (3) Voter registration databases.
- 20 (4) Critical infrastructure related to elections.
- 21 (5) Such other Government goods and services
- 22 as the Director of National Intelligence considers ap-
- 23 propriate.

## **TITLE VI—SECURITY CLEARANCES**

### **SEC. 601. DEFINITIONS.**

In this title:

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

(A) the congressional intelligence committees;

(B) the Committee on Armed Services of the Senate;

(C) the Committee on Appropriations of the Senate;

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

(E) the Committee on Armed Services of the House of Representatives;

(F) the Committee on Appropriations of the House of Representatives;

(G) the Committee on Homeland Security of the House of Representatives; and

(H) the Committee on Oversight and Government Reform of the House of Representatives.



1           (2) COUNCIL.—The term “Council” means the  
 2           Security, Suitability, and Credentialing Performance  
 3           Accountability Council established pursuant to Exec-  
 4           utive Order 13467 (73 Fed. Reg. 38103; 50 U.S.C.  
 5           3161 note), or any successor entity.

6           (3) SECURITY EXECUTIVE AGENT.—The term  
 7           “Security Executive Agent” means the Director of  
 8           National Intelligence acting as the Security Execu-  
 9           tive Agent in accordance with section 605.

10          (4) SUITABILITY AND CREDENTIALING EXECU-  
 11          TIVE AGENT.—The term “Suitability and  
 12          Credentialing Executive Agent” means the Director  
 13          of the Office of Personnel Management acting as the  
 14          Suitability and Credentialing Executive Agent in ac-  
 15          cordance with Executive Order 13467 (73 Fed. Reg.  
 16          38103; 50 U.S.C. 3161 note), or any successor enti-  
 17          ty.

18 **SEC. 602. REPORTS AND PLANS RELATING TO SECURITY**  
 19 **CLEARANCES AND BACKGROUND INVESTIGA-**  
 20 **TIONS.**

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

23               (1) ensuring the trustworthiness and security of  
 24               the workforce, facilities, and information of the Fed-

1 eral Government is of the highest priority to na-  
2 tional security and public safety;

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

7 (3) the current system for security clearance,  
8 suitability and fitness for employment, and  
9 credentialing lacks efficiencies and capabilities to  
10 meet the current threat environment, recruit and re-  
11 tain a trusted workforce, and capitalize on modern  
12 technologies; and

13 (4) changes to policies or processes to improve  
14 this system should be vetted through the Council to  
15 ensure standardization, portability, and reciprocity  
16 in security clearances across the Federal Govern-  
17 ment.

18 (b) ACCOUNTABILITY PLANS AND REPORTS.—

19 (1) PLANS.—Not later than 90 days after the  
20 date of the enactment of this Act, the Council shall  
21 submit to the appropriate congressional committees  
22 the following:

23 (A) A plan to reduce the background inves-  
24 tigation inventory to 500,000 by the end of year  
25 2018 and to 200,000 or an otherwise sustain-

1       able steady-level by the end of year 2019. Such  
2       plan shall include notes of any required changes  
3       in investigative and adjudicative standards or  
4       resources.

5               (B) A plan to consolidate the conduct of  
6       background investigations associated with the  
7       processing for positions of trust in the most ef-  
8       fective and efficient manner between the Na-  
9       tional Background Investigation Bureau and  
10      the Defense Security Service, or a successor or-  
11      ganization. Such plan shall address required  
12      funding, personnel, contracts, information tech-  
13      nology, field office structure, policy, governance,  
14      schedule, transition costs, and effects on stake-  
15      holders.

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

18               (A) IN GENERAL.—Not later than 180  
19      days after the date of the enactment of this  
20      Act, the Chairman of the Council, in coordina-  
21      tion with the members of the Council, shall sub-  
22      mit to the appropriate congressional committees  
23      a report on the future of personnel security to  
24      reflect changes in threats, the workforce, and  
25      technology.

1 (B) CONTENTS.—The report submitted  
2 under subparagraph (A) shall include the fol-  
3 lowing:

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

6 (ii) A discussion of the use of tech-  
7 nologies to prevent, detect, and monitor  
8 threats.

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

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

13 (v) An analysis of how to integrate  
14 data from continuous vetting, insider  
15 threat programs, and human resources  
16 data.

17 (vi) Recommendations on interagency  
18 governance.

19 (3) PLAN FOR IMPLEMENTATION.—Not later  
20 than 180 days after the date of the enactment of  
21 this Act, the Chairman of the Council, in coordina-  
22 tion with the members of the Council, shall submit  
23 to the appropriate congressional committees a plan  
24 to implement the report's framework and rec-  
25 ommendations submitted under paragraph (2)(A).

1           (4) CONGRESSIONAL NOTIFICATIONS.—Not less  
2           frequently than monthly, the Security Executive  
3           Agent shall submit a report to the appropriate con-  
4           gressional committees regarding the status of the  
5           disposition of requests received from departments  
6           and agencies of the Federal Government for a  
7           change to, or approval under, the Federal investiga-  
8           tive standards, the national adjudicative guidelines,  
9           continuous evaluation, or other national policy re-  
10          garding personnel security.

11 **SEC. 603. IMPROVING THE PROCESS FOR SECURITY CLEAR-**  
12 **ANCES.**

13          (a) REVIEWS.—Not later than 180 days after the  
14          date of the enactment of this Act, the Security Executive  
15          Agent, in coordination with the members of the Council,  
16          shall submit to the appropriate congressional committees  
17          a report that includes the following:

18               (1) A review of whether the information re-  
19               quested on the Questionnaire for National Security  
20               Positions (Standard Form 86) and by the Federal  
21               Investigative Standards prescribed by the Office of  
22               Personnel Management and the Office of the Direc-  
23               tor of National Intelligence appropriately support  
24               the adjudicative guidelines under Security Executive  
25               Agent Directive 4 (known as the “National Security

1     Adjudicative Guidelines’’). Such review shall include  
2     identification of whether any such information cur-  
3     rently collected is unnecessary to support the adju-  
4     dicative guidelines.

5           (2) An assessment of whether such Question-  
6     naire, Standards, and guidelines should be revised to  
7     account for the prospect of a holder of a security  
8     clearance becoming an insider threat.

9           (3) Recommendations to improve the back-  
10    ground investigation process by—

11           (A) simplifying the Questionnaire for Na-  
12     tional Security Positions (Standard Form 86)  
13     and increasing customer support to applicants  
14     completing such Questionnaire;

15           (B) using remote techniques and central-  
16     ized locations to support or replace field inves-  
17     tigation work;

18           (C) using secure and reliable digitization of  
19     information obtained during the clearance proc-  
20     ess;

21           (D) building the capacity of the back-  
22     ground investigation labor sector; and

23           (E) replacing periodic reinvestigations with  
24     continuous evaluation techniques in all appro-  
25     priate circumstances.

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

2 Not later than 180 days after the date of the enactment  
3 of this Act, the Security Executive Agent shall, in coordi-  
4 nation with the members of the Council, establish the fol-  
5 lowing:

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

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

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

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

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

21 (D) use of the polygraph;

22 (E) the application of the adjudicative  
23 guidelines under Security Executive Agent Di-  
24 rective 4 (known as the “National Security Ad-  
25 judicative 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;

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

11 (I) reporting on security incidents and job  
12 performance that affect the ability to hold a se-  
13 curity clearance;

14 (J) any recommended changes to the Fed-  
15 eral Acquisition Regulations (FAR) necessary  
16 to ensure that information affecting contractor  
17 clearances or suitability is appropriately and ex-  
18 peditiously shared between and among agencies  
19 and contractors; and

20 (K) portability of contractor security clear-  
21 ances between or among contracts at the same  
22 agency and between or among contracts at dif-  
23 ferent agencies that require the same level of  
24 clearance.

25 (3) A strategy and implementation plan that—



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

4 (B) includes actions to assess the extent to  
5 which automated records checks and other con-  
6 tinuous evaluation methods may be used to ex-  
7 pedite or focus reinvestigations; and

8 (C) provides an exception for certain popu-  
9 lations if the Security Executive Agent—

10 (i) determines such populations re-  
11 quire reinvestigations at regular intervals;  
12 and

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

16 (4) A policy and implementation plan for agen-  
17 cies and departments of the United States, as a part  
18 of the security clearance process, to accept auto-  
19 mated records checks generated pursuant to a secu-  
20 rity clearance applicant's employment with a prior  
21 employer.

22 (5) A policy for the use of certain background  
23 materials on individuals collected by the private sec-  
24 tor for background investigation purposes.

