

116TH CONGRESS
1ST SESSION

S. 245

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

IN THE SENATE OF THE UNITED STATES

JANUARY 28, 2019

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

A BILL

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

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 “Damon Paul Nelson and Matthew Young Pollard Intel-
6 ligence Authorization Act for Fiscal Years 2018 and
7 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.
 Sec. 3. Explanatory statement.

TITLE I—INTELLIGENCE ACTIVITIES

- Sec. 101. Authorization of appropriations.
 Sec. 102. Classified Schedule of Authorizations.
 Sec. 103. 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.
 Sec. 311. Joint Intelligence Community Council.
 Sec. 312. Intelligence community information technology environment.
 Sec. 313. Report on development of secure mobile voice solution for intelligence community.
 Sec. 314. Policy on minimum insider threat standards.
 Sec. 315. Submission of intelligence community policies.
 Sec. 316. Expansion of intelligence community recruitment efforts.

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. Technical modification to the executive schedule.
- Sec. 404. Chief Financial Officer of the Intelligence Community.
- Sec. 405. Chief Information Officer of the Intelligence Community.

Subtitle B—Central Intelligence Agency

- Sec. 411. Central Intelligence Agency subsistence for personnel assigned to austere locations.
- Sec. 412. Expansion of security protective service jurisdiction of the Central Intelligence Agency.
- Sec. 413. Repeal of foreign language proficiency requirement for certain senior level positions in the Central Intelligence Agency.

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

- Sec. 421. Consolidation of Department of Energy Offices of Intelligence and Counterintelligence.
- Sec. 422. Establishment of Energy Infrastructure Security Center.
- Sec. 423. Repeal of Department of Energy Intelligence Executive Committee and budget reporting requirement.

Subtitle D—Other Elements

- Sec. 431. Plan for designation of counterintelligence component of Defense Security Service as an element of intelligence community.
- Sec. 432. Notice not required for private entities.
- Sec. 433. Framework for roles, missions, and functions of Defense Intelligence Agency.
- Sec. 434. Establishment of advisory board for National Reconnaissance Office.
- Sec. 435. Collocation of certain Department of Homeland Security personnel at field locations.

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. Assessment of significant Russian influence campaigns directed at foreign elections and referenda.
- Sec. 506. Foreign counterintelligence and cybersecurity threats to Federal election campaigns.
- Sec. 507. Information sharing with State election officials.
- Sec. 508. Notification of significant foreign cyber intrusions and active measures campaigns directed at elections for Federal offices.
- Sec. 509. 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 background investigations.
- 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 that can be conducted without access to classified information, networks, or facilities.
- Sec. 612. Information sharing program for positions of trust and security clearances.
- 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 Russian Federation.
- 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.
- Sec. 706. Report on outreach strategy addressing threats from United States adversaries to the United States technology sector.
- Sec. 707. Report on Iranian support of proxy forces in Syria and Lebanon.
- Sec. 708. Annual report on Iranian expenditures supporting foreign military and terrorist activities.
- Sec. 709. Expansion of scope of committee to counter active measures and report on establishment of Foreign Malign Influence Center.

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. Review of intelligence community whistleblower matters.
- Sec. 715. Report on role of Director of National Intelligence with respect to certain foreign investments.
- Sec. 716. Report on surveillance by foreign governments against United States telecommunications networks.
- Sec. 717. Biennial report on foreign investment risks.
- Sec. 718. Modification of certain reporting requirement on travel of foreign diplomats.
- Sec. 719. Semiannual reports on investigations of unauthorized disclosures of classified information.

- Sec. 720. Congressional notification of designation of covered intelligence officer as persona non grata.
- Sec. 721. Reports on intelligence community participation in vulnerabilities equities process of Federal Government.
- Sec. 722. Inspectors General reports on classification.
- Sec. 723. Reports on global water insecurity and national security implications and briefing on emerging infectious disease and pandemics.
- Sec. 724. Annual report on memoranda of understanding between elements of intelligence community and other entities of the United States Government regarding significant operational activities or policy.
- Sec. 725. Study on the feasibility of encrypting unclassified wireline and wireless telephone calls.
- Sec. 726. Modification of requirement for annual report on hiring and retention of minority employees.
- Sec. 727. Reports on intelligence community loan repayment and related programs.
- Sec. 728. Repeal of certain reporting requirements.
- Sec. 729. Inspector General of the Intelligence Community report on senior executives of the Office of the Director of National Intelligence.
- Sec. 730. Briefing on Federal Bureau of Investigation offering permanent residence to sources and cooperators.
- Sec. 731. Intelligence assessment of North Korea revenue sources.
- Sec. 732. Report on possible exploitation of virtual currencies by terrorist actors.
- Sec. 733. Inclusion of disciplinary actions in annual report relating to section 702 of the Foreign Intelligence Surveillance Act of 1978.

Subtitle C—Other Matters

- Sec. 741. Public Interest Declassification Board.
- Sec. 742. Securing energy infrastructure.
- Sec. 743. Bug bounty programs.
- Sec. 744. Modification of authorities relating to the National Intelligence University.
- Sec. 745. Technical and clerical amendments to the National Security Act of 1947.
- Sec. 746. Technical amendments related to the Department of Energy.
- Sec. 747. Sense of Congress on notification of certain disclosures of classified information.
- Sec. 748. Sense of Congress on consideration of espionage activities when considering whether or not to provide visas to foreign individuals to be accredited to a United Nations mission in the United States.
- Sec. 749. Sense of Congress on WikiLeaks.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) CONGRESSIONAL INTELLIGENCE COMMIT-
 4 TEES.—The term “congressional intelligence com-
 5 mittees” has the meaning given such term in section

1 3 of the National Security Act of 1947 (50 U.S.C.
2 3003).

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

6 **SEC. 3. EXPLANATORY STATEMENT.**

7 The explanatory statement regarding this Act, print-
8 ed in the Senate section of the Congressional Record, by
9 the Chairman of the Select Committee on Intelligence of
10 the Senate, shall have the same effect with respect to the
11 implementation of this Act as if it were a joint explanatory
12 statement of a committee of conference.

13 **TITLE I—INTELLIGENCE**
14 **ACTIVITIES**

15 **SEC. 101. AUTHORIZATION OF APPROPRIATIONS.**

16 (a) FISCAL YEAR 2019.—Funds are hereby author-
17 ized to be appropriated for fiscal year 2019 for the con-
18 duct of the intelligence and intelligence-related activities
19 of the following elements of the United States Govern-
20 ment:

21 (1) The Office of the Director of National Intel-
22 ligence.

23 (2) The Central Intelligence Agency.

24 (3) The Department of Defense.

25 (4) The Defense Intelligence Agency.

1 (5) The National Security Agency.

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

5 (7) The Coast Guard.

6 (8) The Department of State.

7 (9) The Department of the Treasury.

8 (10) The Department of Energy.

9 (11) The Department of Justice.

10 (12) The Federal Bureau of Investigation.

11 (13) The Drug Enforcement Administration.

12 (14) The National Reconnaissance Office.

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

15 (16) The Department of Homeland Security.

16 (b) FISCAL YEAR 2018.—Funds that were appro-
17 priated for fiscal year 2018 for the conduct of the intel-
18 ligence and intelligence-related activities of the elements
19 of the United States set forth in subsection (a) are hereby
20 authorized.

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

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

1 specified in the classified Schedule of Authorizations pre-
2 pared to accompany this Act.

3 (b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AU-
4 THORIZATIONS.—

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

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

16 (3) LIMITS ON DISCLOSURE.—The President
17 shall not publicly disclose the classified Schedule of
18 Authorizations or any portion of such Schedule ex-
19 cept—

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

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

25 (C) as otherwise required by law.

1 **SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT AC-**
 2 **COUNT.**

3 (a) AUTHORIZATION OF APPROPRIATIONS.—There is
 4 authorized to be appropriated for the Intelligence Commu-
 5 nity Management Account of the Director of National In-
 6 telligence for fiscal year 2019 the sum of \$522,424,000.

7 (b) CLASSIFIED AUTHORIZATION OF APPROPRIA-
 8 TIONS.—In addition to amounts authorized to be appro-
 9 priated for the Intelligence Community Management Ac-
 10 count by subsection (a), there are authorized to be appro-
 11 priated for the Intelligence Community Management Ac-
 12 count for fiscal year 2019 such additional amounts as are
 13 specified in the classified Schedule of Authorizations re-
 14 ferred to in section 102(a).

15 **TITLE II—CENTRAL INTEL-**
 16 **LIGENCE AGENCY RETIRE-**
 17 **MENT AND DISABILITY SYS-**
 18 **TEM**

19 **SEC. 201. AUTHORIZATION OF APPROPRIATIONS.**

20 There is authorized to be appropriated for the Cen-
 21 tral Intelligence Agency Retirement and Disability Fund
 22 \$514,000,000 for fiscal year 2019.

23 **SEC. 202. COMPUTATION OF ANNUITIES FOR EMPLOYEES**
 24 **OF THE CENTRAL INTELLIGENCE AGENCY.**

25 (a) COMPUTATION OF ANNUITIES.—

1 (1) IN GENERAL.—Section 221 of the Central
2 Intelligence Agency Retirement Act (50 U.S.C.
3 2031) is amended—

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

9 (B) in subsection (b)(1)(C)(i), by striking
10 “12-month” and inserting “2-year”;

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

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

16 (E) by redesignating subsections (h), (i),
17 (j), (k), and (l) as subsections (i), (j), (k), (l),
18 and (m), respectively; and

19 (F) by inserting after subsection (g) the
20 following:

21 “(h) CONDITIONAL ELECTION OF INSURABLE INTER-
22 EST SURVIVOR ANNUITY BY PARTICIPANTS MARRIED AT
23 THE TIME OF RETIREMENT.—

24 “(1) AUTHORITY TO MAKE DESIGNATION.—

25 Subject to the rights of former spouses under sub-

1 section (b) and section 222, at the time of retire-
2 ment a married participant found by the Director to
3 be in good health may elect to receive an annuity re-
4 duced in accordance with subsection (f)(1)(B) and
5 designate in writing an individual having an insur-
6 able interest in the participant to receive an annuity
7 under the system after the participant's death, ex-
8 cept that any such election to provide an insurable
9 interest survivor annuity to the participant's spouse
10 shall only be effective if the participant's spouse
11 waives the spousal right to a survivor annuity under
12 this Act. The amount of the annuity shall be equal
13 to 55 percent of the participant's reduced annuity.

14 “(2) REDUCTION IN PARTICIPANT'S ANNUITY.—
15 The annuity payable to the participant making such
16 election shall be reduced by 10 percent of an annuity
17 computed under subsection (a) and by an additional
18 5 percent for each full 5 years the designated indi-
19 vidual is younger than the participant. The total re-
20 duction under this subparagraph may not exceed 40
21 percent.

22 “(3) COMMENCEMENT OF SURVIVOR ANNU-
23 ITY.—The annuity payable to the designated indi-
24 vidual shall begin on the day after the retired partic-

1 ipant dies and terminate on the last day of the
2 month before the designated individual dies.

3 “(4) RECOMPUTATION OF PARTICIPANT’S AN-
4 NUITY ON DEATH OF DESIGNATED INDIVIDUAL.—An
5 annuity that is reduced under this subsection shall,
6 effective the first day of the month following the
7 death of the designated individual, be recomputed
8 and paid as if the annuity had not been so re-
9 duced.”.

10 (2) CONFORMING AMENDMENTS.—

11 (A) CENTRAL INTELLIGENCE AGENCY RE-
12 TIREMENT ACT.—The Central Intelligence
13 Agency Retirement Act (50 U.S.C. 2001 et
14 seq.) is amended—

15 (i) in section 232(b)(1) (50 U.S.C.
16 2052(b)(1)), by striking “221(h),” and in-
17 serting “221(i),”; and

18 (ii) in section 252(h)(4) (50 U.S.C.
19 2082(h)(4)), by striking “221(k)” and in-
20 serting “221(l)”.

21 (B) CENTRAL INTELLIGENCE AGENCY ACT
22 OF 1949.—Subsection (a) of section 14 of the
23 Central Intelligence Agency Act of 1949 (50
24 U.S.C. 3514(a)) is amended by striking

1 “221(h)(2), 221(i), 221(l),” and inserting
2 “221(i)(2), 221(j), 221(m),”.

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

8 (c) PRIOR SERVICE CREDIT.—Subparagraph (A) of
9 section 252(b)(3) of the Central Intelligence Agency Re-
10 tirement Act (50 U.S.C. 2082(b)(3)(A)) is amended by
11 striking “October 1, 1990” both places that term appears
12 and inserting “March 31, 1991”.

13 (d) REEMPLOYMENT COMPENSATION.—Section 273
14 of the Central Intelligence Agency Retirement Act (50
15 U.S.C. 2113) is amended—

16 (1) by redesignating subsections (b) and (c) as
17 subsections (c) and (d), respectively; and

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

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

24 (e) EFFECTIVE DATE AND APPLICATION.—The
25 amendments made by subsection (a)(1)(A) and subsection

1 (c) shall take effect as if enacted on October 28, 2009,
2 and shall apply to computations or participants, respec-
3 tively, as of such date.

4 **TITLE III—GENERAL INTEL-**
5 **LIGENCE COMMUNITY MAT-**
6 **TERS**

7 **SEC. 301. RESTRICTION ON CONDUCT OF INTELLIGENCE**
8 **ACTIVITIES.**

9 The authorization of appropriations by this Act shall
10 not be deemed to constitute authority for the conduct of
11 any intelligence activity which is not otherwise authorized
12 by the Constitution or the laws of the United States.

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

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

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

6 Section 113B of the National Security Act of 1947
7 (50 U.S.C. 3049a) is amended—

8 (1) by amending subsection (a) to read as fol-
9 lows:

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

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

19 “(A) establish higher minimum rates of
20 pay; and

21 “(B) make corresponding increases in all
22 rates of pay of the pay range for each grade or
23 level, subject to subsection (b) or (c), as appli-
24 cable.