1 **SEC. 604. GOALS FOR PROMPTNESS OF DETERMINATIONS**  
2 **REGARDING SECURITY CLEARANCES.**

3 (a) IN GENERAL.—The Council shall take such ac-  
4 tions as may be necessary to ensure that, by December  
5 31, 2021, 90 percent of all determinations regarding—

6 (1) security clearances—

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

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

11 (2) reciprocity of a security clearance at the  
12 same level are recognized in 2 weeks or fewer.

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

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

23 (d) RECIPROCITY DEFINED.—In this section, the  
24 term “reciprocity” means reciprocal recognition by Fed-  
25 eral departments and agencies of eligibility for access to  
26 classified information.

1 **SEC. 605. SECURITY EXECUTIVE AGENT.**

2 (a) IN GENERAL.—The Director of National Intel-  
3 ligence shall serve as the Security Executive Agent for all  
4 departments and agencies of the United States.

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

7 (1) To direct the oversight of investigations, re-  
8 investigations, adjudications, and, as applicable,  
9 polygraphs for eligibility for access to classified in-  
10 formation or eligibility to hold a sensitive position  
11 made by any Federal agency.

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

16 (3) To develop and issue uniform and con-  
17 sistent policies and procedures to ensure the effec-  
18 tive, efficient, timely, and secure completion of inves-  
19 tigations, polygraphs, and adjudications relating to  
20 determinations of eligibility for access to classified  
21 information or eligibility to hold a sensitive position.

22 (4) Unless otherwise designated by law, to serve  
23 as the final authority to designate a Federal agency  
24 or agencies to conduct investigations of persons who  
25 are proposed for access to classified information or  
26 for eligibility to hold a sensitive position to ascertain

1       whether such persons satisfy the criteria for obtain-  
2       ing and retaining access to classified information or  
3       eligibility to hold a sensitive position, as applicable.

4           (5) Unless otherwise designated by law, to serve  
5       as the final authority to designate a Federal agency  
6       or agencies to determine eligibility for access to clas-  
7       sified information or eligibility to hold a sensitive po-  
8       sition in accordance with Executive Order 12968 of  
9       August 2, 1995, as amended.

10          (6) To ensure reciprocal recognition of eligi-  
11       bility for access to classified information or eligibility  
12       to hold a sensitive position among Federal agencies,  
13       including acting as the final authority to arbitrate  
14       and resolve disputes among such agencies involving  
15       the reciprocity of investigations and adjudications of  
16       eligibility.

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

19       (c) AUTHORITIES.—The Security Executive Agent  
20       shall—

21           (1) issue guidelines and instructions to the  
22       heads of Federal agencies to ensure appropriate uni-  
23       formity, centralization, efficiency, effectiveness, time-  
24       liness, and security in processes relating to deter-  
25       minations by such agencies of eligibility for access to

1       classified information or eligibility to hold a sensitive  
2       position, including such matters as investigations,  
3       polygraphs, adjudications, and reciprocity;

4           (2) have the authority to grant exceptions to, or  
5       waivers of, national security investigative require-  
6       ments, including issuing implementing or clarifying  
7       guidance, as necessary;

8           (3) have the authority to assign, in whole or in  
9       part, to the head of any Federal agency (solely or  
10      jointly) any of the duties of the Security Executive  
11      Agent described in subsection (b) or the authorities  
12      described in paragraphs (1) and (2), provided that  
13      the exercise of such assigned duties or authorities is  
14      subject to the oversight of the Security Executive  
15      Agent, including such terms and conditions (includ-  
16      ing approval by the Security Executive Agent) as the  
17      Security Executive Agent determines appropriate;  
18      and

19           (4) define and set standards for continuous  
20      evaluation for continued access to classified informa-  
21      tion and for eligibility to hold a sensitive position.

1 **SEC. 606. REPORT ON UNIFIED, SIMPLIFIED, GOVERNMENT-**  
2 **WIDE STANDARDS FOR POSITIONS OF TRUST**  
3 **AND SECURITY CLEARANCES.**

4 Not later than 90 days after the date of the enact-  
5 ment of this Act, the Security Executive Agent and the  
6 Suitability and Credentialing Executive Agent, in coordi-  
7 nation with the other members of the Council, shall jointly  
8 issue a report regarding the advisability and the risks,  
9 benefits, and costs to the Government and to industry of  
10 consolidating to not more than 3 tiers for positions of  
11 trust and security clearances.

12 **SEC. 607. REPORT ON CLEARANCE IN PERSON CONCEPT.**

13 (a) SENSE OF CONGRESS.—It is the sense of Con-  
14 gress that to reflect the greater mobility of the modern  
15 workforce, alternative methodologies merit analysis to  
16 allow greater flexibility for individuals moving in and out  
17 of positions that require access to classified information,  
18 while still preserving security.

19 (b) REPORT REQUIRED.—Not later than 90 days  
20 after the date of the enactment of this Act, the Security  
21 Executive Agent shall submit a report to the appropriate  
22 congressional committees that describes the requirements,  
23 feasibility, and advisability of implementing a clearance in  
24 person concept described in subsection (c) for maintaining  
25 access to classified information.

1 (c) CLEARANCE IN PERSON CONCEPT.—The clear-  
2 ance in person concept—

3 (1) permits an individual to maintain his or her  
4 eligibility for access to classified information, net-  
5 works, and facilities for up to 3 years after the indi-  
6 vidual's access to classified information would other-  
7 wise lapse; and

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

12 (d) CONTENTS.—The report required under sub-  
13 section (b) shall address—

14 (1) requirements for an individual to voluntarily  
15 remain in a continuous evaluation program validated  
16 by the Security Executive Agent even if the indi-  
17 vidual is not in a position requiring access to classi-  
18 fied information;

19 (2) appropriate safeguards for privacy;

20 (3) advantages to government and industry;

21 (4) the costs and savings associated with imple-  
22 mentation;

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

25 (6) an appropriate funding model; and

1           (7) fairness to small companies and inde-  
2       pendent contractors.

3   **SEC. 608. BUDGET REQUEST DOCUMENTATION ON FUND-**  
4                   **ING FOR CLEARANCES.**

5       (a) IN GENERAL.—As part of the fiscal year 2020  
6   budget request submitted to Congress pursuant to section  
7   1105(a) of title 31, United States Code, the President  
8   shall include exhibits that identify the resources allocated  
9   by each agency to processing security clearances,  
10   disaggregated by type of security clearance.

11       (b) CONTENTS.—Each exhibit submitted under sub-  
12   section (a) shall include, with respect to security clear-  
13   ances, details on the costs of—

14           (1) background investigations and reinvestiga-  
15       tions;

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

18           (3) adjudications;

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

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



1 **SEC. 609. REPORTS ON RECIPROCITY FOR SECURITY**  
2 **CLEARANCES INSIDE OF DEPARTMENTS AND**  
3 **AGENCIES.**

4 (a) **REPORTS TO SECURITY EXECUTIVE AGENT.**—

5 The head of each Federal department or agency shall sub-  
6 mit an annual report to the Security Executive Agent  
7 that—

8 (1) identifies the number of individuals whose  
9 security clearances take more than 2 weeks to be re-  
10 ciprocally recognized after such individuals move to  
11 another part of such department or agency; and

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

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

20 (c) **RECIPROCALLY RECOGNIZED DEFINED.**—In this  
21 section, the term “reciprocally recognized” means recip-  
22 rocal recognition by Federal departments and agencies of  
23 eligibility for access to classified information.

1 **SEC. 610. INTELLIGENCE COMMUNITY REPORTS ON SECU-**  
2 **RITY CLEARANCES.**

3 Section 506H of the National Security Act of 1947  
4 (50 U.S.C. 3104) is amended—

5 (1) in subsection (a)(1)—

6 (A) in subparagraph (A)(ii), by adding  
7 “and” at the end;

8 (B) in subparagraph (B)(ii), by striking “;  
9 and” and inserting a period; and

10 (C) by striking subparagraph (C);

11 (2) by redesignating subsection (b) as sub-  
12 section (c);

13 (3) by inserting after subsection (a) the fol-  
14 lowing:

15 “(b) INTELLIGENCE COMMUNITY REPORTS.—(1)

16 Not later than March 1 of each year, the Director of Na-  
17 tional Intelligence shall submit a report to the congres-  
18 sional intelligence committees, the Committee on Home-  
19 land Security and Governmental Affairs of the Senate,  
20 and the Committee on Homeland Security of the House  
21 of Representatives regarding the security clearances proc-  
22 essed by each element of the intelligence community dur-  
23 ing the preceding fiscal year. Each report submitted under  
24 this paragraph shall separately identify security clearances  
25 processed for Federal employees and contractor employees  
26 sponsored by each such element.

1       “(2) Each report submitted under paragraph (1)  
2 shall include, for each element of the intelligence commu-  
3 nity for the fiscal year covered by the report, the following:

4           “(A) The total number of initial security clear-  
5 ance background investigations sponsored for new  
6 applicants.

7           “(B) The total number of security clearance  
8 periodic reinvestigations sponsored for existing em-  
9 ployees.

10          “(C) The total number of initial security clear-  
11 ance background investigations for new applicants  
12 that were adjudicated with notice of a determination  
13 provided to the prospective applicant, including—

14           “(i) the total number of such adjudications  
15 that were adjudicated favorably and granted ac-  
16 cess to classified information; and

17           “(ii) the total number of such adjudica-  
18 tions that were adjudicated unfavorably and re-  
19 sulted in a denial or revocation of a security  
20 clearance.

21          “(D) The total number of security clearance  
22 periodic background investigations that were adju-  
23 dicated with notice of a determination provided to  
24 the existing employee, including—

1           “(i) the total number of such adjudications  
2           that were adjudicated favorably; and

3           “(ii) the total number of such adjudica-  
4           tions that were adjudicated unfavorably and re-  
5           sulted in a denial or revocation of a security  
6           clearance.

7           “(E) The total number of pending security  
8           clearance background investigations, including initial  
9           applicant investigations and periodic reinvestiga-  
10          tions, that were not adjudicated as of the last day  
11          of such year and that remained pending, categorized  
12          as follows:

13               “(i) For 180 days or shorter.

14               “(ii) For longer than 180 days, but shorter  
15               than 12 months.

16               “(iii) For 12 months or longer, but shorter  
17               than 18 months.

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

20               “(v) For 24 months or longer.

21           “(F) For any security clearance determinations  
22           completed or pending during the year preceding the  
23           year for which the report is submitted that have  
24           taken longer than 12 months to complete—

1           “(i) an explanation of the causes for the  
2           delays incurred during the period covered by  
3           the report; and

4           “(ii) the number of such delays involving a  
5           polygraph requirement.

6           “(G) The percentage of security clearance in-  
7           vestigations, including initial and periodic reinves-  
8           tigations, that resulted in a denial or revocation of  
9           a security clearance.

10          “(H) The percentage of security clearance in-  
11          vestigations that resulted in incomplete information.

12          “(I) The percentage of security clearance inves-  
13          tigations that did not result in enough information  
14          to make a decision on potentially adverse informa-  
15          tion.

16          “(3) The report required under this subsection shall  
17          be submitted in unclassified form, but may include a clas-  
18          sified annex.”; and

19          (4) in subsection (c), as redesignated, by strik-  
20          ing “subsection (a)(1)” and inserting “subsections  
21          (a)(1) and (b)”.

1 **SEC. 611. PERIODIC REPORT ON POSITIONS IN THE INTEL-**  
2 **LIGENCE COMMUNITY WHICH CAN BE CON-**  
3 **DUCTED WITHOUT ACCESS TO CLASSIFIED**  
4 **INFORMATION, NETWORKS, OR FACILITIES.**

5 Not later than 180 days after the date of the enact-  
6 ment of this Act and not less frequently than once every  
7 5 years thereafter, the Director of National Intelligence  
8 shall submit to the congressional intelligence committees  
9 a report that reviews the intelligence community for which  
10 positions can be conducted without access to classified in-  
11 formation, networks, or facilities, or may only require a  
12 security clearance at the secret level.

13 **SEC. 612. INFORMATION SHARING PROGRAM FOR POSI-**  
14 **TIONS OF TRUST.**

15 (a) AGENCY DEFINED.—In this section, the term  
16 “agency” has the meaning given the term “Executive  
17 agency” in section 105 of title 5, United States Code.

18 (b) PROGRAM REQUIRED.—Not later than 90 days  
19 after the date of the enactment of this Act, the Security  
20 Executive Agent shall establish a program to share be-  
21 tween and among agencies and industry partners of the  
22 Federal Government information regarding individuals ap-  
23 plying for and in positions of trust, including derogatory  
24 and suitability information.

25 (c) GOAL.—The goal of the program required by sub-  
26 section (b) shall be to alert agencies and industry partners

1 as to individuals who may require further vetting or  
2 should be subject to certain insider threat programs re-  
3 garding granted access, or continued access, to classified  
4 information, especially when such individuals change agen-  
5 cies, employers, or contracts.

6 (d) PRIVACY SAFEGUARDS.—The Security Executive  
7 Agent shall ensure that the program required by sub-  
8 section (b) includes such safeguards for privacy as the Se-  
9 curity Executive Agent considers appropriate.

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

13 (1) sufficient information is provided to the pri-  
14 vate sector so that employers in the private sector  
15 can make informed decisions about hiring and reten-  
16 tion in positions of trust; and

17 (2) agencies and private sector entities that re-  
18 ceive information under the program have the capa-  
19 bilities in place to safeguard personnel privacy in  
20 compliance with applicable law and policy.

21 (f) IMPLEMENTATION PLAN.—

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

1        appropriate congressional committees for the implementa-  
2        tion of the program required under subsection (b).

3            (2) CONTENTS.—The plan required under para-  
4        graph (1) shall include—

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

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

10 **SEC. 613. REPORT ON PROTECTIONS FOR CONFIDEN-**  
11 **TIALITY OF WHISTLEBLOWER-RELATED COM-**  
12 **MUNICATIONS.**

13        Not later than 180 days after the date of the enact-  
14        ment of this Act, the Security Executive Agent shall, in  
15        coordination with the Inspector General of the Intelligence  
16        Community, submit to the appropriate congressional com-  
17        mittees a report detailing the controls employed by the in-  
18        telligence community to ensure that continuous evaluation  
19        programs, including those involving user activity moni-  
20        toring, protect the confidentiality of whistleblower-related  
21        communications.



1           **TITLE VII—REPORTS AND**  
2                   **OTHER MATTERS**  
3           **Subtitle A—Matters Relating to**  
4           **Russia and Other Foreign Powers**

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

8           (a) APPROPRIATE CONGRESSIONAL COMMITTEES.—

9   The term “appropriate congressional committees”  
10 means—

11           (1) the congressional intelligence committees;  
12           and

13           (2) the Committee on Armed Services of the  
14           Senate and the Committee on Armed Services of the  
15           House of Representatives.

16           (b) LIMITATION.—

17           (1) IN GENERAL.—No amount may be ex-  
18           pended by the Federal Government, other than the  
19           Department of Defense, to enter into or implement  
20           any bilateral agreement between the United States  
21           and the Russian Federation regarding cybersecurity,  
22           including the establishment or support of any cyber-  
23           security unit, unless, at least 30 days prior to the  
24           conclusion of any such agreement, the Director of  
25           National Intelligence submits to the appropriate con-

gressional committees a report on such agreement that includes the elements required by subsection (c).

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

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

(1) The purpose of the agreement.

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

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

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

1 (d) RULE OF CONSTRUCTION.—This section shall not  
2 be construed to affect any existing authority of the Direc-  
3 tor of National Intelligence, the Director of the Central  
4 Intelligence Agency, or any other head of an element of  
5 the intelligence community, to share or receive foreign in-  
6 telligence on a case-by-case basis.

7 **SEC. 702. 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, the real property in Maryland, and the  
11 real property in San Francisco, California, that were  
12 under the control of the Government of Russia in 2016  
13 and were removed from such control in response to various  
14 transgressions by the Government of Russia, including the  
15 interference by the Government of Russia in the 2016  
16 election in the United States.

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

23 (c) FORM OF REPORT.—The report required by this  
24 section shall be submitted in classified and unclassified  
25 forms.

1 **SEC. 703. ASSESSMENT OF THREAT FINANCE RELATING TO**  
2 **RUSSIA.**

3 (a) **THREAT FINANCE DEFINED.**—In this section,  
4 the term “threat finance” means—

5 (1) the financing of cyber operations, global in-  
6 fluence campaigns, intelligence service activities, pro-  
7 liferation, terrorism, or transnational crime and  
8 drug organizations;

9 (2) the methods and entities used to spend,  
10 store, move, raise, conceal, or launder money or  
11 value, on behalf of threat actors;

12 (3) sanctions evasion; and

13 (4) other forms of threat finance activity do-  
14 mestically or internationally, as defined by the Presi-  
15 dent.

16 (b) **REPORT REQUIRED.**—Not later than 60 days  
17 after the date of the enactment of this Act, the Director  
18 of National Intelligence, in coordination with the Assistant  
19 Secretary of the Treasury for Intelligence and Analysis,  
20 shall submit to the congressional intelligence committees  
21 a report containing an assessment of Russian threat fi-  
22 nance. The assessment shall be based on intelligence from  
23 all sources, including from the Office of Terrorism and  
24 Financial Intelligence of the Department of the Treasury.