25 “(2) TREATMENT.—The special rate supple-
26 ments resulting from the establishment of higher

1 rates under paragraph (1) shall be basic pay for the
2 same or similar purposes as those specified in sec-
3 tion 5305(j) of title 5, United States Code.”;

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

6 (3) by inserting after subsection (a) the fol-
7 lowing:

8 “(b) SPECIAL RATES OF PAY FOR CYBER POSI-
9 TIONS.—

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

13 “(A) not to exceed the rate of basic pay
14 payable for level II of the Executive Schedule
15 under section 5313 of title 5, United States
16 Code, if the Director certifies to the Under Sec-
17 retary of Defense for Intelligence, in consulta-
18 tion with the Under Secretary of Defense for
19 Personnel and Readiness, that the rate of pay
20 is for positions that perform functions that exe-
21 cute the cyber mission of the Agency; or

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

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

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

10 “(A) any allowance, differential, bonus,
11 award, or other similar cash payment in addi-
12 tion to basic pay that is authorized under title
13 10, United States Code, (or any other applica-
14 ble law in addition to title 5 of such Code, ex-
15 cluding the Fair Labor Standards Act of 1938
16 (29 U.S.C. 201 et seq.)) shall also be counted
17 as part of aggregate compensation; and

18 “(B) aggregate compensation may not ex-
19 ceed the rate established for the Vice President
20 of the United States under section 104 of title
21 3, United States Code.

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

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

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

13 (5) in subsection (d), as redesignated by para-
14 graph (2), by inserting “or (b)” after “by subsection
15 (a)”;

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

18 (A) in paragraph (1), by striking “Not
19 later than 90 days after the date of the enact-
20 ment of the Intelligence Authorization Act for
21 Fiscal Year 2017” and inserting “Not later
22 than 90 days after the date of the enactment of
23 the Damon Paul Nelson and Matthew Young
24 Pollard Intelligence Authorization Act for Fis-
25 cal Years 2018 and 2019”; and

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

3 **SEC. 304. MODIFICATION OF APPOINTMENT OF CHIEF IN-**
4 **FORMATION OFFICER OF THE INTELLIGENCE**
5 **COMMUNITY.**

6 Section 103G(a) of the National Security Act of 1947
7 (50 U.S.C. 3032(a)) is amended by striking “President”
8 and inserting “Director”.

9 **SEC. 305. DIRECTOR OF NATIONAL INTELLIGENCE REVIEW**
10 **OF PLACEMENT OF POSITIONS WITHIN THE**
11 **INTELLIGENCE COMMUNITY ON THE EXECU-**
12 **TIVE SCHEDULE.**

13 (a) REVIEW.—The Director of National Intelligence,
14 in coordination with the Director of the Office of Per-
15 sonnel Management, shall conduct a review of positions
16 within the intelligence community regarding the placement
17 of such positions on the Executive Schedule under sub-
18 chapter II of chapter 53 of title 5, United States Code.
19 In carrying out such review, the Director of National In-
20 telligence, in coordination with the Director of the Office
21 of Personnel Management, shall determine—

22 (1) the standards under which such review will
23 be conducted;

24 (2) which positions should or should not be on
25 the Executive Schedule; and

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

4 (b) REPORT.—Not later than 60 days after the date
5 on which the review under subsection (a) is completed, the
6 Director of National Intelligence shall submit to the con-
7 gressional intelligence committees, the Committee on
8 Homeland Security and Governmental Affairs of the Sen-
9 ate, and the Committee on Oversight and Reform of the
10 House of Representatives an unredacted report describing
11 the standards by which the review was conducted and the
12 outcome of the review.

13 **SEC. 306. SUPPLY CHAIN AND COUNTERINTELLIGENCE**
14 **RISK MANAGEMENT TASK FORCE.**

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 Armed Services and the
20 Committee on Homeland Security and Governmental
21 Affairs of the Senate.

22 (3) The Committee on Armed Services, the
23 Committee on Homeland Security, and the Com-
24 mittee on Oversight and Reform of the House of
25 Representatives.

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

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

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

13 (2) a representative of the General Services Ad-
14 ministration;

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

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

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

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

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

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

6 (e) ANNUAL REPORT.—The Supply Chain and Coun-
7 terintelligence Risk Management Task Force established
8 under subsection (b) shall submit to the appropriate con-
9 gressional committees an annual report that describes the
10 activities of the Task Force during the previous year, in-
11 cluding identification of the supply chain and counterintel-
12 ligence risks shared with the acquisition community of the
13 United States Government by the intelligence community.

14 **SEC. 307. CONSIDERATION OF ADVERSARIAL TELE-**
15 **COMMUNICATIONS AND CYBERSECURITY IN-**
16 **FRAStructure WHEN SHARING INTEL-**
17 **LIGENCE WITH FOREIGN GOVERNMENTS AND**
18 **ENTITIES.**

19 Whenever the head of an element of the intelligence
20 community enters into an intelligence sharing agreement
21 with a foreign government or any other foreign entity, the
22 head of the element shall consider the pervasiveness of
23 telecommunications and cybersecurity infrastructure,
24 equipment, and services provided by adversaries of the
25 United States, particularly China and Russia, or entities

1 of such adversaries in the country or region of the foreign
2 government or other foreign entity entering into the agree-
3 ment.

4 **SEC. 308. CYBER PROTECTION SUPPORT FOR THE PER-**
5 **SONNEL OF THE INTELLIGENCE COMMUNITY**
6 **IN POSITIONS HIGHLY VULNERABLE TO**
7 **CYBER ATTACK.**

8 (a) DEFINITIONS.—In this section:

9 (1) PERSONAL ACCOUNTS.—The term “personal
10 accounts” means accounts for online and tele-
11 communications services, including telephone, resi-
12 dential internet access, email, text and multimedia
13 messaging, cloud computing, social media, health
14 care, and financial services, used by personnel of the
15 intelligence community outside of the scope of their
16 employment with elements of the intelligence com-
17 munity.

18 (2) PERSONAL TECHNOLOGY DEVICES.—The
19 term “personal technology devices” means tech-
20 nology devices used by personnel of the intelligence
21 community outside of the scope of their employment
22 with elements of the intelligence community, includ-
23 ing networks to which such devices connect.

24 (b) AUTHORITY TO PROVIDE CYBER PROTECTION
25 SUPPORT.—

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

6 (2) AT-RISK PERSONNEL.—The personnel de-
7 scribed in this paragraph are personnel of the intel-
8 ligence community—

9 (A) who the Director determines to be
10 highly vulnerable to cyber attacks and hostile
11 information collection activities because of the
12 positions occupied by such personnel in the in-
13 telligence community; and

14 (B) whose personal technology devices or
15 personal accounts are highly vulnerable to cyber
16 attacks and hostile information collection activi-
17 ties.

18 (c) NATURE OF CYBER PROTECTION SUPPORT.—
19 Subject to the availability of resources, the cyber protec-
20 tion support provided to personnel under subsection (b)
21 may include training, advice, assistance, and other services
22 relating to cyber attacks and hostile information collection
23 activities.

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

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

4 (2) to authorize cyber protection support for
5 senior intelligence community personnel using per-
6 sonal devices, networks, and personal accounts in an
7 official capacity.

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

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

15 (2) guidance for the use of cyber protection
16 support and tracking of support requests for per-
17 sonnel receiving cyber protection support under sub-
18 section (b).

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

21 (a) MODIFICATION OF EFFECTIVE DATE.—Sub-
22 section (f) of section 309 of the Intelligence Authorization
23 Act for Fiscal Year 2012 (Public Law 112–87; 50 U.S.C.
24 3329 note) is amended by striking “the date that is 180
25 days after”.

1 (b) REPEAL OF SUNSET.—Such section is amended
2 by striking subsection (g).

3 (c) REPORTS.—Such section, as amended by sub-
4 section (b), is further amended—

5 (1) by redesignating subsection (f), as amended
6 by subsection (a), as subsection (g); and

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

9 “(f) ANNUAL REPORTS.—

10 “(1) IN GENERAL.—Except as provided in para-
11 graph (2), not later than 180 days after the date of
12 the enactment of the Damon Paul Nelson and Mat-
13 thew Young Pollard Intelligence Authorization Act
14 for Fiscal Years 2018 and 2019 and not less fre-
15 quently than once each calendar year thereafter, the
16 Director of National Intelligence shall, in consulta-
17 tion with each head of a covered agency, submit to
18 the congressional intelligence committees (as defined
19 in section 3 of the National Security Act of 1947
20 (50 U.S.C. 3003)), a report that details the deter-
21 minations and notifications made under subsection
22 (c) during the most recently completed calendar
23 year.

24 “(2) INITIAL REPORT.—The first report sub-
25 mitted under paragraph (1) shall detail all the deter-

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

6 **SEC. 311. JOINT INTELLIGENCE COMMUNITY COUNCIL.**

7 (a) MEETINGS.—Section 101A(d) of the National Se-
8 curity Act of 1947 (50 U.S.C. 3022(d)) is amended—

9 (1) by striking “regular”; and

10 (2) by inserting “as the Director considers ap-
11 propriate” after “Council”.

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

14 (1) IN GENERAL.—No later than 180 days after
15 the date of the enactment of this Act, the Director
16 of National Intelligence, in coordination with the Ex-
17 ecutive Office of the President and members of the
18 Joint Intelligence Community Council, shall submit
19 to the congressional intelligence committees a report
20 on the function and utility of the Joint Intelligence
21 Community Council.

22 (2) CONTENTS.—The report required by para-
23 graph (1) shall include the following:

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

4 (B) A description of the effect and accom-
5 plishments of the Council.

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

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

13 (E) Such other matters relating to the
14 function and utility of the Council as the Direc-
15 tor considers appropriate.

16 (3) FORM.—The report submitted under para-
17 graph (1) shall be submitted in unclassified form,
18 but may include a classified annex.

19 **SEC. 312. INTELLIGENCE COMMUNITY INFORMATION TECH-**
20 **NOLOGY ENVIRONMENT.**

21 (a) DEFINITIONS.—In this section:

22 (1) CORE SERVICE.—The term “core service”
23 means a capability that is available to multiple ele-
24 ments of the intelligence community and required

1 for consistent operation of the intelligence commu-
2 nity information technology environment.

3 (2) INTELLIGENCE COMMUNITY INFORMATION
4 TECHNOLOGY ENVIRONMENT.—The term “intel-
5 ligence community information technology environ-
6 ment” means all of the information technology serv-
7 ices across the intelligence community, including the
8 data sharing and protection environment across mul-
9 tiple classification domains.

10 (b) ROLES AND RESPONSIBILITIES.—

11 (1) DIRECTOR OF NATIONAL INTELLIGENCE.—
12 The Director of National Intelligence shall be re-
13 sponsible for coordinating the performance by ele-
14 ments of the intelligence community of the intel-
15 ligence community information technology environ-
16 ment, including each of the following:

17 (A) Ensuring compliance with all applica-
18 ble environment rules and regulations of such
19 environment.

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

22 (C) Documenting standards and practices
23 of such environment.

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

1 disagreements arising out of the implementa-
2 tion of such environment.

3 (E) Delegating responsibilities to the ele-
4 ments of the intelligence community and car-
5 rying out such other responsibilities as are nec-
6 essary for the effective implementation of such
7 environment.

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

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

12 (B) providing the Director with informa-
13 tion requested and required to fulfill the re-
14 sponsibilities of the Director under paragraph
15 (1).

16 (3) USE OF CORE SERVICES.—

17 (A) IN GENERAL.—Except as provided in
18 subparagraph (B), each element of the intel-
19 ligence community shall use core services when
20 such services are available.

21 (B) EXCEPTION.—The Director of Na-
22 tional Intelligence may provide for a written ex-
23 ception to the requirement under subparagraph
24 (A) if the Director determines there is a com-

1 pelling financial or mission need for such excep-
2 tion.

3 (c) MANAGEMENT ACCOUNTABILITY.—Not later than
4 90 days after the date of the enactment of this Act, the
5 Director of National Intelligence shall designate and main-
6 tain one or more accountable executives of the intelligence
7 community information technology environment to be re-
8 sponsible for—

9 (1) management, financial control, and integra-
10 tion of such environment;

11 (2) overseeing the performance of each core
12 service, including establishing measurable service re-
13 quirements and schedules;

14 (3) to the degree feasible, ensuring testing of
15 each core service of such environment, including
16 testing by the intended users, to evaluate perform-
17 ance against measurable service requirements and to
18 ensure the capability meets user requirements; and

19 (4) coordinate transition or restructuring ef-
20 forts of such environment, including phaseout of leg-
21 acy systems.

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

1 plan for the intelligence community information tech-
2 nology environment.

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

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

11 (A) key performance parameters; and

12 (B) an assessment of current, measured
13 performance.

14 (2) Implementation milestones for the intel-
15 ligence community information technology environ-
16 ment, including each of the following:

17 (A) A schedule for expected deliveries of
18 core service capabilities during each of the fol-
19 lowing phases:

20 (i) Concept refinement and technology
21 maturity demonstration.

22 (ii) Development, integration, and
23 demonstration.

24 (iii) Production, deployment, and
25 sustainment.

1 (iv) System retirement.

2 (B) Dependencies of such core service ca-
3 pabilities.

4 (C) Plans for the transition or restruc-
5 turing necessary to incorporate core service ca-
6 pabilities.

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

9 (3) Such other matters as the Director deter-
10 mines appropriate.

11 (f) BUSINESS PLAN.—Not later than 180 days after
12 the date of the enactment of this Act, and during each
13 of the second and fourth fiscal quarters thereafter, the Di-
14 rector of National Intelligence shall submit to the congres-
15 sional intelligence committees a business plan that in-
16 cludes each of the following:

17 (1) A systematic approach to identify core serv-
18 ice funding requests for the intelligence community
19 information technology environment within the pro-
20 posed budget, including multiyear plans to imple-
21 ment the long-term roadmap required by subsection
22 (e).

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

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

4 (3) A uniform effort by which each element of
5 the intelligence community shall identify transition
6 and restructuring costs for new, existing, and retir-
7 ing services of the intelligence community informa-
8 tion technology environment, as well as services of
9 such environment that have changed designations as
10 a core service.

11 (g) QUARTERLY PRESENTATIONS.—Beginning not
12 later than 180 days after the date of the enactment of
13 this Act, the Director of National Intelligence shall provide
14 to the congressional intelligence committees quarterly up-
15 dates regarding ongoing implementation of the intelligence
16 community information technology environment as com-
17 pared to the requirements in the most recently submitted
18 security plan required by subsection (d), long-term road-
19 map required by subsection (e), and business plan re-
20 quired by subsection (f).