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

1           (1) A summary of leading examples from the 3-  
2           year period preceding the date of the submittal of  
3           the report of threat finance activities conducted by,  
4           for the benefit of, or at the behest of—

5                   (A) officials of the Government of Russia;

6                   (B) persons subject to sanctions under any  
7           provision of law imposing sanctions with respect  
8           to Russia;

9                   (C) Russian nationals subject to sanctions  
10          under any other provision of law; or

11                  (D) Russian oligarchs or individuals in-  
12          volved in organized crime.

13          (2) An assessment with respect to any trends or  
14          patterns in threat finance activities relating to Rus-  
15          sia, including common methods of conducting such  
16          activities and global nodes of money laundering used  
17          by Russian threat actors described in paragraph (1)  
18          and associated entities.

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

22          (4) A summary of engagement and coordination  
23          with international partners on threat finance relat-  
24          ing to Russia, especially in Europe, including exam-  
25          ples of such engagement and coordination.

1           (5) An identification of any resource and collec-  
2       tion gaps.

3           (6) An identification of—

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

7                (B) any vulnerabilities within the United  
8       States legal and financial system, including spe-  
9       cific sectors, which have been or could be ex-  
10      ploited in connection with Russian threat fi-  
11      nance activities; and

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

18           (7) Any other matters the Director determines  
19      appropriate.

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

22      **SEC. 704. NOTIFICATION OF AN ACTIVE MEASURES CAM-**  
23                                   **PAIGN.**

24      (a) DEFINITIONS.—In this section:

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

4           (A) the congressional intelligence commit-  
5       tees; and

6           (B) the Committee on Armed Services of  
7       the Senate and the Committee on Armed Serv-  
8       ices of the House of Representatives.

9           (2) CONGRESSIONAL LEADERSHIP.—The term  
10      “congressional leadership” includes the following:

11           (A) The majority leader of the Senate.

12           (B) The minority leader of the Senate.

13           (C) The Speaker of the House of Rep-  
14      resentatives.

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

17      (b) REQUIREMENT FOR NOTIFICATION.—The Direc-  
18      tor of National Intelligence, in cooperation with the Direc-  
19      tor of the Federal Bureau of Investigation and the head  
20      of any other relevant agency, shall notify the congressional  
21      leadership and the Chairman and Vice Chairman or Rank-  
22      ing Member of each of the appropriate congressional com-  
23      mittees, and of other relevant committees of jurisdiction,  
24      each time the Director of National Intelligence determines  
25      there is credible information that a foreign power has, is,

1 or will attempt to employ a covert influence or active  
 2 measures campaign with regard to the modernization, em-  
 3 ployment, doctrine, or force posture of the nuclear deter-  
 4 rent or missile defense.

5 (c) CONTENT OF NOTIFICATION.—Each notification  
 6 required by subsection (a) shall include information con-  
 7 cerning actions taken by the United States to expose or  
 8 halt an attempt referred to in subsection (a).

9 **SEC. 705. NOTIFICATION OF TRAVEL BY ACCREDITED DIP-**  
 10 **LOMATIC AND CONSULAR PERSONNEL OF**  
 11 **THE RUSSIAN FEDERATION IN THE UNITED**  
 12 **STATES.**

13 In carrying out the advance notification requirements  
 14 set out in section 502 of the Intelligence Authorization  
 15 Act for Fiscal Year 2017 (division N of Public Law 115–  
 16 31; 131 Stat. 825; 22 U.S.C. 254a note), the Secretary  
 17 of State shall—

18 (1) ensure that the Russian Federation provides  
 19 notification to the Secretary of State at least 2 busi-  
 20 ness days in advance of all travel that is subject to  
 21 such requirements by accredited diplomatic and con-  
 22 sular personnel of the Russian Federation in the  
 23 United States, and take necessary action to secure  
 24 full compliance by Russian personnel and address  
 25 any noncompliance; and



(2) provide notice of travel described in paragraph (1) to the Director of National Intelligence and the Director of the Federal Bureau of Investigation within 1 hour of receiving notice of such travel.

## **Subtitle B—Reports**

### **SEC. 711. TECHNICAL CORRECTION TO INSPECTOR GENERAL STUDY.**

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

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

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

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

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

(a) HOMELAND SECURITY INTELLIGENCE ENTERPRISE DEFINED.—In this section, the term “Homeland Security Intelligence Enterprise” has the meaning given such term in Department of Homeland Security Instruction Number 264–01–001, or successor authority.

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

1 Secretary of Homeland Security, in consultation with the  
2 Under Secretary of Homeland Security for Intelligence  
3 and Analysis, shall submit to the congressional intelligence  
4 committees, the Committee on Homeland Security and  
5 Governmental Affairs of the Senate, and the Committee  
6 on Homeland Security of the House of Representatives a  
7 report on the authorities of the Under Secretary.

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

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

15 (A) the obstacles to exercising the authori-  
16 ties of the Chief Intelligence Officer of the De-  
17 partment and the Homeland Security Intel-  
18 ligence Council, of which the Chief Intelligence  
19 Officer is the chair; and

20 (B) the legal and policy changes necessary  
21 to effectively coordinate, organize, and lead in-  
22 telligence activities of the Department of Home-  
23 land Security.

24 (2) A description of the actions that the Sec-  
25 retary has taken to address the inability of the

1 Under Secretary to require components of the De-  
2 partment, other than the Office of Intelligence and  
3 Analysis of the Department to—

4 (A) coordinate intelligence programs; and

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

7 **SEC. 713. REPORT ON CYBER EXCHANGE PROGRAM.**

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

15 (1) an employee of an element of the intel-  
16 ligence community with demonstrated expertise and  
17 work experience in cybersecurity or related dis-  
18 ciplines may elect to be temporarily detailed to a pri-  
19 vate technology company that has elected to receive  
20 the detailee; and

21 (2) an employee of a private technology com-  
22 pany with demonstrated expertise and work experi-  
23 ence in cybersecurity or related disciplines may elect  
24 to be temporarily detailed to an element of the intel-

1       ligence community that has elected to receive the  
2       detailee.

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

5           (1) An assessment of the feasibility of estab-  
6       lishing the exchange program described in such sub-  
7       section.

8           (2) Identification of any challenges in estab-  
9       lishing the exchange program.

10          (3) An evaluation of the benefits to the intel-  
11       ligence community that would result from the ex-  
12       change program.

13 **SEC. 714. REPORT ON ROLE OF DIRECTOR OF NATIONAL IN-**  
14 **TELLIGENCE WITH RESPECT TO CERTAIN**  
15 **FOREIGN INVESTMENTS.**

16       (a) REPORT.—Not later than 180 days after the date  
17 of the enactment of this Act, the Director of National In-  
18 telligence, in consultation with the heads of the elements  
19 of the intelligence community determined appropriate by  
20 the Director, shall submit to the congressional intelligence  
21 committees a report on the role of the Director in pre-  
22 paring analytic materials in connection with the evaluation  
23 by the Federal Government of national security risks asso-  
24 ciated with potential foreign investments into the United  
25 States.

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

3 (1) a description of the current process for the  
 4 provision of the analytic materials described in sub-  
 5 section (a);

6 (2) identification of the most significant bene-  
 7 fits and drawbacks of such process with respect to  
 8 the role of the Director, including any benefits or  
 9 drawbacks relating to the time allotted to the Direc-  
 10 tor to prepare such materials; and

11 (3) recommendations to improve such process.

12 **SEC. 715. REPORT ON SURVEILLANCE BY FOREIGN GOV-**  
 13 **ERNMENTS AGAINST UNITED STATES TELE-**  
 14 **COMMUNICATIONS NETWORKS.**

15 (a) APPROPRIATE CONGRESSIONAL COMMITTEES  
 16 DEFINED.—In this section, the term “appropriate con-  
 17 gressional committees” means the following:

18 (1) The congressional intelligence committees.