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

1 tives or strategies related to or impacting such environ-
2 ment, and changes or deficiencies in the execution of the
3 security plan required by subsection (d), long-term road-
4 map required by subsection (e), and business plan re-
5 quired by subsection (f).

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

8 **SEC. 313. REPORT ON DEVELOPMENT OF SECURE MOBILE**
9 **VOICE SOLUTION FOR INTELLIGENCE COM-**
10 **MUNITY.**

11 (a) IN GENERAL.—Not later than 180 days after the
12 date of the enactment of this Act, the Director of National
13 Intelligence, in coordination with the Director of the Cen-
14 tral Intelligence Agency and the Director of the National
15 Security Agency, shall submit to the congressional intel-
16 ligence committees a classified report on the feasibility,
17 desirability, cost, and required schedule associated with
18 the implementation of a secure mobile voice solution for
19 the intelligence community.

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

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

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

1 fied voice communications that operates on commer-
2 cial mobile networks in a secure manner and identi-
3 fying the accompanying security risks to such net-
4 works.

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

10 **SEC. 314. POLICY ON MINIMUM INSIDER THREAT STAND-**
11 **ARDS.**

12 (a) **POLICY REQUIRED.**—Not later than 60 days after
13 the date of the enactment of this Act, the Director of Na-
14 tional Intelligence shall establish a policy for minimum in-
15 sider threat standards that is consistent with the National
16 Insider Threat Policy and Minimum Standards for Execu-
17 tive Branch Insider Threat Programs.

18 (b) **IMPLEMENTATION.**—Not later than 180 days
19 after the date of the enactment of this Act, the head of
20 each element of the intelligence community shall imple-
21 ment the policy established under subsection (a).

22 **SEC. 315. SUBMISSION OF INTELLIGENCE COMMUNITY**
23 **POLICIES.**

24 (a) **DEFINITIONS.**—In this section:

1 (1) ELECTRONIC REPOSITORY.—The term
2 “electronic repository” means the electronic distribu-
3 tion mechanism, in use as of the date of the enact-
4 ment of this Act, or any successor electronic dis-
5 tribution mechanism, by which the Director of Na-
6 tional Intelligence submits to the congressional intel-
7 ligence committees information.

8 (2) POLICY.—The term “policy”, with respect
9 to the intelligence community, includes unclassified
10 or classified—

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

13 (B) executive correspondence of the Direc-
14 tor of National Intelligence; and

15 (C) any equivalent successor policy instru-
16 ments.

17 (b) SUBMISSION OF POLICIES.—

18 (1) CURRENT POLICY.—Not later than 180
19 days after the date of the enactment of this Act, the
20 Director of National Intelligence shall submit to the
21 congressional intelligence committees using the elec-
22 tronic repository all nonpublicly available policies
23 issued by the Director of National Intelligence for
24 the intelligence community that are in effect as of
25 the date of the submission.

1 (2) CONTINUOUS UPDATES.—Not later than 15
2 days after the date on which the Director of Na-
3 tional Intelligence issues, modifies, or rescinds a pol-
4 icy of the intelligence community, the Director
5 shall—

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

9 (B) update the electronic repository with
10 respect to such addition, modification, or re-
11 moval.

12 **SEC. 316. EXPANSION OF INTELLIGENCE COMMUNITY RE-**
13 **CRUITMENT EFFORTS.**

14 In order to further increase the diversity of the intel-
15 ligence community workforce, not later than 90 days after
16 the date of the enactment of this Act, the Director of Na-
17 tional Intelligence, in consultation with heads of elements
18 of the Intelligence Community, shall create, implement,
19 and submit to the congressional intelligence committees a
20 written plan to ensure that rural and underrepresented re-
21 gions are more fully and consistently represented in such
22 elements' employment recruitment efforts. Upon receipt of
23 the plan, the congressional committees shall have 60 days
24 to submit comments to the Director of National Intel-
25 ligence before such plan shall be implemented.

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 Damon Paul Nelson and Matthew Young Pol-
12 lard Intelligence Authorization Act for Fiscal Years 2018
13 and 2019, each individual designated as the program man-
14 ager shall be appointed by the Director of National Intel-
15 ligence.”.

16 **SEC. 403. TECHNICAL MODIFICATION TO THE EXECUTIVE**
17 **SCHEDULE.**

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

20 “Director of the National Counterintelligence and Se-
21 curity Center.”.

22 **SEC. 404. CHIEF FINANCIAL OFFICER OF THE INTEL-**
23 **LIGENCE COMMUNITY.**

24 Section 103I(a) of the National Security Act of 1947
25 (50 U.S.C. 3034(a)) is amended by adding at the end the

1 following new sentence: “The Chief Financial Officer shall
2 report directly to the Director of National Intelligence.”.

3 **SEC. 405. CHIEF INFORMATION OFFICER OF THE INTEL-**
4 **LIGENCE COMMUNITY.**

5 Section 103G(a) of the National Security Act of 1947
6 (50 U.S.C. 3032(a)) is amended by adding at the end the
7 following new sentence: “The Chief Information Officer
8 shall report directly to the Director of National Intel-
9 ligence.”.

10 **Subtitle B—Central Intelligence**
11 **Agency**

12 **SEC. 411. CENTRAL INTELLIGENCE AGENCY SUBSISTENCE**
13 **FOR PERSONNEL ASSIGNED TO AUSTERE LO-**
14 **CATIONS.**

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

17 (1) in paragraph (1), by striking “(50 U.S.C.
18 403–4a).,” and inserting “(50 U.S.C. 403–4a),”;

19 (2) in paragraph (6), by striking “and” at the
20 end;

21 (3) in paragraph (7), by striking the period at
22 the end and inserting “; and”; and

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

1 “(8) Upon the approval of the Director, pro-
 2 vide, during any fiscal year, with or without reim-
 3 bursement, subsistence to any personnel assigned to
 4 an overseas location designated by the Agency as an
 5 austere location.”.

6 **SEC. 412. EXPANSION OF SECURITY PROTECTIVE SERVICE**
 7 **JURISDICTION OF THE CENTRAL INTEL-**
 8 **LIGENCE AGENCY.**

9 Subsection (a) of section 15 of the Central Intel-
 10 ligence Act of 1949 (50 U.S.C. 3515(a)) is amended—

11 (1) in the subsection heading, by striking “Po-
 12 LICEMEN” and inserting “POLICE OFFICERS”; and

13 (2) in paragraph (1)—

14 (A) in subparagraph (B), by striking “500
 15 feet;” and inserting “500 yards;”; and

16 (B) in subparagraph (D), by striking “500
 17 feet.” and inserting “500 yards.”.

18 **SEC. 413. REPEAL OF FOREIGN LANGUAGE PROFICIENCY**
 19 **REQUIREMENT FOR CERTAIN SENIOR LEVEL**
 20 **POSITIONS IN THE CENTRAL INTELLIGENCE**
 21 **AGENCY.**

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

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

5 **Subtitle C—Office of Intelligence**
6 **and Counterintelligence of De-**
7 **partment of Energy**

8 **SEC. 421. CONSOLIDATION OF DEPARTMENT OF ENERGY**
9 **OFFICES OF INTELLIGENCE AND COUNTER-**
10 **INTELLIGENCE.**

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

14 “OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE
15 “SEC. 215. (a) DEFINITIONS.—In this section, the
16 terms ‘intelligence community’ and ‘National Intelligence
17 Program’ have the meanings given such terms in section
18 3 of the National Security Act of 1947 (50 U.S.C. 3003).

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

22 “(c) DIRECTOR.—(1) The head of the Office shall be
23 the Director of the Office of Intelligence and Counterintel-
24 ligence, who shall be an employee in the Senior Executive
25 Service, the Senior Intelligence Service, the Senior Na-
26 tional Intelligence Service, or any other Service that the

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

4 “(2) The Secretary shall select an individual to serve
5 as the Director from among individuals who have substan-
6 tial expertise in matters relating to the intelligence com-
7 munity, including foreign intelligence and counterintel-
8 ligence.

9 “(d) DUTIES.—(1) Subject to the authority, direc-
10 tion, and control of the Secretary, the Director shall per-
11 form such duties and exercise such powers as the Sec-
12 retary may prescribe.

13 “(2) The Director shall be responsible for estab-
14 lishing policy for intelligence and counterintelligence pro-
15 grams and activities at the Department.”.

16 (b) CONFORMING REPEAL.—Section 216 of the De-
17 partment of Energy Organization Act (42 U.S.C. 7144c)
18 is hereby repealed.

19 (c) CLERICAL AMENDMENT.—The table of contents
20 at the beginning of the Department of Energy Organiza-
21 tion Act is amended by striking the items relating to sec-
22 tions 215 and 216 and inserting the following new item:

“215. Office of Intelligence and Counterintelligence.”.

1 **SEC. 422. ESTABLISHMENT OF ENERGY INFRASTRUCTURE**
2 **SECURITY CENTER.**

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

6 “(e) ENERGY INFRASTRUCTURE SECURITY CEN-
7 TER.—(1)(A) The President shall establish an Energy In-
8 frastructure Security Center, taking into account all ap-
9 propriate government tools to analyze and disseminate in-
10 telligence relating to the security of the energy infrastruc-
11 ture of the United States.

12 “(B) The Secretary shall appoint the head of the En-
13 ergy Infrastructure Security Center.

14 “(C) The Energy Infrastructure Security Center shall
15 be located within the Office of Intelligence and Counter-
16 intelligence.

17 “(2) In establishing the Energy Infrastructure Secu-
18 rity Center, the Director of the Office of Intelligence and
19 Counterintelligence shall address the following missions
20 and objectives to coordinate and disseminate intelligence
21 relating to the security of the energy infrastructure of the
22 United States:

23 “(A) Establishing a primary organization with-
24 in the United States Government for analyzing and
25 integrating all intelligence possessed or acquired by

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

3 “(B) Ensuring that appropriate departments
4 and agencies have full access to and receive intel-
5 ligence support needed to execute the plans or activi-
6 ties of the agencies, and perform independent, alter-
7 native analyses.

8 “(C) Establishing a central repository on known
9 and suspected foreign threats to the energy infra-
10 structure of the United States, including with re-
11 spect to any individuals, groups, or entities engaged
12 in activities targeting such infrastructure, and the
13 goals, strategies, capabilities, and networks of such
14 individuals, groups, or entities.

15 “(D) Disseminating intelligence information re-
16 lating to the security of the energy infrastructure of
17 the United States, including threats and analyses, to
18 the President, to the appropriate departments and
19 agencies, and to the appropriate committees of Con-
20 gress.

21 “(3) The President may waive the requirements of
22 this subsection, and any parts thereof, if the President de-
23 termines that such requirements do not materially improve
24 the ability of the United States Government to prevent
25 and halt attacks against the energy infrastructure of the

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

4 “(4) If the President decides not to exercise the waiv-
 5 er authority granted by paragraph (3), the President shall
 6 submit to Congress from time to time updates and plans
 7 regarding the establishment of an Energy Infrastructure
 8 Security Center.”.

9 **SEC. 423. REPEAL OF DEPARTMENT OF ENERGY INTEL-**
 10 **LIGENCE EXECUTIVE COMMITTEE AND BUDG-**
 11 **ET REPORTING REQUIREMENT.**

12 Section 214 of the Department of Energy Organiza-
 13 tion Act (42 U.S.C. 7144a) is amended—

14 (1) by striking “(a) DUTY OF SECRETARY.—”;

15 and

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

17 **Subtitle D—Other Elements**

18 **SEC. 431. PLAN FOR DESIGNATION OF COUNTERINTEL-**
 19 **LIGENCE COMPONENT OF DEFENSE SECU-**
 20 **RITY SERVICE AS AN ELEMENT OF INTEL-**
 21 **LIGENCE COMMUNITY.**

22 Not later than 90 days after the date of the enact-
 23 ment of this Act, the Director of National Intelligence and
 24 Under Secretary of Defense for Intelligence, in coordina-
 25 tion with the Director of the National Counterintelligence

1 and Security Center, shall submit to the congressional in-
2 telligence committees, the Committee on Armed Services
3 of the Senate, and the Committee on Armed Services of
4 the House of Representatives a plan to designate the coun-
5 terintelligence component of the Defense Security Service
6 of the Department of Defense as an element of the intel-
7 ligence community by not later than January 1, 2019.

8 Such plan shall—

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

15 (2) not address the personnel security functions
16 of the Defense Security Service.

17 **SEC. 432. NOTICE NOT REQUIRED FOR PRIVATE ENTITIES.**

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

20 (1) by redesignating subsection (j) as sub-
21 section (k); and

22 (2) by inserting after subsection (i) the fol-
23 lowing:

24 “(j) **RULE OF CONSTRUCTION.**—Nothing in this sec-
25 tion shall be construed to require the Secretary to provide

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

3 **SEC. 433. FRAMEWORK FOR ROLES, MISSIONS, AND FUNC-**
4 **TIONS OF DEFENSE INTELLIGENCE AGENCY.**

5 (a) IN GENERAL.—The Director of National Intel-
6 ligence and the Secretary of Defense shall jointly establish
7 a framework to ensure the appropriate balance of re-
8 sources for the roles, missions, and functions of the De-
9 fense Intelligence Agency in its capacity as an element of
10 the intelligence community and as a combat support agen-
11 cy. The framework shall include supporting processes to
12 provide for the consistent and regular reevaluation of the
13 responsibilities and resources of the Defense Intelligence
14 Agency to prevent imbalanced priorities, insufficient or
15 misaligned resources, and the unauthorized expansion of
16 mission parameters.

17 (b) MATTERS FOR INCLUSION.—The framework re-
18 quired under subsection (a) shall include each of the fol-
19 lowing:

20 (1) A lexicon providing for consistent defini-
21 tions of relevant terms used by both the intelligence
22 community and the Department of Defense, includ-
23 ing each of the following:

24 (A) Defense intelligence enterprise.

25 (B) Enterprise manager.

- 1 (C) Executive agent.
- 2 (D) Function.
- 3 (E) Functional manager.
- 4 (F) Mission.
- 5 (G) Mission manager.
- 6 (H) Responsibility.
- 7 (I) Role.
- 8 (J) Service of common concern.

9 (2) An assessment of the necessity of maintain-
10 ing separate designations for the intelligence com-
11 munity and the Department of Defense for intel-
12 ligence functional or enterprise management con-
13 structs.

14 (3) A repeatable process for evaluating the ad-
15 dition, transfer, or elimination of defense intelligence
16 missions, roles, and functions, currently performed
17 or to be performed in the future by the Defense In-
18 telligence Agency, which includes each of the fol-
19 lowing:

20 (A) A justification for the addition, trans-
21 fer, or elimination of a mission, role, or func-
22 tion.

23 (B) The identification of which, if any, ele-
24 ment of the Federal Government performs the
25 considered mission, role, or function.

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

3 (i) an assessment of the most appro-
4 priate agency or element to perform such
5 mission, role, or function, taking into ac-
6 count the resource profiles, scope of re-
7 sponsibilities, primary customers, and ex-
8 isting infrastructure necessary to support
9 such mission, role, or function; and

10 (ii) a determination of the appropriate
11 resource profile and an identification of the
12 projected resources needed and the pro-
13 posed source of such resources over the fu-
14 ture-years defense program, to be provided
15 in writing to any elements of the intel-
16 ligence community or the Department of
17 Defense affected by the assumption, trans-
18 fer, or elimination of any mission, role, or
19 function.

20 (D) In the case of any mission, role, or
21 function proposed to be assumed, transferred,
22 or eliminated, an assessment, which shall be
23 completed jointly by the heads of each element
24 affected by such assumption, transfer, or elimi-
25 nation, of the risks that would be assumed by

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

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

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

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

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

20 **SEC. 434. ESTABLISHMENT OF ADVISORY BOARD FOR NA-**
21 **TIONAL RECONNAISSANCE OFFICE.**

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

25 “(d) ADVISORY BOARD.—

1 “(1) ESTABLISHMENT.—There is established in
2 the National Reconnaissance Office an advisory
3 board (in this section referred to as the ‘Board’).

4 “(2) DUTIES.—The Board shall—

5 “(A) study matters relating to the mission
6 of the National Reconnaissance Office, includ-
7 ing with respect to promoting innovation, com-
8 petition, and resilience in space, overhead re-
9 connaissance, acquisition, and other matters;
10 and

11 “(B) advise and report directly to the Di-
12 rector with respect to such matters.

13 “(3) MEMBERS.—

14 “(A) NUMBER AND APPOINTMENT.—

15 “(i) IN GENERAL.—The Board shall
16 be composed of 5 members appointed by
17 the Director from among individuals with
18 demonstrated academic, government, busi-
19 ness, or other expertise relevant to the mis-
20 sion and functions of the National Recon-
21 naissance Office.

22 “(ii) NOTIFICATION.—Not later than
23 30 days after the date on which the Direc-
24 tor appoints a member to the Board, the
25 Director shall notify the congressional in-

1 intelligence committees and the congressional
2 defense committees (as defined in section
3 101(a) of title 10, United States Code) of
4 such appointment.

5 “(B) TERMS.—Each member shall be ap-
6 pointed for a term of 2 years. Except as pro-
7 vided by subparagraph (C), a member may not
8 serve more than 3 terms.

9 “(C) VACANCY.—Any member appointed to
10 fill a vacancy occurring before the expiration of
11 the term for which the member’s predecessor
12 was appointed shall be appointed only for the
13 remainder of that term. A member may serve
14 after the expiration of that member’s term until
15 a successor has taken office.

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

19 “(E) TRAVEL EXPENSES.—Each member
20 shall receive travel expenses, including per diem
21 in lieu of subsistence, in accordance with appli-
22 cable provisions under subchapter I of chapter
23 57 of title 5, United States Code.

24 “(F) EXECUTIVE SECRETARY.—The Direc-
25 tor may appoint an executive secretary, who

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

2
3 “(4) MEETINGS.—The Board shall meet not
4 less than quarterly, but may meet more frequently
5 at the call of the Director.

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

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

13
14 “(7) TERMINATION.—The Board shall terminate on the date that is 3 years after the date of the
15 first meeting of the Board.”.

16
17 (b) INITIAL APPOINTMENTS.—Not later than 180
18 days after the date of the enactment of this Act, the Director of the National Reconnaissance Office shall appoint
19 the initial 5 members to the advisory board under subsection (d) of section 106A of the National Security Act
20 of 1947 (50 U.S.C. 3041a), as added by subsection (a).
21
22

1 **SEC. 435. COLLOCATION OF CERTAIN DEPARTMENT OF**
2 **HOMELAND SECURITY PERSONNEL AT FIELD**
3 **LOCATIONS.**

4 (a) IDENTIFICATION OF OPPORTUNITIES FOR COL-
5 LOCATION.—Not later than 60 days after the date of the
6 enactment of this Act, the Under Secretary of Homeland
7 Security for Intelligence and Analysis shall identify, in
8 consultation with the Commissioner of U.S. Customs and
9 Border Protection, the Administrator of the Transpor-
10 tation Security Administration, the Director of U.S. Immi-
11 gration and Customs Enforcement, and the heads of such
12 other elements of the Department of Homeland Security
13 as the Under Secretary considers appropriate, opportuni-
14 ties for collocation of officers of the Office of Intelligence
15 and Analysis in the field outside of the greater Wash-
16 ington, District of Columbia, area in order to support
17 operational units from U.S. Customs and Border Protec-
18 tion, the Transportation Security Administration, U.S.
19 Immigration and Customs Enforcement, and other ele-
20 ments of the Department of Homeland Security.

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

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;

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

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

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

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

21 (A) The majority leader of the Senate.

22 (B) The minority leader of the Senate.

23 (C) The Speaker of the House of Rep-
24 resentatives.

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

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

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

23 (c) FORM.—The report submitted under subsection
24 (b) shall be submitted in unclassified form, but may in-
25 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 a 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) IN GENERAL.—The Director of National Intel-
14 ligence, in coordination with the Director of the Central
15 Intelligence Agency, the Director of the National Security
16 Agency, the Director of the Federal Bureau of Investiga-
17 tion, the Secretary of Homeland Security, and the heads
18 of other relevant elements of the intelligence community,
19 shall—

20 (1) commence not later than 1 year before any
21 regularly scheduled Federal election occurring after
22 December 31, 2018, and complete not later than
23 180 days before such election, an assessment of se-
24 curity vulnerabilities of State election systems; and

1 (2) not later than 180 days before any regularly
2 scheduled Federal election occurring after December
3 31, 2018, submit a report on such security
4 vulnerabilities and an assessment of foreign intel-
5 ligence threats to the election to—

6 (A) congressional leadership; and

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

9 (c) UPDATE.—Not later than 90 days before any reg-
10 ularly scheduled Federal election occurring after Decem-
11 ber 31, 2018, the Director of National Intelligence shall—

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

14 (2) submit the updated assessment to—

15 (A) congressional leadership; and

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

18 **SEC. 504. STRATEGY FOR COUNTERING RUSSIAN CYBER**

19 **THREATS TO UNITED STATES ELECTIONS.**

20 (a) **APPROPRIATE CONGRESSIONAL COMMITTEES**

21 **DEFINED.**—In this section, the term “appropriate con-
22 gressional committees” means the following:

23 (1) The congressional intelligence committees.

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

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

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

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

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

1 (c) ELEMENTS OF THE STRATEGY.—The strategy re-
2 quired by subsection (b) shall include the following ele-
3 ments:

4 (1) A whole-of-government approach to pro-
5 tecting United States electoral systems and proc-
6 esses that includes the agencies and departments in-
7 dicated in subsection (b) as well as any other agen-
8 cies and departments of the United States, as deter-
9 mined appropriate by the Director of National Intel-
10 ligence and the Secretary of Homeland Security.

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

14 (3) Technical security measures, including
15 auditable paper trails for voting machines, securing
16 wireless and internet connections, and other tech-
17 nical safeguards.

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

21 (5) Improvements in the identification and at-
22 tribution of Russian government or nongovernment
23 cyber threat actors.

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

1 (b) ASSESSMENT REQUIRED.—Not later than 60
2 days after the date of the enactment of this Act, the Direc-
3 tor of National Intelligence shall submit to the congres-
4 sional intelligence committees a report containing an ana-
5 lytical assessment of the most significant Russian influ-
6 ence campaigns, if any, conducted during the 3-year pe-
7 riod preceding the date of the enactment of this Act, as
8 well as the most significant current or planned such Rus-
9 sian influence campaigns, if any. Such assessment shall
10 include—

11 (1) a summary of such significant Russian in-
12 fluence campaigns, including, at a minimum, the
13 specific means by which such campaigns were con-
14 ducted, are being conducted, or likely will be con-
15 ducted, as appropriate, and the specific goal of each
16 such campaign;

17 (2) a summary of any defenses against or re-
18 sponses to such Russian influence campaigns by the
19 foreign state holding the elections or referenda;

20 (3) a summary of any relevant activities by ele-
21 ments of the intelligence community undertaken for
22 the purpose of assisting the government of such for-
23 eign state in defending against or responding to
24 such Russian influence campaigns; and

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

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

7 **SEC. 506. FOREIGN COUNTERINTELLIGENCE AND CYBERSE-**
8 **CURITY THREATS TO FEDERAL ELECTION**
9 **CAMPAIGNS.**

10 (a) REPORTS REQUIRED.—

11 (1) IN GENERAL.—As provided in paragraph
12 (2), for each Federal election, the Director of Na-
13 tional Intelligence, in coordination with the Under
14 Secretary of Homeland Security for Intelligence and
15 Analysis and the Director of the Federal Bureau of
16 Investigation, shall make publicly available on an
17 internet website an advisory report on foreign coun-
18 terintelligence and cybersecurity threats to election
19 campaigns for Federal offices. Each such report
20 shall include, consistent with the protection of
21 sources and methods, each of the following:

22 (A) A description of foreign counterintel-
23 ligence and cybersecurity threats to election
24 campaigns for Federal offices.

1 (B) A summary of best practices that elec-
2 tion campaigns for Federal offices can employ
3 in seeking to counter such threats.

4 (C) An identification of any publicly avail-
5 able resources, including United States Govern-
6 ment resources, for countering such threats.

7 (2) SCHEDULE FOR SUBMITTAL.—A report
8 under this subsection shall be made available as fol-
9 lows:

10 (A) In the case of a report regarding an
11 election held for the office of Senator or Mem-
12 ber of the House of Representatives during
13 2018, not later than the date that is 60 days
14 after the date of the enactment of this Act.

15 (B) In the case of a report regarding an
16 election for a Federal office during any subse-
17 quent year, not later than the date that is 1
18 year before the date of the election.

19 (3) INFORMATION TO BE INCLUDED.—A report
20 under this subsection shall reflect the most current
21 information available to the Director of National In-
22 telligence regarding foreign counterintelligence and
23 cybersecurity threats.

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

1 Bureau of Investigation and the Under Secretary of
2 Homeland Security for Intelligence and Analysis jointly
3 determine that an election campaign for Federal office is
4 subject to a heightened foreign counterintelligence or cy-
5 bersecurity threat, the Director and the Under Secretary,
6 consistent with the protection of sources and methods,
7 may make available additional information to the appro-
8 priate representatives of such campaign.

9 **SEC. 507. INFORMATION SHARING WITH STATE ELECTION**
10 **OFFICIALS.**

11 (a) STATE DEFINED.—In this section, the term
12 “State” means any State of the United States, the Dis-
13 trict of Columbia, the Commonwealth of Puerto Rico, and
14 any territory or possession of the United States.

15 (b) 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 (c) 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 and the
13 Under Secretary responsible for overseeing critical
14 infrastructure protection, cybersecurity, and other
15 related programs of the Department (as specified in
16 section 103(a)(1)(H) of the Homeland Security Act
17 of 2002 (6 U.S.C. 113(a)(1)(H))) with sharing any
18 appropriate classified information related to threats
19 to election systems and to the integrity of the elec-
20 tion process with chief election officials and such
21 designees who have received a security clearance
22 under subsection (b).

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

1 ligence and the Under Secretary responsible for
2 overseeing critical infrastructure protection, cyberse-
3 curity, and other related programs of the Depart-
4 ment (as specified in section 103(a)(1)(H) of the
5 Homeland Security Act of 2002 (6 U.S.C.
6 113(a)(1)(H))) to facilitate the sharing of informa-
7 tion to the affected Secretaries of State or States.

8 **SEC. 508. NOTIFICATION OF SIGNIFICANT FOREIGN CYBER**
9 **INTRUSIONS AND ACTIVE MEASURES CAM-**
10 **PAIGNS DIRECTED AT ELECTIONS FOR FED-**
11 **ERAL OFFICES.**

12 (a) DEFINITIONS.—In this section:

13 (1) ACTIVE MEASURES CAMPAIGN.—The term
14 “active measures campaign” means a foreign semi-
15 covert or covert intelligence operation.

16 (2) CANDIDATE, ELECTION, AND POLITICAL
17 PARTY.—The terms “candidate”, “election”, and
18 “political party” have the meanings given those
19 terms in section 301 of the Federal Election Cam-
20 paign Act of 1971 (52 U.S.C. 30101).

21 (3) CONGRESSIONAL LEADERSHIP.—The term
22 “congressional leadership” includes the following:

23 (A) The majority leader of the Senate.

24 (B) The minority leader of the Senate.

1 (C) The Speaker of the House of Rep-
2 resentatives.

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

5 (4) CYBER INTRUSION.—The term “cyber in-
6 trusion” means an electronic occurrence that actu-
7 ally or imminently jeopardizes, without lawful au-
8 thority, electronic election infrastructure, or the in-
9 tegrity, confidentiality, or availability of information
10 within such infrastructure.

11 (5) ELECTRONIC ELECTION INFRASTRUC-
12 TURE.—The term “electronic election infrastruc-
13 ture” means an electronic information system of any
14 of the following that is related to an election for
15 Federal office:

16 (A) The Federal Government.

17 (B) A State or local government.

18 (C) A political party.

19 (D) The election campaign of a candidate.

20 (6) FEDERAL OFFICE.—The term “Federal of-
21 fice” has the meaning given that term in section 301
22 of the Federal Election Campaign Act of 1971 (52
23 U.S.C. 30101).

24 (7) HIGH CONFIDENCE.—The term “high con-
25 fidence”, with respect to a determination, means

1 that the determination is based on high-quality in-
2 formation from multiple sources.