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

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

1 (b) REPORT.—Not later than 180 days after the date  
 2 of the enactment of this Act, the Director of National In-  
 3 telligence shall, in coordination with the Director of the  
 4 Central Intelligence Agency, the Director of the National  
 5 Security Agency, the Director of the Federal Bureau of  
 6 Investigation, and the Secretary of Homeland Security,  
 7 submit to the appropriate congressional committees a re-  
 8 port describing—

9 (1) any attempts known to the intelligence com-  
 10 munity by foreign governments to exploit cybersecu-  
 11 rity vulnerabilities in United States telecommuni-  
 12 cations networks (including Signaling System No. 7)  
 13 to target for surveillance of United States persons,  
 14 including employees of the Federal Government; and

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

20 **SEC. 716. BIENNIAL REPORT ON FOREIGN INVESTMENT**  
 21 **RISKS.**

22 (a) INTELLIGENCE COMMUNITY INTERAGENCY  
 23 WORKING GROUP.—

24 (1) REQUIREMENT TO ESTABLISH.—The Direc-  
 25 tor of National Intelligence shall establish an intel-

1       ligence community interagency working group to  
2       prepare the biennial reports required by subsection  
3       (b).

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

7               (3) MEMBERSHIP.—Such interagency working  
8       group shall be composed of representatives of each  
9       element of the intelligence community that the Di-  
10      rector of National Intelligence determines appro-  
11      priate.

12      (b) BIENNIAL REPORT ON FOREIGN INVESTMENT  
13      RISKS.—

14              (1) REPORT REQUIRED.—Not later than 180  
15      days after the date of the enactment of this Act, and  
16      biennially thereafter, the Director of National Intel-  
17      ligence shall submit to the congressional intelligence  
18      committees, the Committee on Homeland Security  
19      and Governmental Affairs of the Senate, and the  
20      Committee on Homeland Security of the House of  
21      Representatives a report on foreign investment risks  
22      prepared by the interagency working group estab-  
23      lished under subsection (a).

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

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

7                   (B) Any strategy used by a foreign country  
 8                   that such interagency working group has identi-  
 9                   fied to be a country of special concern to use  
 10                  foreign investment to target the acquisition of  
 11                  critical technologies, critical materials, or crit-  
 12                  ical infrastructure.

13                  (C) Any economic espionage efforts di-  
 14                  rected at the United States by a foreign coun-  
 15                  try, particularly such a country of special con-  
 16                  cern.

17 **SEC. 717. MODIFICATION OF CERTAIN REPORTING RE-**  
 18 **QUIREMENT ON TRAVEL OF FOREIGN DIP-**  
 19 **LOMATS.**

20           Section 502(d)(2) of the Intelligence Authorization  
 21   Act for Fiscal Year 2017 (Public Law 115–31; 22 U.S.C.  
 22   254a note) is amended by striking “the number” and in-  
 23   serting “a best estimate”.



1 **SEC. 718. SEMIANNUAL REPORTS ON INVESTIGATIONS OF**  
 2 **UNAUTHORIZED DISCLOSURES OF CLASSI-**  
 3 **FIED INFORMATION.**

4 (a) IN GENERAL.—Title XI of the National Security  
 5 Act of 1947 (50 U.S.C. 3231 et seq.) is amended by add-  
 6 ing at the end the following new section:

7 **“SEC. 1105. SEMIANNUAL REPORTS ON INVESTIGATIONS OF**  
 8 **UNAUTHORIZED DISCLOSURES OF CLASSI-**  
 9 **FIED INFORMATION.**

10 “(a) DEFINITIONS.—In this section:

11 “(1) COVERED OFFICIAL.—The term ‘covered  
 12 official’ means—

13 “(A) the heads of each element of the in-  
 14 telligence community; and

15 “(B) the inspectors general with oversight  
 16 responsibility for an element of the intelligence  
 17 community.

18 “(2) INVESTIGATION.—The term ‘investigation’  
 19 means any inquiry, whether formal or informal, into  
 20 the existence of an unauthorized public disclosure of  
 21 classified information.

22 “(3) UNAUTHORIZED DISCLOSURE OF CLASSI-  
 23 FIED INFORMATION.—The term ‘unauthorized dis-  
 24 closure of classified information’ means any unau-  
 25 thorized disclosure of classified information to any  
 26 recipient.

1           “(4) UNAUTHORIZED PUBLIC DISCLOSURE OF  
2           CLASSIFIED INFORMATION.—The term ‘unauthorized  
3           public disclosure of classified information’ means the  
4           unauthorized disclosure of classified information to a  
5           journalist or media organization.

6           “(b) INTELLIGENCE COMMUNITY REPORTING.—

7           “(1) IN GENERAL.—Not less frequently than  
8           once every 6 months, each covered official shall sub-  
9           mit to the congressional intelligence committees a  
10          report on investigations of unauthorized public dis-  
11          closures of classified information.

12          “(2) ELEMENTS.—Each report submitted under  
13          paragraph (1) shall include, with respect to the pre-  
14          ceding 6-month period, the following:

15               “(A) The number of investigations opened  
16               by the covered official regarding an unauthor-  
17               ized public disclosure of classified information.

18               “(B) The number of investigations com-  
19               pleted by the covered official regarding an un-  
20               authorized public disclosure of classified infor-  
21               mation.

22               “(C) Of the number of such completed in-  
23               vestigations identified under subparagraph (B),  
24               the number referred to the Attorney General  
25               for criminal investigation.

1       “(c) DEPARTMENT OF JUSTICE REPORTING.—

2               “(1) IN GENERAL.—Not less frequently than  
3       once every 6 months, the Assistant Attorney General  
4       for National Security of the Department of Justice,  
5       in consultation with the Director of the Federal Bu-  
6       reau of Investigation, shall submit to the congres-  
7       sional intelligence committees, the Committee on the  
8       Judiciary of the Senate, and the Committee on the  
9       Judiciary of the House of Representatives a report  
10      on the status of each referral made to the Depart-  
11      ment of Justice from any element of the intelligence  
12      community regarding an unauthorized disclosure of  
13      classified information made during the most recent  
14      365-day period or any referral that has not yet been  
15      closed, regardless of the date the referral was made.

16              “(2) CONTENTS.—Each report submitted under  
17      paragraph (1) shall include, for each referral covered  
18      by the report, at a minimum, the following:

19                  “(A) The date the referral was received.

20                  “(B) A statement indicating whether the  
21              alleged unauthorized disclosure described in the  
22              referral was substantiated by the Department  
23              of Justice.

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

4           “(D) A statement indicating whether an  
5           open criminal investigation related to the refer-  
6           ral is active.

7           “(E) A statement indicating whether any  
8           criminal charges have been filed related to the  
9           referral.

10          “(F) A statement indicating whether the  
11          Department of Justice has been able to at-  
12          tribute the unauthorized disclosure to a par-  
13          ticular entity or individual.

14          “(d) FORM OF REPORTS.—Each report submitted  
15          under this section shall be submitted in unclassified form,  
16          but may have a classified annex.”.

17          (b) CLERICAL AMENDMENT.—The table of contents  
18          in the first section of the National Security Act of 1947  
19          is amended by inserting after the item relating to section  
20          1104 the following new item:

“Sec. 1105. Semiannual reports on investigations of unauthorized disclosures of  
classified information.”.

1 **SEC. 719. CONGRESSIONAL NOTIFICATION OF DESIGNA-**  
2 **TION OF COVERED INTELLIGENCE OFFICER**  
3 **AS PERSONA NON GRATA.**

4 (a) INTELLIGENCE OFFICER DEFINED.—In this sec-  
5 tion, the term “covered intelligence officer” means—

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

8 (2) a known or suspected foreign intelligence of-  
9 ficer serving in a United States post.

10 (b) REQUIREMENT FOR REPORTS.—Not later than  
11 72 hours after a covered intelligence officer is designated  
12 as a persona non grata, the Director of National Intel-  
13 ligence, in consultation with the Secretary of State, shall  
14 submit to the congressional intelligence committees a noti-  
15 fication of that designation. Each such notification shall  
16 include—

17 (1) the date of the designation;

18 (2) the basis for the designation; and

19 (3) a justification for the expulsion.

20 **SEC. 720. INSPECTORS GENERAL REPORTS ON CLASSIFICA-**  
21 **TION.**

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

1           (1) The accuracy of the application of classi-  
2           fication and handling markers on a representative  
3           sample of finished reports, including such reports  
4           that are compartmented.

5           (2) Compliance with declassification procedures.

6           (3) The effectiveness of processes for identi-  
7           fying topics of public or historical importance that  
8           merit prioritization for a declassification review.

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

11           (1) The Inspector General of the Intelligence  
12          Community.

13           (2) The Inspector General of the Central Intel-  
14          ligence Agency.

15           (3) The Inspector General of the National Se-  
16          curity Agency.

17           (4) The Inspector General of the Defense Intel-  
18          ligence Agency.

19           (5) The Inspector General of the National Re-  
20          connaissance Office.

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

1 **SEC. 721. REPORTS ON INTELLIGENCE COMMUNITY PAR-**  
2 **TICIPATION IN VULNERABILITIES EQUITIES**  
3 **PROCESS OF FEDERAL GOVERNMENT.**

4 (a) DEFINITIONS.—In this section:

5 (1) VULNERABILITIES EQUITIES POLICY AND  
6 PROCESS DOCUMENT.—The term “Vulnerabilities  
7 Equities Policy and Process document” means the  
8 executive branch document entitled “Vulnerabilities  
9 Equities Policy and Process” dated November 15,  
10 2017.

11 (2) VULNERABILITIES EQUITIES PROCESS.—  
12 The term “Vulnerabilities Equities Process” means  
13 the interagency review of vulnerabilities, pursuant to  
14 the Vulnerabilities Equities Policy and Process docu-  
15 ment or any successor document.

16 (3) VULNERABILITY.—The term “vulnerability”  
17 means a weakness in an information system or its  
18 components (for example, system security proce-  
19 dures, hardware design, and internal controls) that  
20 could be exploited or could affect confidentiality, in-  
21 tegrity, or availability of information.

22 (b) REPORTS ON PROCESS AND CRITERIA UNDER  
23 VULNERABILITIES EQUITIES POLICY AND PROCESS.—

24 (1) IN GENERAL.—Not later than 90 days after  
25 the date of the enactment of this Act, the Director  
26 of National Intelligence shall submit to the congres-

1 sional intelligence committees a written report de-  
2 scribing—

3 (A) with respect to each element of the in-  
4 telligence community—

5 (i) the title of the official or officials  
6 responsible for determining whether, pur-  
7 suant to criteria contained in the  
8 Vulnerabilities Equities Policy and Process  
9 document or any successor document, a  
10 vulnerability must be submitted for review  
11 under the Vulnerabilities Equities Process;  
12 and

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

15 (B) the roles or responsibilities of that ele-  
16 ment during a review of a vulnerability sub-  
17 mitted to the Vulnerabilities Equities Process.

18 (2) CHANGES TO PROCESS OR CRITERIA.—Not  
19 later than 30 days after any significant change is  
20 made to the process and criteria used by any ele-  
21 ment of the intelligence community for determining  
22 whether to submit a vulnerability for review under  
23 the Vulnerabilities Equities Process, such element  
24 shall submit to the congressional intelligence com-  
25 mittees a report describing such change.



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

5       (c) ANNUAL REPORTS.—

6           (1) IN GENERAL.—Not less frequently than  
7       once each calendar year, the Director of National In-  
8       telligence shall submit to the congressional intel-  
9       ligence committees a classified report containing,  
10      with respect to the previous year—

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

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

19           (C) the aggregate number, by category, of  
20           the vulnerabilities excluded from review under  
21           the Vulnerabilities Equities Process, as de-  
22           scribed in paragraph 5.4 of the Vulnerabilities  
23           Equities Policy and Process document.

1           (2) UNCLASSIFIED INFORMATION.—Each report  
 2       submitted under paragraph (1) shall include an un-  
 3       classified appendix that contains—

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

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

11          (3) NON-DUPLICATION.—The Director of Na-  
 12      tional Intelligence may forgo submission of an an-  
 13      nual report required under this subsection for a cal-  
 14      endar year, if the Director notifies the intelligence  
 15      committees in writing that, with respect to the same  
 16      calendar year, an annual report required by para-  
 17      graph 4.3 of the Vulnerabilities Equities Policy and  
 18      Process document already has been submitted to  
 19      Congress, and such annual report contains the infor-  
 20      mation that would otherwise be required to be in-  
 21      cluded in an annual report under this subsection.

22   **SEC. 722. REPORTS ON GLOBAL WATER INSECURITY AND**  
 23       **NATIONAL SECURITY IMPLICATIONS.**

24          (a) REPORTS REQUIRED.—Not later than 180 days  
 25      after the date of the enactment of this Act and not less

1 frequently than once every 5 years thereafter, the Director  
2 of National Intelligence shall submit to the congressional  
3 intelligence committees a report on the implications of  
4 water insecurity on the national security interest of the  
5 United States, including consideration of social, economic,  
6 agricultural, and environmental factors.

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

11 (1) of strategic, economic, or humanitarian in-  
12 terest to the United States—

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

16 (B) where challenges relating to water in-  
17 security are likely to emerge and become signifi-  
18 cant during the 5-year or the 20-year period be-  
19 ginning on the date of the report; and

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

23 (c) CONSULTATION.—In researching a report re-  
24 quired by subsection (a), the Director shall consult with—

1           (1) such stakeholders within the intelligence  
2           community, the Department of Defense, and the De-  
3           partment of State as the Director considers appro-  
4           priate; and

5           (2) such additional Federal agencies and per-  
6           sons in the private sector as the Director considers  
7           appropriate.

8           (d) FORM.—Each report submitted under subsection  
9           (a) shall be submitted in unclassified form, but may in-  
10          clude a classified annex.

11 **SEC. 723. ANNUAL REPORT ON MEMORANDA OF UNDER-**  
12 **STANDING BETWEEN ELEMENTS OF INTEL-**  
13 **LIGENCE COMMUNITY AND OTHER ENTITIES**  
14 **OF THE UNITED STATES GOVERNMENT RE-**  
15 **GARDING SIGNIFICANT OPERATIONAL AC-**  
16 **TIVITIES OR POLICY.**

17          Section 311 of the Intelligence Authorization Act for  
18          Fiscal Year 2017 (50 U.S.C. 3313) is amended—

19               (1) by redesignating subsection (b) as sub-  
20               section (c); and

21               (2) by striking subsection (a) and inserting the  
22               following:

23               “(a) IN GENERAL.—Each year, concurrent with the  
24               annual budget request submitted by the President to Con-  
25               gress under section 1105 of title 31, United States Code,

1 each head of an element of the intelligence community  
 2 shall submit to the congressional intelligence committees  
 3 a report that lists each memorandum of understanding or  
 4 other agreement regarding significant operational activi-  
 5 ties or policy entered into during the most recently com-  
 6 pleted fiscal year between or among such element and any  
 7 other entity of the United States Government.

8 “(b) PROVISION OF DOCUMENTS.—Each head of an  
 9 element of an intelligence community who receives a re-  
 10 quest from the Select Committee on Intelligence of the  
 11 Senate or the Permanent Select Committee on Intelligence  
 12 of the House of Representatives for a copy of a memo-  
 13 randum of understanding or other document listed in a  
 14 report submitted by the head under subsection (a) shall  
 15 submit to such committee the requested copy as soon as  
 16 practicable after receiving such request.”.

17 **SEC. 724. REPEAL OF REPORT REQUIREMENT FOR INSPEC-**  
 18 **TORS GENERAL OF CERTAIN ELEMENTS OF**  
 19 **INTELLIGENCE COMMUNITY.**

20 (a) IN GENERAL.—Section 8H of the Inspector Gen-  
 21 eral Act of 1978 (5 U.S.C. App.) is amended—

22 (1) by striking subsection (g); and

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

25 (b) CONFORMING AMENDMENTS.—

1           (1) NATIONAL SECURITY ACT OF 1947.—Section  
 2           507(a) of the National Security Act of 1947 (50  
 3           U.S.C. 3106(a)) is amended—

4                   (A) by striking paragraph (1); and

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

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

12 **SEC. 725. REPEAL OF REQUIREMENT FOR ANNUAL PER-**  
 13 **SONNEL LEVEL ASSESSMENTS FOR THE IN-**  
 14 **TELLIGENCE COMMUNITY.**

15          Section 506B of the National Security Act of 1947  
 16          (50 U.S.C. 3098) is hereby repealed.

17 **SEC. 726. REPORT ON OUTREACH STRATEGY ADDRESSING**  
 18 **THREATS FROM UNITED STATES ADVER-**  
 19 **SARIES TO THE UNITED STATES TECH-**  
 20 **NOLOGY SECTOR.**

21          (a) REPORT REQUIRED.—Not later than 180 days  
 22          after the date of the enactment of this Act, the Director  
 23          of National Intelligence shall submit to the appropriate  
 24          committees of Congress a report detailing outreach by the  
 25          intelligence community and the Defense Intelligence En-

1 terprise to United States industrial, commercial, scientific,  
2 technical, and academic communities on matters relating  
3 to the efforts of adversaries of the United States to ac-  
4 quire critical United States technology, intellectual prop-  
5 erty, and research and development information.

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

8 (1) A review of the current outreach efforts of  
9 the intelligence community and the Defense Intel-  
10 ligence Enterprise described in subsection (a), in-  
11 cluding the type of information conveyed in the out-  
12 reach.