3 (8) MODERATE CONFIDENCE.—The term “mod-
4 erate confidence”, with respect to a determination,
5 means that a determination is credibly sourced and
6 plausible but not of sufficient quality or corrobo-
7 rated sufficiently to warrant a higher level of con-
8 fidence.

9 (9) OTHER APPROPRIATE CONGRESSIONAL COM-
10 MITTEES.—The term “other appropriate congres-
11 sional committees” means—

12 (A) the Committee on Armed Services, the
13 Committee on Homeland Security and Govern-
14 mental Affairs, and the Committee on Appro-
15 priations of the Senate; and

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

20 (b) DETERMINATIONS OF SIGNIFICANT FOREIGN
21 CYBER INTRUSIONS AND ACTIVE MEASURES CAM-
22 PAIGNS.—The Director of National Intelligence, the Di-
23 rector of the Federal Bureau of Investigation, and the
24 Secretary of Homeland Security shall jointly carry out

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

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

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

12 (c) BRIEFING.—

13 (1) IN GENERAL.—Not later than 14 days after
14 making a determination under subsection (b), the
15 Director of National Intelligence, the Director of the
16 Federal Bureau of Investigation, and the Secretary
17 of Homeland Security shall jointly provide a briefing
18 to the congressional leadership, the congressional in-
19 telligence committees and, consistent with the pro-
20 tection of sources and methods, the other appro-
21 priate congressional committees. The briefing shall
22 be classified and address, at a minimum, the fol-
23 lowing:

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

4 (B) An identification of the foreign state
5 or foreign nonstate person, group, or other enti-
6 ty, to which such intrusion or campaign has
7 been attributed.

8 (C) The desirability and feasibility of the
9 public release of information about the cyber in-
10 trusion or active measures campaign.

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

13 (2) ELECTRONIC ELECTION INFRASTRUCTURE
14 BRIEFINGS.—With respect to a significant foreign
15 cyber intrusion covered by a determination under
16 subsection (b), the Secretary of Homeland Security,
17 in consultation with the Director of National Intel-
18 ligence and the Director of the Federal Bureau of
19 Investigation, shall offer to the owner or operator of
20 any electronic election infrastructure directly af-
21 fected by such intrusion, a briefing on such intru-
22 sion, including steps that may be taken to mitigate
23 such intrusion. Such briefing may be classified and
24 made available only to individuals with appropriate
25 security clearances.

1 (3) PROTECTION OF SOURCES AND METH-
2 ODS.—This subsection shall be carried out in a man-
3 ner that is consistent with the protection of sources
4 and methods.

5 **SEC. 509. DESIGNATION OF COUNTERINTELLIGENCE OFFI-**
6 **CER TO LEAD ELECTION SECURITY MATTERS.**

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

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

18 (1) The Federal Government election security
19 supply chain.

20 (2) Election voting systems and software.

21 (3) Voter registration databases.

22 (4) Critical infrastructure related to elections.

23 (5) Such other Government goods and services
24 as the Director of National Intelligence considers ap-
25 propriate.

TITLE VI—SECURITY

CLEARANCES

3 SEC. 601. DEFINITIONS.

4 In this title:

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

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

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

12 (C) the Committee on Appropriations of
13 the Senate;

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

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

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

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

22 (H) the Committee on Oversight and Re-
23 form of the House of Representatives.

24 (2) APPROPRIATE INDUSTRY PARTNERS.—The
25 term “appropriate industry partner” means a con-

1 tractor, licensee, or grantee (as defined in section
2 101(a) of Executive Order 12829 (50 U.S.C. 3161
3 note; relating to National Industrial Security Pro-
4 gram)) that is participating in the National Indus-
5 trial Security Program established by such Executive
6 order.

7 (3) CONTINUOUS VETTING.—The term “contin-
8 uous vetting” has the meaning given such term in
9 Executive Order 13467 (50 U.S.C. 3161 note; relat-
10 ing to reforming processes related to suitability for
11 government employment, fitness for contractor em-
12 ployees, and eligibility for access to classified na-
13 tional security information).

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

18 (5) SECURITY EXECUTIVE AGENT.—The term
19 “Security Executive Agent” means the officer serv-
20 ing as the Security Executive Agent pursuant to sec-
21 tion 803 of the National Security Act of 1947, as
22 added by section 605.

23 (6) SUITABILITY AND CREDENTIALING EXECU-
24 TIVE AGENT.—The term “Suitability and Credential-
25 ing Executive Agent” means the Director of the Of-

1 fice of Personnel Management acting as the Suit-
2 ability and Credentialing Executive Agent in accord-
3 ance with Executive Order 13467 (50 U.S.C. 3161
4 note; relating to reforming processes related to suit-
5 ability for government employment, fitness for con-
6 tractor employees, and eligibility for access to classi-
7 fied national security information), or any successor
8 entity.

9 **SEC. 602. REPORTS AND PLANS RELATING TO SECURITY**
10 **CLEARANCES AND BACKGROUND INVESTIGA-**
11 **TIONS.**

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

14 (1) ensuring the trustworthiness and security of
15 the workforce, facilities, and information of the Fed-
16 eral Government is of the highest priority to na-
17 tional security and public safety;

18 (2) the President and Congress should priori-
19 tize the modernization of the personnel security
20 framework to improve its efficiency, effectiveness,
21 and accountability;

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

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

3 (4) changes to policies or processes to improve
4 this system should be vetted through the Council to
5 ensure standardization, portability, and reciprocity
6 in security clearances across the Federal Govern-
7 ment.

8 (b) ACCOUNTABILITY PLANS AND REPORTS.—

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

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

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

1 organization. Such plan shall address required
2 funding, personnel, contracts, information tech-
3 nology, field office structure, policy, governance,
4 schedule, transition costs, and effects on stake-
5 holders.

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

8 (A) IN GENERAL.—Not later than 180
9 days after the date of the enactment of this
10 Act, the Chairman of the Council, in coordina-
11 tion with the members of the Council, shall sub-
12 mit to the appropriate congressional committees
13 and make available to appropriate industry
14 partners a report on the future of personnel se-
15 curity to reflect changes in threats, the work-
16 force, and technology.

17 (B) CONTENTS.—The report submitted
18 under subparagraph (A) shall include the fol-
19 lowing:

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

22 (ii) A discussion of the use of tech-
23 nologies to prevent, detect, and monitor
24 threats.

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

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

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

9 (vi) Recommendations on interagency
10 governance.

11 (3) PLAN FOR IMPLEMENTATION.—Not later
12 than 180 days after the date of the enactment of
13 this Act, the Chairman of the Council, in coordina-
14 tion with the members of the Council, shall submit
15 to the appropriate congressional committees and
16 make available to appropriate industry partners a
17 plan to implement the report’s framework and rec-
18 ommendations submitted under paragraph (2)(A).

19 (4) CONGRESSIONAL NOTIFICATIONS.—Not less
20 frequently than quarterly, the Security Executive
21 Agent shall make available to the public a report re-
22 garding the status of the disposition of requests re-
23 ceived from departments and agencies of the Federal
24 Government for a change to, or approval under, the
25 Federal investigative standards, the national adju-

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

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

5 (A) simplifying the Questionnaire for Na-
6 tional Security Positions (Standard Form 86)
7 and increasing customer support to applicants
8 completing such questionnaire;

9 (B) using remote techniques and central-
10 ized locations to support or replace field inves-
11 tigation work;

12 (C) using secure and reliable digitization of
13 information obtained during the clearance proc-
14 ess;

15 (D) building the capacity of the back-
16 ground investigation labor sector; and

17 (E) replacing periodic reinvestigations with
18 continuous evaluation techniques in all appro-
19 priate circumstances.

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

21 Not later than 180 days after the date of the enactment
22 of this Act, the Security Executive Agent shall, in coordi-
23 nation with the members of the Council, establish the fol-
24 lowing:

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

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

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

12 (B) standardization in the forms that
13 agencies issue to initiate the process for a secu-
14 rity clearance;

15 (C) digitization of background investiga-
16 tion-related forms;

17 (D) use of the polygraph;

18 (E) the application of the adjudicative
19 guidelines under Security Executive Agent Di-
20 rective 4 (known as the “National Security Ad-
21 judicative Guidelines”);

22 (F) reciprocal recognition of clearances
23 across agencies and departments of the United
24 States, regardless of status of periodic reinves-
25 tigation;

1 (G) tracking of clearance files as individ-
2 uals move from employment with an agency or
3 department of the United States to employment
4 in the private sector;

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

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

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

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

23 (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 (6) Uniform standards for agency continuous
2 evaluation programs to ensure quality and reci-
3 procuity in accepting enrollment in a continuous vet-
4 ting program as a substitute for a periodic investiga-
5 tion for continued access to classified information.

6 **SEC. 604. GOALS FOR PROMPTNESS OF DETERMINATIONS**
7 **REGARDING SECURITY CLEARANCES.**

8 (a) **RECIPROCITY DEFINED.**—In this section, the
9 term “reciprocity” means reciprocal recognition by Fed-
10 eral departments and agencies of eligibility for access to
11 classified information.

12 (b) **IN GENERAL.**—The Council shall reform the se-
13 curity clearance process with the objective that, by Decem-
14 ber 31, 2021, 90 percent of all determinations, other than
15 determinations regarding populations identified under sec-
16 tion 603(b)(3)(C), regarding—

17 (1) security clearances—

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

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

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

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

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

4 (d) EQUIVALENT METRICS.—

5 (1) IN GENERAL.—If the Council develops a set
6 of performance metrics that it certifies to the appro-
7 priate congressional committees should achieve sub-
8 stantially equivalent outcomes as those outlined in
9 subsections (b) and (c), the Council may use those
10 metrics for purposes of compliance within this provi-
11 sion.

12 (2) NOTICE.—If the Council uses the authority
13 provided by paragraph (1) to use metrics as de-
14 scribed in such paragraph, the Council shall, not
15 later than 30 days after communicating such metrics
16 to departments and agencies, notify the appropriate
17 congressional committees that it is using such au-
18 thority.

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

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

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

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

5 (2) by inserting after section 802 the following:

6 **“SEC. 803. SECURITY EXECUTIVE AGENT.**

7 “(a) IN GENERAL.—The Director of National Intel-
8 ligence, or such other officer of the United States as the
9 President may designate, shall serve as the Security Exec-
10 utive Agent for all departments and agencies of the United
11 States.
12 States.

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

15 “(1) To direct the oversight of investigations,
16 reinvestigations, adjudications, and, as applicable,
17 polygraphs for eligibility for access to classified in-
18 formation or eligibility to hold a sensitive position
19 made by any Federal agency.

20 “(2) To review the national security back-
21 ground investigation and adjudication programs of
22 Federal agencies to determine whether such pro-
23 grams are being implemented in accordance with
24 this section.

25 “(3) To develop and issue uniform and con-
26 sistent policies and procedures to ensure the effec-

1 tive, efficient, timely, and secure completion of inves-
2 tigations, polygraphs, and adjudications relating to
3 determinations of eligibility for access to classified
4 information or eligibility to hold a sensitive position.

5 “(4) Unless otherwise designated by law, to
6 serve as the final authority to designate a Federal
7 agency or agencies to conduct investigations of per-
8 sons who are proposed for access to classified infor-
9 mation or for eligibility to hold a sensitive position
10 to ascertain whether such persons satisfy the criteria
11 for obtaining and retaining access to classified infor-
12 mation or eligibility to hold a sensitive position, as
13 applicable.

14 “(5) Unless otherwise designated by law, to
15 serve as the final authority to designate a Federal
16 agency or agencies to determine eligibility for access
17 to classified information or eligibility to hold a sen-
18 sitive position in accordance with Executive Order
19 12968 (50 U.S.C. 3161 note; relating to access to
20 classified information).

21 “(6) To ensure reciprocal recognition of eligi-
22 bility for access to classified information or eligibility
23 to hold a sensitive position among Federal agencies,
24 including acting as the final authority to arbitrate
25 and resolve disputes among such agencies involving

1 the reciprocity of investigations and adjudications of
2 eligibility.

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

5 “(c) AUTHORITIES.—The Security Executive Agent
6 shall—

7 “(1) issue guidelines and instructions to the
8 heads of Federal agencies to ensure appropriate uni-
9 formity, centralization, efficiency, effectiveness, time-
10 liness, and security in processes relating to deter-
11 minations by such agencies of eligibility for access to
12 classified information or eligibility to hold a sensitive
13 position, including such matters as investigations,
14 polygraphs, adjudications, and reciprocity;

15 “(2) have the authority to grant exceptions to,
16 or waivers of, national security investigative require-
17 ments, including issuing implementing or clarifying
18 guidance, as necessary;

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

1 Agent, including such terms and conditions (includ-
2 ing approval by the Security Executive Agent) as the
3 Security Executive Agent determines appropriate;
4 and

5 “(4) define and set standards for continuous
6 evaluation for continued access to classified informa-
7 tion and for eligibility to hold a sensitive position.”.

8 (b) REPORT ON RECOMMENDATIONS FOR REVISING
9 AUTHORITIES.—Not later than 30 days after the date on
10 which the Chairman of the Council submits to the appro-
11 priate congressional committees the report required by
12 section 602(b)(2)(A), the Chairman shall submit to the
13 appropriate congressional committees such recommenda-
14 tions as the Chairman may have for revising the authori-
15 ties of the Security Executive Agent.

16 (c) CONFORMING AMENDMENT.—Section
17 103H(j)(4)(A) of such Act (50 U.S.C. 3033(j)(4)(A)) is
18 amended by striking “in section 804” and inserting “in
19 section 805”.

20 (d) CLERICAL AMENDMENT.—The table of contents
21 in the matter preceding section 2 of such Act (50 U.S.C.
22 3002) is amended by striking the items relating to sections
23 803 and 804 and inserting the following:

“Sec. 803. Security Executive Agent.

“Sec. 804. Exceptions.

“Sec. 805. Definitions.”.

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

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

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

21 (b) REPORT REQUIRED.—Not later than 90 days
22 after the date of the enactment of this Act, the Security
23 Executive Agent shall submit to the appropriate congress-
24 sional committees and make available to appropriate in-
25 dustry partners a report that describes the requirements,

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

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

5 (1) permits an individual who once held a secu-
6 rity clearance to maintain his or her eligibility for
7 access to classified information, networks, and facili-
8 ties for up to 3 years after the individual’s eligibility
9 for access to classified information would otherwise
10 lapse; and

11 (2) recognizes, unless otherwise directed by the
12 Security Executive Agent, an individual’s security
13 clearance and background investigation as current,
14 regardless of employment status, contingent on en-
15 rollment in a continuous vetting program.