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

16 (3) An assessment of potential methods for im-  
17 proving the effectiveness of such outreach, including  
18 an assessment of the following:

19 (A) Those critical technologies, infrastruc-  
20 ture, or related supply chains that are at risk  
21 from the efforts of adversaries described in sub-  
22 section (a).

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

1           appropriate, to allow for tailored classified brief-  
2           ings on specific targeted threats.

3           (C) The advisability of partnering with en-  
4           tities of the Federal Government that are not  
5           elements of the intelligence community and rel-  
6           evant regulatory and industry groups described  
7           in subsection (a), to convey key messages across  
8           sectors targeted by United States adversaries.

9           (D) Strategies to assist affected elements  
10          of the communities described in subparagraph  
11          (C) in mitigating, deterring, and protecting  
12          against the broad range of threats from the ef-  
13          forts of adversaries described in subsection (a),  
14          with focus on producing information that en-  
15          ables private entities to justify business deci-  
16          sions related to national security concerns.

17          (E) The advisability of the establishment  
18          of a United States Government-wide task force  
19          to coordinate outreach and activities to combat  
20          the threats from efforts of adversaries described  
21          in subsection (a).

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

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



1 aged to consult with other government agencies, think  
 2 tanks, academia, representatives of the financial industry,  
 3 or such other entities as the Director considers appro-  
 4 priate.

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

8 (e) APPROPRIATE COMMITTEES OF CONGRESS DE-  
 9 FINED.—In this section, the term “appropriate commit-  
 10 tees of Congress” means—

11 (1) the congressional intelligence committees;

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

15 (3) the Committee on Armed Services, Com-  
 16 mittee on Homeland Security, and the Committee on  
 17 Oversight and Government Reform of the House of  
 18 Representatives.

19 **SEC. 727. STUDY ON THE FEASIBILITY OF ENCRYPTING UN-**  
 20 **CLASSIFIED WIRELINE AND WIRELESS TELE-**  
 21 **PHONE CALLS.**

22 (a) STUDY REQUIRED.—Not later than 180 days  
 23 after the date of the enactment of this Act, the Director  
 24 of National Intelligence shall complete a study on the fea-  
 25 sibility of encrypting unclassified wireline and wireless

1 telephone calls between personnel in the intelligence com-  
2 munity.

3 (b) REPORT.—Not later than 90 days after the date  
4 on which the Director completes the study required by  
5 subsection (a), the Director shall submit to the congres-  
6 sional intelligence committees a report on the Director’s  
7 findings with respect to such study.

8 **SEC. 728. MODIFICATION OF REQUIREMENT FOR ANNUAL**  
9 **REPORT ON HIRING AND RETENTION OF MI-**  
10 **NORITY EMPLOYEES.**

11 (a) EXPANSION OF PERIOD OF REPORT.—Subsection  
12 (a) of section 114 of the National Security Act of 1947  
13 (50 U.S.C. 3050) is amended by inserting “and the pre-  
14 ceding 5 fiscal years” after “fiscal year”.

15 (b) CLARIFICATION ON DISAGGREGATION OF  
16 DATA.—Subsection (b) of such section is amended, in the  
17 matter before paragraph (1), by striking “disaggregated  
18 data by category of covered person from each element of  
19 the intelligence community” and inserting “data,  
20 disaggregated by category of covered person and by ele-  
21 ment of the intelligence community,”.

## 1                   **Subtitle C—Other Matters**

### 2   **SEC. 731. TECHNICAL AMENDMENTS RELATED TO THE DE-** 3                   **PARTMENT OF ENERGY.**

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

6                   (1) CLARIFICATION OF FUNCTIONS OF THE AD-  
 7           MINISTRATOR FOR NUCLEAR SECURITY.—Subsection  
 8           (b) of section 3212 of the National Nuclear Security  
 9           Administration Act (50 U.S.C. 2402(b)) is amend-  
 10          ed—

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

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

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

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

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

23           (b) ATOMIC ENERGY DEFENSE ACT.—Section  
 24   4524(b)(2) of the Atomic Energy Defense Act (50 U.S.C.

1 2674(b)(2)) is amended by inserting “Intelligence and”  
 2 after “The Director of”.

3 (c) NATIONAL SECURITY ACT OF 1947.—Paragraph  
 4 (2) of section 106(b) of the National Security Act of 1947  
 5 (50 U.S.C. 3041(b)(2)) is amended—

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

8 (2) by striking subparagraph (F);

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

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

15 **SEC. 732. SECURING ENERGY INFRASTRUCTURE.**

16 (a) DEFINITIONS.—In this section:

17 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
 18 TEES.—The term “appropriate congressional com-  
 19 mittees” means—

20 (A) the congressional intelligence commit-  
 21 tees;

22 (B) the Committee on Homeland Security  
 23 and Governmental Affairs and the Committee  
 24 on Energy and Natural Resources of the Sen-  
 25 ate; and

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

4 (2) COVERED ENTITY.—The term “covered en-  
5 tity” means an entity identified pursuant to section  
6 9(a) of Executive Order 13636 of February 12,  
7 2013 (78 Fed. Reg. 11742), relating to identifica-  
8 tion of critical infrastructure where a cybersecurity  
9 incident could reasonably result in catastrophic re-  
10 gional or national effects on public health or safety,  
11 economic security, or national security.

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

15 (4) INDUSTRIAL CONTROL SYSTEM.—The term  
16 “industrial control system” means an operational  
17 technology used to measure, control, or manage in-  
18 dustrial functions, and includes supervisory control  
19 and data acquisition systems, distributed control  
20 systems, and programmable logic or embedded con-  
21 trollers.

22 (5) NATIONAL LABORATORY.—The term “Na-  
23 tional Laboratory” has the meaning given the term  
24 in section 2 of the Energy Policy Act of 2005 (42  
25 U.S.C. 15801).

1           (6) PROGRAM.—The term “Program” means  
2           the pilot program established under subsection (b).

3           (7) SECRETARY.—The term “Secretary” means  
4           the Secretary of Energy.

5           (8) SECURITY VULNERABILITY.—The term “se-  
6           curity vulnerability” means any attribute of hard-  
7           ware, software, process, or procedure that could en-  
8           able or facilitate the defeat of a security control.

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

14               (1) partnering with covered entities in the en-  
15               ergy sector (including critical component manufac-  
16               turers in the supply chain) that voluntarily partici-  
17               pate in the Program to identify new classes of secu-  
18               rity vulnerabilities of the covered entities; and

19               (2) evaluating technology and standards, in  
20               partnership with covered entities, to isolate and de-  
21               fend industrial control systems of covered entities  
22               from security vulnerabilities and exploits in the most  
23               critical systems of the covered entities, including—

24                       (A) analog and nondigital control systems;

25                       (B) purpose-built control systems; and

1 (C) physical controls.

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

4 (1) ESTABLISHMENT.—The Secretary shall es-  
5 tablish a working group—

6 (A) to evaluate the technology and stand-  
7 ards used in the Program under subsection  
8 (b)(2); and

9 (B) to develop a national cyber-informed  
10 engineering strategy to isolate and defend cov-  
11 ered entities from security vulnerabilities and  
12 exploits in the most critical systems of the cov-  
13 ered entities.

14 (2) MEMBERSHIP.—The working group estab-  
15 lished under paragraph (1) shall be composed of not  
16 fewer than 10 members, to be appointed by the Sec-  
17 retary, at least 1 member of which shall represent  
18 each of the following:

19 (A) The Department of Energy.

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

23 (C)(i) The Department of Homeland Secu-  
24 rity; or

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

3 (D) The North American Electric Reli-  
4 ability Corporation.

5 (E) The Nuclear Regulatory Commission.

6 (F)(i) The Office of the Director of Na-  
7 tional Intelligence; or

8 (ii) the intelligence community.

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

10 (ii) the Assistant Secretary of Defense for  
11 Homeland Security and America's Security Af-  
12 fairs.

13 (H) A State or regional energy agency.

14 (I) A national research body or academic  
15 institution.

16 (J) The National Laboratories.

17 (d) REPORTS ON THE PROGRAM.—

18 (1) INTERIM REPORT.—Not later than 180  
19 days after the date on which funds are first dis-  
20 bursed under the Program, the Secretary shall sub-  
21 mit to the appropriate congressional committees an  
22 interim report that—

23 (A) describes the results of the Program;

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



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

4 (2) FINAL REPORT.—Not later than 2 years  
5 after the date on which funds are first disbursed  
6 under the Program, the Secretary shall submit to  
7 the appropriate congressional committees a final re-  
8 port that—

9 (A) describes the results of the Program;

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

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

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

18 (1) shall be deemed to be voluntarily shared in-  
19 formation;

20 (2) shall be exempt from disclosure under sec-  
21 tion 552 of title 5, United States Code, or any provi-  
22 sion of any State, Tribal, or local freedom of infor-  
23 mation law, open government law, open meetings  
24 law, open records law, sunshine law, or similar law

1 requiring the disclosure of information or records;  
2 and

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

8 (f) PROTECTION FROM LIABILITY.—

9 (1) IN GENERAL.—A cause of action against a  
10 covered entity for engaging in the voluntary activi-  
11 ties authorized under subsection (b)—

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

14 (B) shall be promptly dismissed by the ap-  
15 plicable court.

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

20 (g) NO NEW REGULATORY AUTHORITY FOR FED-  
21 ERAL AGENCIES.—Nothing in this section authorizes the  
22 Secretary or the head of any other department or agency  
23 of the Federal Government to issue new regulations.

24 (h) AUTHORIZATION OF APPROPRIATIONS.—

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

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

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

10 **SEC. 733. SENSE OF CONGRESS ON WIKILEAKS.**

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

15 **SEC. 734. BUG BOUNTY PROGRAMS.**

16           (a) DEFINITIONS.—In this section:

17           (1) APPROPRIATE COMMITTEES OF CON-  
 18           GRESS.—The term “appropriate committees of Con-  
 19           gress” means—

20                   (A) the congressional intelligence commit-  
 21                   tees;

22                   (B) the Committee on Homeland Security  
 23                   and Governmental Affairs and the Committee  
 24                   on Armed Services of the Senate; and

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

4 (2) BUG BOUNTY PROGRAM.—The term “bug  
5 bounty program” means a program under which an  
6 approved computer security specialist or security re-  
7 searcher is temporarily authorized to identify and re-  
8 port vulnerabilities within the information system of  
9 an agency or department of the United States in ex-  
10 change for compensation.

11 (3) INFORMATION SYSTEM.—The term “infor-  
12 mation system” has the meaning given such term in  
13 section 3502 of title 44, United States Code.

14 (b) BUG BOUNTY PROGRAM PLAN.—

15 (1) REQUIREMENT.—Not later than 180 days  
16 after the date of the enactment of this Act, the Sec-  
17 retary of Homeland Security, in consultation with  
18 the Secretary of Defense, shall submit to the appro-  
19 priate committees of Congress a strategic plan for  
20 appropriate agencies and departments of the United  
21 States to implement bug bounty programs.

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

24 (A) an assessment of—

1 (i) the “Hack the Pentagon” pilot  
 2 program carried out by the Department of  
 3 Defense in 2016 and subsequent bug boun-  
 4 ty programs in identifying and reporting  
 5 vulnerabilities within the information sys-  
 6 tems of the Department of Defense; and

7 (ii) private sector bug bounty pro-  
 8 grams, including such programs imple-  
 9 mented by leading technology companies in  
 10 the United States; and

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

14 **SEC. 735. SENSE OF CONGRESS ON CONSIDERATION OF ES-**  
 15 **PIONAGE ACTIVITIES WHEN CONSIDERING**  
 16 **WHETHER OR NOT TO PROVIDE VISAS TO**  
 17 **FOREIGN INDIVIDUALS TO BE ACCREDITED**  
 18 **TO A UNITED NATIONS MISSION IN THE**  
 19 **UNITED STATES.**

20 It is the sense of the Congress that the Secretary of  
 21 State, in considering whether or not to provide a visa to  
 22 a foreign individual to be accredited to a United Nations  
 23 mission in the United States, should consider—

24 (1) known and suspected intelligence activities,  
 25 espionage activities, including activities constituting

1 precursors to espionage, carried out by the indi-  
 2 vidual against the United States, foreign allies of the  
 3 United States, or foreign partners of the United  
 4 States; and

5 (2) the status of an individual as a known or  
 6 suspected intelligence officer for a foreign adversary.

7 **SEC. 736. PUBLIC INTEREST DECLASSIFICATION BOARD.**

8 Section 710(b) of the Public Interest Declassification  
 9 Act of 2000 (Public Law 106–567; 50 U.S.C. 3161 note)  
 10 is amended by striking “December 31, 2018” and insert-  
 11 ing “December 31, 2022”.

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

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

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

19 “(5) The National Intelligence University.”.

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

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

5 (b) ACCEPTANCE OF FACULTY RESEARCH  
 6 GRANTS.—Section 2161 of such title is amended by add-  
 7 ing at the end the following:

8 “(d) ACCEPTANCE OF FACULTY RESEARCH  
 9 GRANTS.—The Secretary of Defense may authorize the  
 10 President of the National Intelligence University to accept  
 11 qualifying research grants in the same manner and to the  
 12 same degree as the President of the National Defense Uni-  
 13 versity under section 2165(e) of this title.”.

14 (c) ADMISSION OF PRIVATE SECTOR CIVILIANS.—

15 (1) IN GENERAL.—Chapter 108 of such title is  
 16 amended by inserting after section 2167a the fol-  
 17 lowing:

18 **“§ 2167b. National Intelligence University: admission**  
 19 **of private sector civilians to receive in-**  
 20 **struction**

21 “(a) AUTHORITY FOR ADMISSION.—(1) The Sec-  
 22 retary of Defense may permit eligible private sector em-  
 23 ployees who work in organizations relevant to national se-  
 24 curity to receive instruction at the National Intelligence  
 25 University in accordance with this section.

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

4       “(3) Upon successful completion of the course of in-  
5   struction in which enrolled, any such private sector em-  
6   ployee may be awarded an appropriate diploma or degree  
7   under section 2161 of this title.

8       “(b) ELIGIBLE PRIVATE SECTOR EMPLOYEES.—(1)  
9   For purposes of this section, an eligible private sector em-  
10   ployee is an individual employed by a private firm that  
11   is engaged in providing to the Department of Defense, the  
12   intelligence community, or other Government departments  
13   or agencies significant and substantial intelligence or de-  
14   fense-related systems, products, or services or whose work  
15   product is relevant to national security policy or strategy.

16       “(2) A private sector employee admitted for instruc-  
17   tion at the National Intelligence University remains eligi-  
18   ble for such instruction only so long as that person re-  
19   mains employed by the same firm, holds appropriate secu-  
20   rity clearances, and complies with any other applicable se-  
21   curity protocols.

22       “(c) ANNUAL CERTIFICATION BY SECRETARY OF DE-  
23   FENSE.—Private sector employees may receive instruction  
24   at the National Intelligence University during any aca-  
25   demic year only if, before the start of that academic year,



1 the Secretary of Defense determines, and certifies to the  
2 Committee on Armed Services of the Senate and the Com-  
3 mittee on Armed Services of the House of Representatives,  
4 that providing instruction to private sector employees  
5 under this section during that year will further the na-  
6 tional security interests of the United States.

7 “(d) PROGRAM REQUIREMENTS.—The Secretary of  
8 Defense shall ensure that—

9 “(1) the curriculum in which private sector em-  
10 ployees may be enrolled under this section is not  
11 readily available through other schools and con-  
12 centrates on national security relevant issues; and

13 “(2) the course offerings at the National Intel-  
14 ligence University are determined by the needs of  
15 the Department of Defense and the intelligence com-  
16 munity.

17 “(e) TUITION.—The President of the National Intel-  
18 ligence University shall charge students enrolled under  
19 this section a rate that—

20 “(1) is at least the rate charged for employees  
21 of the United States outside the Department of De-  
22 fense, less infrastructure costs; and

23 “(2) considers the value to the school and  
24 course of the private sector student.

1       “(f) STANDARDS OF CONDUCT.—While receiving in-  
 2       struction at the National Intelligence University, students  
 3       enrolled under this section, to the extent practicable, are  
 4       subject to the same regulations governing academic per-  
 5       formance, attendance, norms of behavior, and enrollment  
 6       as apply to Government civilian employees receiving in-  
 7       struction at the university.

8       “(g) USE OF FUNDS.—(1) Amounts received by the  
 9       National Intelligence University for instruction of students  
 10      enrolled under this section shall be retained by the univer-  
 11      sity to defray the costs of such instruction.

12      “(2) The source, and the disposition, of such funds  
 13      shall be specifically identified in records of the univer-  
 14      sity.”.

15               (2) CLERICAL AMENDMENT.—The table of sec-  
 16      tions at the beginning of chapter 108 of such title  
 17      is amended by inserting after the item relating to  
 18      section 2167a the following:

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



Calendar No. 494

115<sup>TH</sup> CONGRESS  
2<sup>D</sup> Session

**S. 3153**

**A BILL**

To authorize appropriations for fiscal years 2018 and 2019 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

JUNE 28, 2018

Read twice and placed on the calendar