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

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

23 (2) appropriate safeguards for privacy;

24 (3) advantages to government and industry;

1 (4) the costs and savings associated with imple-
2 mentation;

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

5 (6) an appropriate funding model; and

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

8 **SEC. 608. BUDGET REQUEST DOCUMENTATION ON FUND-**
9 **ING FOR BACKGROUND INVESTIGATIONS.**

10 (a) IN GENERAL.—As part of the fiscal year 2020
11 budget request submitted to Congress pursuant to section
12 1105(a) of title 31, United States Code, the President
13 shall include exhibits that identify the resources expended
14 by each agency during the prior fiscal year for processing
15 background investigations and continuous evaluation pro-
16 grams, disaggregated by tier and whether the individual
17 was a Government employee or contractor.

18 (b) CONTENTS.—Each exhibit submitted under sub-
19 section (a) shall include details on—

20 (1) the costs of background investigations or re-
21 investigations;

22 (2) the costs associated with background inves-
23 tigations for Government or contract personnel;

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

1 background investigation or reinvestigation was con-
2 ducted, other than costs associated with adjudica-
3 tion;

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

6 (5) a summary of transfers and reprogram-
7 mings that were executed in the previous year to
8 support the processing of security clearances.

9 **SEC. 609. REPORTS ON RECIPROCITY FOR SECURITY**
10 **CLEARANCES INSIDE OF DEPARTMENTS AND**
11 **AGENCIES.**

12 (a) **RECIPROCALLY RECOGNIZED DEFINED.**—In this
13 section, the term “reciprocally recognized” means recip-
14 rocal recognition by Federal departments and agencies of
15 eligibility for access to classified information.

16 (b) **REPORTS TO SECURITY EXECUTIVE AGENT.**—
17 The head of each Federal department or agency shall sub-
18 mit an annual report to the Security Executive Agent
19 that—

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

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

4 (c) ANNUAL REPORT.—Not less frequently than once
5 each year, the Security Executive Agent shall submit to
6 the appropriate congressional committees and make avail-
7 able to industry partners an annual report that summa-
8 rizes the information received pursuant to subsection (b)
9 during the period covered by such report.

10 **SEC. 610. INTELLIGENCE COMMUNITY REPORTS ON SECU-**
11 **RITY CLEARANCES.**

12 Section 506H of the National Security Act of 1947
13 (50 U.S.C. 3104) is amended—

14 (1) in subsection (a)(1)—

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

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

19 (C) by striking subparagraph (C);

20 (2) by redesignating subsection (b) as sub-
21 section (c);

22 (3) by inserting after subsection (a) the fol-
23 lowing:

24 “(b) INTELLIGENCE COMMUNITY REPORTS.—(1)(A)

25 Not later than March 1 of each year, the Director of Na-

1 tional Intelligence shall submit a report to the congres-
2 sional intelligence committees, the Committee on Home-
3 land Security and Governmental Affairs of the Senate, the
4 Committee on Homeland Security of the House of Rep-
5 resentatives, and the Committee on Oversight and Reform
6 of the House of Representatives regarding the security
7 clearances processed by each element of the intelligence
8 community during the preceding fiscal year.

9 “(B) The Director shall submit to the Committee on
10 Armed Services of the Senate and the Committee on
11 Armed Services of the House of Representatives such por-
12 tions of the report submitted under subparagraph (A) as
13 the Director determines address elements of the intel-
14 ligence community that are within the Department of De-
15 fense.

16 “(C) Each report submitted under this paragraph
17 shall separately identify security clearances processed for
18 Federal employees and contractor employees sponsored by
19 each such element.

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

23 “(A) The total number of initial security clear-
24 ance background investigations sponsored for new
25 applicants.

1 “(B) The total number of security clearance
2 periodic reinvestigations sponsored for existing em-
3 ployees.

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

8 “(i) the total number of such adjudications
9 that were adjudicated favorably and granted ac-
10 cess to classified information; and

11 “(ii) the total number of such adjudica-
12 tions that were adjudicated unfavorably and re-
13 sulted in a denial or revocation of a security
14 clearance.

15 “(D) The total number of security clearance
16 periodic background investigations that were adju-
17 dicated with notice of a determination provided to
18 the existing employee, including—

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

21 “(ii) the total number of such adjudica-
22 tions that were adjudicated unfavorably and re-
23 sulted in a denial or revocation of a security
24 clearance.

1 “(E) The total number of pending security
2 clearance background investigations, including initial
3 applicant investigations and periodic reinvestiga-
4 tions, that were not adjudicated as of the last day
5 of such year and that remained pending, categorized
6 as follows:

7 “(i) For 180 days or shorter.

8 “(ii) For longer than 180 days, but shorter
9 than 12 months.

10 “(iii) For 12 months or longer, but shorter
11 than 18 months.

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

14 “(v) For 24 months or longer.

15 “(F) For any security clearance determinations
16 completed or pending during the year preceding the
17 year for which the report is submitted that have
18 taken longer than 12 months to complete—

19 “(i) an explanation of the causes for the
20 delays incurred during the period covered by
21 the report; and

22 “(ii) the number of such delays involving a
23 polygraph requirement.

24 “(G) The percentage of security clearance in-
25 vestigations, including initial and periodic reinves-

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

3 **SEC. 612. INFORMATION SHARING PROGRAM FOR POSI-**
4 **TIONS OF TRUST AND SECURITY CLEAR-**
5 **ANCES.**

6 (a) PROGRAM REQUIRED.—

7 (1) IN GENERAL.—Not later than 90 days after
8 the date of the enactment of this Act, the Security
9 Executive Agent and the Suitability and Credential-
10 ing Executive Agent shall establish and implement a
11 program to share between and among agencies of
12 the Federal Government and industry partners of
13 the Federal Government relevant background infor-
14 mation regarding individuals applying for and cur-
15 rently occupying national security positions and posi-
16 tions of trust, in order to ensure the Federal Gov-
17 ernment maintains a trusted workforce.

18 (2) DESIGNATION.—The program established
19 under paragraph (1) shall be known as the “Trusted
20 Information Provider Program” (in this section re-
21 ferred to as the “Program”).

22 (b) PRIVACY SAFEGUARDS.—The Security Executive
23 Agent and the Suitability and Credentialing Executive
24 Agent shall ensure that the Program includes such safe-
25 guards for privacy as the Security Executive Agent and

1 the Suitability and Credentialing Executive Agent consider
2 appropriate.

3 (c) PROVISION OF INFORMATION TO THE FEDERAL
4 GOVERNMENT.—The Program shall include requirements
5 that enable investigative service providers and agencies of
6 the Federal Government to leverage certain pre-employ-
7 ment information gathered during the employment or mili-
8 tary recruiting process, and other relevant security or
9 human resources information obtained during employment
10 with or for the Federal Government, that satisfy Federal
11 investigative standards, while safeguarding personnel pri-
12 vacy.

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

- 16 (1) Date and place of birth.
- 17 (2) Citizenship or immigration and naturaliza-
18 tion information.
- 19 (3) Education records.
- 20 (4) Employment records.
- 21 (5) Employment or social references.
- 22 (6) Military service records.
- 23 (7) State and local law enforcement checks.
- 24 (8) Criminal history checks.
- 25 (9) Financial records or information.

1 (10) Foreign travel, relatives, or associations.

2 (11) Social media checks.

3 (12) Such other information or records as may
4 be relevant to obtaining or maintaining national se-
5 curity, suitability, fitness, or credentialing eligibility.

6 (e) IMPLEMENTATION PLAN.—

7 (1) IN GENERAL.—Not later than 90 days after
8 the date of the enactment of this Act, the Security
9 Executive Agent and the Suitability and Credential-
10 ing Executive Agent shall jointly submit to the ap-
11 propriate congressional committees and make avail-
12 able to appropriate industry partners a plan for the
13 implementation of the Program.

14 (2) ELEMENTS.—The plan required by para-
15 graph (1) shall include the following:

16 (A) Mechanisms that address privacy, na-
17 tional security, suitability or fitness, credential-
18 ing, and human resources or military recruit-
19 ment processes.

20 (B) Such recommendations for legislative
21 or administrative action as the Security Execu-
22 tive Agent and the Suitability and Credentialing
23 Executive Agent consider appropriate to carry
24 out or improve the Program.

1 (f) PLAN FOR PILOT PROGRAM ON TWO-WAY INFOR-
2 MATION SHARING.—

3 (1) IN GENERAL.—Not later than 180 days
4 after the date of the enactment of this Act, the Se-
5 curity Executive Agent and the Suitability and Cre-
6 dentialing Executive Agent shall jointly submit to
7 the appropriate congressional committees and make
8 available to appropriate industry partners a plan for
9 the implementation of a pilot program to assess the
10 feasibility and advisability of expanding the Program
11 to include the sharing of information held by the
12 Federal Government related to contract personnel
13 with the security office of the employers of those
14 contractor personnel.

15 (2) ELEMENTS.—The plan required by para-
16 graph (1) shall include the following:

17 (A) Mechanisms that address privacy, na-
18 tional security, suitability or fitness, credential-
19 ing, and human resources or military recruit-
20 ment processes.

21 (B) Such recommendations for legislative
22 or administrative action as the Security Execu-
23 tive Agent and the Suitability and Credentialing
24 Executive Agent consider appropriate to carry
25 out or improve the pilot program.

1 (g) REVIEW.—Not later than 1 year after the date
2 of the enactment of this Act, the Security Executive Agent
3 and the Suitability and Credentialing Executive Agent
4 shall jointly submit to the appropriate congressional com-
5 mittees and make available to appropriate industry part-
6 ners a review of the plans submitted under subsections
7 (e)(1) and (f)(1) and utility and effectiveness of the pro-
8 grams described in such plans.

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

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

8 (a) **APPROPRIATE CONGRESSIONAL COMMITTEES**
9 **DEFINED.**—In this section, the term “appropriate con-
10 gressional committees” means—

- 11 (1) the congressional intelligence committees;
12 (2) the Committee on Armed Services of the
13 Senate and the Committee on Armed Services of the
14 House of Representatives; and
15 (3) the Committee on Foreign Relations of the
16 Senate and the Committee on Foreign Affairs of the
17 House of Representatives.

18 (b) **LIMITATION.**—

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

1 conclusion of any such agreement, the Director of
2 National Intelligence submits to the appropriate con-
3 gressional committees a report on such agreement
4 that includes the elements required by subsection
5 (c).

6 (2) DEPARTMENT OF DEFENSE AGREE-
7 MENTS.—Any agreement between the Department of
8 Defense and the Russian Federation regarding cy-
9 bersecurity shall be conducted in accordance with
10 section 1232 of the National Defense Authorization
11 Act for Fiscal Year 2017 (Public Law 114–328), as
12 amended by section 1231 of the National Defense
13 Authorization Act for Fiscal Year 2018 (Public Law
14 115–91).

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

18 (1) The purpose of the agreement.

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

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

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

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

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

9 **SEC. 702. REPORT ON RETURNING RUSSIAN COMPOUNDS.**

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

19 (b) **REQUIREMENT FOR REPORT.**—Not later than
20 180 days after the date of the enactment of this Act, the
21 Director of National Intelligence shall submit to the con-
22 gressional intelligence committees, and the Committee on
23 Foreign Relations of the Senate and the Committee on
24 Foreign Affairs of the House of Representatives (only with
25 respect to the unclassified report), a report on the intel-

1 ligen ce risks of returning the covered compounds to Rus-
2 sian control.

3 (c) FORM OF REPORT.—The report required by this
4 section shall be submitted in classified and unclassified
5 forms.

6 **SEC. 703. ASSESSMENT OF THREAT FINANCE RELATING TO**
7 **RUSSIA.**

8 (a) THREAT FINANCE DEFINED.—In this section,
9 the term “threat finance” means—

10 (1) the financing of cyber operations, global in-
11 fluence campaigns, intelligence service activities, pro-
12 liferation, terrorism, or transnational crime and
13 drug organizations;

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

17 (3) sanctions evasion; and

18 (4) other forms of threat finance activity do-
19 mestic ally or internationally, as defined by the Presi-
20 dent.

21 (b) REPORT REQUIRED.—Not later than 60 days
22 after the date of the enactment of this Act, the Director
23 of National Intelligence, in coordination with the Assistant
24 Secretary of the Treasury for Intelligence and Analysis,
25 shall submit to the congressional intelligence committees

1 a report containing an assessment of Russian threat fi-
2 nance. The assessment shall be based on intelligence from
3 all sources, including from the Office of Terrorism and
4 Financial Intelligence of the Department of the Treasury.

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

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

11 (A) officials of the Government of Russia;

12 (B) persons subject to sanctions under any
13 provision of law imposing sanctions with respect
14 to Russia;

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

17 (D) Russian oligarchs or organized crimi-
18 nals.

19 (2) An assessment with respect to any trends or
20 patterns in threat finance activities relating to Rus-
21 sia, including common methods of conducting such
22 activities and global nodes of money laundering used
23 by Russian threat actors described in paragraph (1)
24 and associated entities.

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

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

8 (5) An identification of any resource and collec-
9 tion gaps.

10 (6) An identification of—

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

14 (B) any vulnerabilities within the United
15 States legal and financial system, including spe-
16 cific sectors, which have been or could be ex-
17 ploited in connection with Russian threat fi-
18 nance activities; and

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

1 (7) Any other matters the Director determines
2 appropriate.

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

5 **SEC. 704. NOTIFICATION OF AN ACTIVE MEASURES CAM-**
6 **PAIGN.**

7 (a) DEFINITIONS.—In this section:

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

11 (A) the congressional intelligence commit-
12 tees;

13 (B) the Committee on Armed Services of
14 the Senate and the Committee on Armed Serv-
15 ices of the House of Representatives; and

16 (C) the Committee on Foreign Relations of
17 the Senate and the Committee on Foreign Af-
18 fairs of the House of Representatives.

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

21 (A) The majority leader of the Senate.

22 (B) The minority leader of the Senate.

23 (C) The Speaker of the House of Rep-
24 resentatives.

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

3 (b) REQUIREMENT FOR NOTIFICATION.—The Direc-
4 tor of National Intelligence, in cooperation with the Direc-
5 tor of the Federal Bureau of Investigation and the head
6 of any other relevant agency, shall notify the congressional
7 leadership and the Chairman and Vice Chairman or Rank-
8 ing Member of each of the appropriate congressional com-
9 mittees, and of other relevant committees of jurisdiction,
10 each time the Director of National Intelligence determines
11 there is credible information that a foreign power has, is,
12 or will attempt to employ a covert influence or active
13 measures campaign with regard to the modernization, em-
14 ployment, doctrine, or force posture of the nuclear deter-
15 rent or missile defense.

16 (c) CONTENT OF NOTIFICATION.—Each notification
17 required by subsection (b) shall include information con-
18 cerning actions taken by the United States to expose or
19 halt an attempt referred to in subsection (b).

20 **SEC. 705. NOTIFICATION OF TRAVEL BY ACCREDITED DIP-**
21 **LOMATIC AND CONSULAR PERSONNEL OF**
22 **THE RUSSIAN FEDERATION IN THE UNITED**
23 **STATES.**

24 In carrying out the advance notification requirements
25 set out in section 502 of the Intelligence Authorization

1 Act for Fiscal Year 2017 (division N of Public Law 115–
2 31; 131 Stat. 825; 22 U.S.C. 254a note), the Secretary
3 of State shall—

4 (1) ensure that the Russian Federation provides
5 notification to the Secretary of State at least 2 busi-
6 ness days in advance of all travel that is subject to
7 such requirements by accredited diplomatic and con-
8 sular personnel of the Russian Federation in the
9 United States, and take necessary action to secure
10 full compliance by Russian personnel and address
11 any noncompliance; and

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

16 **SEC. 706. REPORT ON OUTREACH STRATEGY ADDRESSING**
17 **THREATS FROM UNITED STATES ADVER-**
18 **SARIES TO THE UNITED STATES TECH-**
19 **NOLOGY SECTOR.**

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

23 (1) the congressional intelligence committees;

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

4 (3) the Committee on Armed Services, Com-
5 mittee on Homeland Security, and the Committee on
6 Oversight and Reform of the House of Representa-
7 tives.

8 (b) REPORT REQUIRED.—Not later than 180 days
9 after the date of the enactment of this Act, the Director
10 of National Intelligence shall submit to the appropriate
11 committees of Congress a report detailing outreach by the
12 intelligence community and the Defense Intelligence En-
13 terprise to United States industrial, commercial, scientific,
14 technical, and academic communities on matters relating
15 to the efforts of adversaries of the United States to ac-
16 quire critical United States technology, intellectual prop-
17 erty, and research and development information.

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

20 (1) A review of the current outreach efforts of
21 the intelligence community and the Defense Intel-
22 ligence Enterprise described in subsection (b), in-
23 cluding the type of information conveyed in the out-
24 reach.

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

4 (3) An assessment of potential methods for im-
5 proving the effectiveness of such outreach, including
6 an assessment of the following:

7 (A) Those critical technologies, infrastruc-
8 ture, or related supply chains that are at risk
9 from the efforts of adversaries described in sub-
10 section (b).

11 (B) The necessity and advisability of
12 granting security clearances to company or
13 community leadership, when necessary and ap-
14 propriate, to allow for tailored classified brief-
15 ings on specific targeted threats.

16 (C) The advisability of partnering with en-
17 tities of the Federal Government that are not
18 elements of the intelligence community and rel-
19 evant regulatory and industry groups described
20 in subsection (b), to convey key messages across
21 sectors targeted by United States adversaries.

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

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

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

7 (B) the Committee on Armed Services, the
8 Committee on Foreign Affairs, and the Perma-
9 nent Select Committee on Intelligence of the
10 House of Representatives.

11 (2) ARMS OR RELATED MATERIAL.—The term
12 “arms or related material” means—

13 (A) nuclear, biological, chemical, or radio-
14 logical weapons or materials or components of
15 such weapons;

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

18 (C) destabilizing numbers and types of ad-
19 vanced conventional weapons;

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

1 (E) defense information, as that term is
2 defined in section 644 of the Foreign Assist-
3 ance Act of 1961 (22 U.S.C. 2403); or

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

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

16 (c) MATTERS FOR INCLUSION.—The report required
17 under subsection (b) shall include information relating to
18 the following matters with respect to both the strategic
19 and tactical implications for the United States and its al-
20 lies:

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

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

3 (2) A description of Iranian and Iranian-con-
4 trolled personnel, including Hizballah, Shiite mili-
5 tias, and Iran's Revolutionary Guard Corps forces,
6 operating within Syria, including the number and
7 geographic distribution of such personnel operating
8 within 30 kilometers of the Israeli borders with
9 Syria and Lebanon.

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

13 (4) A description of any rocket-producing facili-
14 ties in Lebanon for nonstate actors, including wheth-
15 er such facilities were assessed to be built at the di-
16 rection of Hizballah leadership, Iranian leadership,
17 or in consultation between Iranian leadership and
18 Hizballah leadership.

19 (5) An analysis of the foreign and domestic
20 supply chains that significantly facilitate, support, or
21 otherwise aid Hizballah's acquisition or development
22 of missile production facilities, including the geo-
23 graphic distribution of such foreign and domestic
24 supply chains.

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

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

6 (A) Hizballah;

7 (B) Houthi rebels in Yemen;

8 (C) Hamas;

9 (D) proxy forces in Iraq and Syria; or

10 (E) any other entity or country the Direc-
11 tor determines to be relevant.

12 (2) The amount spent in such calendar year for
13 ballistic missile research and testing or other activi-
14 ties that the Director determines are destabilizing to
15 the Middle East region.

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

19 **SEC. 709. EXPANSION OF SCOPE OF COMMITTEE TO**
20 **COUNTER ACTIVE MEASURES AND REPORT**
21 **ON ESTABLISHMENT OF FOREIGN MALIGN IN-**
22 **FLUENCE CENTER.**

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

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

5 (A) in subsections (a) through (h)—

6 (i) by inserting “, the People’s Repub-
7 lic of China, the Islamic Republic of Iran,
8 the Democratic People’s Republic of
9 Korea, or other nation state” after “Rus-
10 sian Federation” each place it appears;
11 and

12 (ii) by inserting “, China, Iran, North
13 Korea, or other nation state” after “Rus-
14 sia” each place it appears; and

15 (B) in the section heading, by inserting “,

16 **THE PEOPLE’S REPUBLIC OF CHINA, THE**
17 **ISLAMIC REPUBLIC OF IRAN, THE DEMO-**
18 **CRATIC PEOPLE’S REPUBLIC OF KOREA,**
19 **OR OTHER NATION STATE”** after “**RUSSIAN**
20 **FEDERATION”**.

21 (2) CLERICAL AMENDMENT.—The table of con-
22 tents in section 1(b) of such Act is amended by
23 striking the item relating to section 501 and insert-
24 ing the following new item:

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

1 (b) REPORT REQUIRED.—

2 (1) IN GENERAL.—Not later than 180 days
3 after the date of the enactment of this Act, the Di-
4 rector of National Intelligence, in coordination with
5 such elements of the intelligence community as the
6 Director considers relevant, shall submit to the con-
7 gressional intelligence committees a report on the
8 feasibility and advisability of establishing a center,
9 to be known as the “Foreign Malign Influence Re-
10 sponse Center”, that—

11 (A) is comprised of analysts from all ap-
12 propriate elements of the intelligence commu-
13 nity, including elements with related diplomatic
14 and law enforcement functions;

15 (B) has access to all intelligence and other
16 reporting acquired by the United States Gov-
17 ernment on foreign efforts to influence, through
18 overt and covert malign activities, United
19 States political processes and elections;

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

1 (D) provides for enhanced dissemination of
 2 such assessment to United States policy mak-
 3 ers.

4 (2) CONTENTS.—The Report required by para-
 5 graph (1) shall include the following:

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

9 (B) Such recommendations and other mat-
 10 ters as the Director considers appropriate.

11 **Subtitle B—Reports**

12 **SEC. 711. TECHNICAL CORRECTION TO INSPECTOR GEN- 13 ERAL STUDY.**

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

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

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

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

22 **SEC. 712. REPORTS ON AUTHORITIES OF THE CHIEF INTEL- 23 LIGENCE OFFICER OF THE DEPARTMENT OF 24 HOMELAND SECURITY.**

25 (a) DEFINITIONS.—In this section:

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

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

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

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

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

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

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

23 (1) An analysis of whether the Under Secretary
24 has the legal and policy authority necessary to orga-
25 nize and lead the Homeland Security Intelligence

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

3 (A) the obstacles to exercising the authori-
4 ties of the Chief Intelligence Officer of the De-
5 partment and the Homeland Security Intel-
6 ligence Council, of which the Chief Intelligence
7 Officer is the chair; and

8 (B) the legal and policy changes necessary
9 to effectively coordinate, organize, and lead in-
10 telligence activities of the Department of Home-
11 land Security.

12 (2) A description of the actions that the Sec-
13 retary has taken to address the inability of the
14 Under Secretary to require components of the De-
15 partment, other than the Office of Intelligence and
16 Analysis of the Department to—

17 (A) coordinate intelligence programs; and

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

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

21 (a) REPORT.—Not later than 90 days after the date
22 of the enactment of this Act, the Director of National In-
23 telligence shall submit to the congressional intelligence
24 committees a report on the potential establishment of a
25 fully voluntary exchange program between elements of the

1 intelligence community and private technology companies
2 under which—

3 (1) an employee of an element of the intel-
4 ligence community with demonstrated expertise and
5 work experience in cybersecurity or related dis-
6 ciplines may elect to be temporarily detailed to a pri-
7 vate technology company that has elected to receive
8 the detailee; and

9 (2) an employee of a private technology com-
10 pany with demonstrated expertise and work experi-
11 ence in cybersecurity or related disciplines may elect
12 to be temporarily detailed to an element of the intel-
13 ligence community that has elected to receive the
14 detailee.

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

17 (1) An assessment of the feasibility of estab-
18 lishing the exchange program described in such sub-
19 section.

20 (2) Identification of any challenges in estab-
21 lishing the exchange program.

22 (3) An evaluation of the benefits to the intel-
23 ligence community that would result from the ex-
24 change program.

1 **SEC. 714. REVIEW OF INTELLIGENCE COMMUNITY WHIS-**
2 **TLBLOWER MATTERS.**

3 (a) REVIEW OF WHISTLEBLOWER MATTERS.—The
4 Inspector General of the Intelligence Community, in con-
5 sultation with the inspectors general for the Central Intel-
6 ligence Agency, the National Security Agency, the Na-
7 tional Geospatial-Intelligence Agency, the Defense Intel-
8 ligence Agency, and the National Reconnaissance Office,
9 shall conduct a review of the authorities, policies, inves-
10 tigatory standards, and other practices and procedures re-
11 lating to intelligence community whistleblower matters,
12 with respect to such inspectors general.

13 (b) OBJECTIVE OF REVIEW.—The objective of the re-
14 view required under subsection (a) is to identify any dis-
15 crepancies, inconsistencies, or other issues, which frustrate
16 the timely and effective reporting of intelligence commu-
17 nity whistleblower matters to appropriate inspectors gen-
18 eral and to the congressional intelligence committees, and
19 the fair and expeditious investigation and resolution of
20 such matters.

21 (c) CONDUCT OF REVIEW.—The Inspector General of
22 the Intelligence Community shall take such measures as
23 the Inspector General determines necessary in order to en-
24 sure that the review required by subsection (a) is con-
25 ducted in an independent and objective fashion.

1 (d) REPORT.—Not later than 270 days after the date
2 of the enactment of this Act, the Inspector General of the
3 Intelligence Community shall submit to the congressional
4 intelligence committees a written report containing the re-
5 sults of the review required under subsection (a), along
6 with recommendations to improve the timely and effective
7 reporting of intelligence community whistleblower matters
8 to inspectors general and to the congressional intelligence
9 committees and the fair and expeditious investigation and
10 resolution of such matters.

11 **SEC. 715. REPORT ON ROLE OF DIRECTOR OF NATIONAL IN-**
12 **TELLIGENCE WITH RESPECT TO CERTAIN**
13 **FOREIGN INVESTMENTS.**

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

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

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

4 (2) an identification of the most significant ben-
5 efits and drawbacks of such process with respect to
6 the role of the Director, including the sufficiency of
7 resources and personnel to prepare such materials;
8 and

9 (3) recommendations to improve such process.

10 **SEC. 716. REPORT ON SURVEILLANCE BY FOREIGN GOV-**
11 **ERNMENTS AGAINST UNITED STATES TELE-**
12 **COMMUNICATIONS NETWORKS.**

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

16 (1) The congressional intelligence committees.

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

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

23 (b) REPORT.—Not later than 180 days after the date
24 of the enactment of this Act, the Director of National In-
25 telligence shall, in coordination with the Director of the

1 Central Intelligence Agency, the Director of the National
2 Security Agency, the Director of the Federal Bureau of
3 Investigation, and the Secretary of Homeland Security,
4 submit to the appropriate congressional committees a re-
5 port describing—

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

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

17 **SEC. 717. BIENNIAL REPORT ON FOREIGN INVESTMENT**
18 **RISKS.**

19 (a) INTELLIGENCE COMMUNITY INTERAGENCY
20 WORKING GROUP.—

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

25 (b).

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

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

9 (b) BIENNIAL REPORT ON FOREIGN INVESTMENT
10 RISKS.—

11 (1) REPORT REQUIRED.—Not later than 180
12 days after the date of the enactment of this Act and
13 not less frequently than once every 2 years there-
14 after, the Director of National Intelligence shall sub-
15 mit to the congressional intelligence committees, the
16 Committee on Homeland Security and Governmental
17 Affairs of the Senate, and the Committee on Home-
18 land Security of the House of Representatives a re-
19 port on foreign investment risks prepared by the
20 interagency working group established under sub-
21 section (a).

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

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

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

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

14 **SEC. 718. MODIFICATION OF CERTAIN REPORTING RE-**
15 **QUIREMENT ON TRAVEL OF FOREIGN DIP-**
16 **LOMATS.**

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

20 **SEC. 719. SEMIANNUAL REPORTS ON INVESTIGATIONS OF**
21 **UNAUTHORIZED DISCLOSURES OF CLASSI-**
22 **FIED INFORMATION.**

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

1 **“SEC. 1105. SEMIANNUAL REPORTS ON INVESTIGATIONS OF**
2 **UNAUTHORIZED DISCLOSURES OF CLASSI-**
3 **FIED INFORMATION.**

4 “(a) DEFINITIONS.—In this section:

5 “(1) COVERED OFFICIAL.—The term ‘covered
6 official’ means—

7 “(A) the heads of each element of the in-
8 telligence community; and

9 “(B) the inspectors general with oversight
10 responsibility for an element of the intelligence
11 community.

12 “(2) INVESTIGATION.—The term ‘investigation’
13 means any inquiry, whether formal or informal, into
14 the existence of an unauthorized public disclosure of
15 classified information.

16 “(3) UNAUTHORIZED DISCLOSURE OF CLASSI-
17 FIED INFORMATION.—The term ‘unauthorized dis-
18 closure of classified information’ means any unau-
19 thorized disclosure of classified information to any
20 recipient.

21 “(4) UNAUTHORIZED PUBLIC DISCLOSURE OF
22 CLASSIFIED INFORMATION.—The term ‘unauthorized
23 public disclosure of classified information’ means the
24 unauthorized disclosure of classified information to a
25 journalist or media organization.

26 “(b) INTELLIGENCE COMMUNITY REPORTING.—

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

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

9 “(A) The number of investigations opened
10 by the covered official regarding an unauthor-
11 ized public disclosure of classified information.

12 “(B) The number of investigations com-
13 pleted by the covered official regarding an un-
14 authorized public disclosure of classified infor-
15 mation.

16 “(C) Of the number of such completed in-
17 vestigations identified under subparagraph (B),
18 the number referred to the Attorney General
19 for criminal investigation.

20 “(c) DEPARTMENT OF JUSTICE REPORTING.—

21 “(1) IN GENERAL.—Not less frequently than
22 once every 6 months, the Assistant Attorney General
23 for National Security of the Department of Justice,
24 in consultation with the Director of the Federal Bu-
25 reau of Investigation, shall submit to the congress-

1 sional intelligence committees, the Committee on the
2 Judiciary of the Senate, and the Committee on the
3 Judiciary of the House of Representatives a report
4 on the status of each referral made to the Depart-
5 ment of Justice from any element of the intelligence
6 community regarding an unauthorized disclosure of
7 classified information made during the most recent
8 365-day period or any referral that has not yet been
9 closed, regardless of the date the referral was made.

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

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

14 “(B) A statement indicating whether the
15 alleged unauthorized disclosure described in the
16 referral was substantiated by the Department
17 of Justice.

18 “(C) A statement indicating the highest
19 level of classification of the information that
20 was revealed in the unauthorized disclosure.

21 “(D) A statement indicating whether an
22 open criminal investigation related to the refer-
23 ral is active.

1 “(E) A statement indicating whether any
2 criminal charges have been filed related to the
3 referral.

4 “(F) A statement indicating whether the
5 Department of Justice has been able to at-
6 tribute the unauthorized disclosure to a par-
7 ticular entity or individual.

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

11 (b) CLERICAL AMENDMENT.—The table of contents
12 in the first section of the National Security Act of 1947
13 is amended by inserting after the item relating to section
14 1104 the following new item:

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

15 **SEC. 720. CONGRESSIONAL NOTIFICATION OF DESIGNA-**
16 **TION OF COVERED INTELLIGENCE OFFICER**
17 **AS PERSONA NON GRATA.**

18 (a) COVERED INTELLIGENCE OFFICER DEFINED.—
19 In this section, the term “covered intelligence officer”
20 means—

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

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

1 (b) REQUIREMENT FOR REPORTS.—Not later than
2 72 hours after a covered intelligence officer is designated
3 as a persona non grata, the Director of National Intel-
4 ligence, in consultation with the Secretary of State, shall
5 submit to the congressional intelligence committees, the
6 Committee on Foreign Relations of the Senate, and the
7 Committee on Foreign Affairs of the House of Representa-
8 tives a notification of that designation. Each such notifica-
9 tion shall include—

- 10 (1) the date of the designation;
- 11 (2) the basis for the designation; and
- 12 (3) a justification for the expulsion.

13 **SEC. 721. REPORTS ON INTELLIGENCE COMMUNITY PAR-**
14 **TICIPATION IN VULNERABILITIES EQUITIES**
15 **PROCESS OF FEDERAL GOVERNMENT.**

16 (a) DEFINITIONS.—In this section:

17 (1) VULNERABILITIES EQUITIES POLICY AND
18 PROCESS DOCUMENT.—The term “Vulnerabilities
19 Equities Policy and Process document” means the
20 executive branch document entitled “Vulnerabilities
21 Equities Policy and Process” dated November 15,
22 2017.

23 (2) VULNERABILITIES EQUITIES PROCESS.—
24 The term “Vulnerabilities Equities Process” means
25 the interagency review of vulnerabilities, pursuant to

1 the Vulnerabilities Equities Policy and Process docu-
2 ment or any successor document.

3 (3) VULNERABILITY.—The term “vulnerability”
4 means a weakness in an information system or its
5 components (for example, system security proce-
6 dures, hardware design, and internal controls) that
7 could be exploited or could affect confidentiality, in-
8 tegrity, or availability of information.

9 (b) REPORTS ON PROCESS AND CRITERIA UNDER
10 VULNERABILITIES EQUITIES POLICY AND PROCESS.—

11 (1) IN GENERAL.—Not later than 90 days after
12 the date of the enactment of this Act, the Director
13 of National Intelligence shall submit to the congress-
14 sional intelligence committees a written report de-
15 scribing—

16 (A) with respect to each element of the in-
17 telligence community—

18 (i) the title of the official or officials
19 responsible for determining whether, pur-
20 suant to criteria contained in the Vulnera-
21 bilities Equities Policy and Process docu-
22 ment or any successor document, a vulner-
23 ability must be submitted for review under
24 the Vulnerabilities Equities Process; and

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

3 (B) the roles or responsibilities of that ele-
4 ment during a review of a vulnerability sub-
5 mitted to the Vulnerabilities Equities Process.

6 (2) CHANGES TO PROCESS OR CRITERIA.—Not
7 later than 30 days after any significant change is
8 made to the process and criteria used by any ele-
9 ment of the intelligence community for determining
10 whether to submit a vulnerability for review under
11 the Vulnerabilities Equities Process, such element
12 shall submit to the congressional intelligence com-
13 mittees a report describing such change.

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

18 (c) ANNUAL REPORTS.—

19 (1) IN GENERAL.—Not less frequently than
20 once each calendar year, the Director of National In-
21 telligence shall submit to the congressional intel-
22 ligence committees a classified report containing,
23 with respect to the previous year—

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

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

9 (C) the aggregate number, by category, of
10 the vulnerabilities excluded from review under
11 the Vulnerabilities Equities Process, as de-
12 scribed in paragraph 5.4 of the Vulnerabilities
13 Equities Policy and Process document.

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

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

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

24 (3) NON-DUPLICATION.—The Director of Na-
25 tional Intelligence may forgo submission of an an-

1 nual report required under this subsection for a cal-
2 endar year, if the Director notifies the intelligence
3 committees in writing that, with respect to the same
4 calendar year, an annual report required by para-
5 graph 4.3 of the Vulnerabilities Equities Policy and
6 Process document already has been submitted to
7 Congress, and such annual report contains the infor-
8 mation that would otherwise be required to be in-
9 cluded in an annual report under this subsection.

10 **SEC. 722. INSPECTORS GENERAL REPORTS ON CLASSIFICA-**
11 **TION.**

12 (a) **REPORTS REQUIRED.**—Not later than October 1,
13 2019, each Inspector General listed in subsection (b) shall
14 submit to the congressional intelligence committees a re-
15 port that includes, with respect to the department or agen-
16 cy of the Inspector General, analyses of the following:

17 (1) The accuracy of the application of classi-
18 fication and handling markers on a representative
19 sample of finished reports, including such reports
20 that are compartmented.

21 (2) Compliance with declassification procedures.

22 (3) The effectiveness of processes for identi-
23 fying topics of public or historical importance that
24 merit prioritization for a declassification review.

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

3 (1) The Inspector General of the Intelligence
4 Community.

5 (2) The Inspector General of the Central Intel-
6 ligence Agency.

7 (3) The Inspector General of the National Se-
8 curity Agency.

9 (4) The Inspector General of the Defense Intel-
10 ligence Agency.

11 (5) The Inspector General of the National Re-
12 connaissance Office.

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

15 **SEC. 723. REPORTS ON GLOBAL WATER INSECURITY AND**
16 **NATIONAL SECURITY IMPLICATIONS AND**
17 **BRIEFING ON EMERGING INFECTIOUS DIS-**
18 **EASE AND PANDEMICS.**

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

21 (1) REPORTS REQUIRED.—Not later than 180
22 days after the date of the enactment of this Act and
23 not less frequently than once every 5 years there-
24 after, the Director of National Intelligence shall sub-
25 mit to the congressional intelligence committees a

1 report on the implications of water insecurity on the
2 national security interest of the United States, in-
3 cluding consideration of social, economic, agricul-
4 tural, and environmental factors.

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

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

12 (i) that are, as of the date of the re-
13 port, at the greatest risk of instability,
14 conflict, human insecurity, or mass dis-
15 placement; or

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

21 (B) where challenges relating to water in-
22 security are likely to imperil the national secu-
23 rity interests of the United States or allies of
24 the United States.

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

4 (A) such stakeholders within the intel-
5 ligence community, the Department of Defense,
6 and the Department of State as the Director
7 considers appropriate; and

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

11 (4) FORM.—Each report submitted under para-
12 graph (1) shall be submitted in unclassified form,
13 but may include a classified annex.

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

16 (1) APPROPRIATE CONGRESSIONAL COMMIT-
17 TEES DEFINED.—In this subsection, the term “ap-
18 propriate congressional committees” means—

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

21 (B) the Committee on Foreign Affairs, the
22 Committee on Armed Services, and the Com-
23 mittee on Appropriations of the House of Rep-
24 resentatives; and

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

4 (2) BRIEFING.—Not later than 120 days after
5 the date of the enactment of this Act, the Director
6 of National Intelligence shall provide to the appro-
7 priate congressional committees a briefing on the an-
8 ticipated geopolitical effects of emerging infectious
9 disease (including deliberate, accidental, and natu-
10 rally occurring infectious disease threats) and
11 pandemics, and their implications on the national se-
12 curity of the United States.

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

15 (A) the economic, social, political, and se-
16 curity risks, costs, and impacts of emerging in-
17 fectious diseases on the United States and the
18 international political and economic system;

19 (B) the economic, social, political, and se-
20 curity risks, costs, and impacts of a major
21 transnational pandemic on the United States
22 and the international political and economic
23 system; and

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

4 (4) EXAMINATION OF RESPONSE CAPACITY.—In
5 examining the risks, costs, and impacts of emerging
6 infectious disease and a possible transnational pan-
7 demic under paragraph (3), the Director of National
8 Intelligence shall also examine in the briefing under
9 paragraph (2) the response capacity within affected
10 countries and the international system. In consid-
11 ering response capacity, the Director shall include—

12 (A) the ability of affected nations to effec-
13 tively detect and manage emerging infectious
14 diseases and a possible transnational pandemic;

15 (B) the role and capacity of international
16 organizations and nongovernmental organiza-
17 tions to respond to emerging infectious disease
18 and a possible pandemic, and their ability to co-
19 ordinate with affected and donor nations; and

20 (C) the effectiveness of current inter-
21 national frameworks, agreements, and health
22 systems to respond to emerging infectious dis-
23 eases and a possible transnational pandemic.

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

1 **SEC. 724. ANNUAL REPORT ON MEMORANDA OF UNDER-**
2 **STANDING BETWEEN ELEMENTS OF INTEL-**
3 **LIGENCE COMMUNITY AND OTHER ENTITIES**
4 **OF THE UNITED STATES GOVERNMENT RE-**
5 **GARDING SIGNIFICANT OPERATIONAL AC-**
6 **TIVITIES OR POLICY.**

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

9 (1) by redesignating subsection (b) as sub-
10 section (c); and

11 (2) by striking subsection (a) and inserting the
12 following:

13 “(a) IN GENERAL.—Each year, concurrent with the
14 annual budget request submitted by the President to Con-
15 gress under section 1105 of title 31, United States Code,
16 each head of an element of the intelligence community
17 shall submit to the congressional intelligence committees
18 a report that lists each memorandum of understanding or
19 other agreement regarding significant operational activi-
20 ties or policy entered into during the most recently com-
21 pleted fiscal year between or among such element and any
22 other entity of the United States Government.

23 “(b) PROVISION OF DOCUMENTS.—Each head of an
24 element of an intelligence community who receives a re-
25 quest from the Select Committee on Intelligence of the
26 Senate or the Permanent Select Committee on Intelligence

1 of the House of Representatives for a copy of a memo-
2 randum of understanding or other document listed in a
3 report submitted by the head under subsection (a) shall
4 submit to such committee the requested copy as soon as
5 practicable after receiving such request.”.

6 **SEC. 725. STUDY ON THE FEASIBILITY OF ENCRYPTING UN-**
7 **CLASSIFIED WIRELINE AND WIRELESS TELE-**
8 **PHONE CALLS.**

9 (a) **STUDY REQUIRED.**—Not later than 180 days
10 after the date of the enactment of this Act, the Director
11 of National Intelligence shall complete a study on the fea-
12 sibility of encrypting unclassified wireline and wireless
13 telephone calls between personnel in the intelligence com-
14 munity.

15 (b) **REPORT.**—Not later than 90 days after the date
16 on which the Director completes the study required by
17 subsection (a), the Director shall submit to the congres-
18 sional intelligence committees a report on the Director’s
19 findings with respect to such study.

20 **SEC. 726. MODIFICATION OF REQUIREMENT FOR ANNUAL**
21 **REPORT ON HIRING AND RETENTION OF MI-**
22 **NORITY EMPLOYEES.**

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

1 (50 U.S.C. 3050) is amended by inserting “and the pre-
2 ceding 5 fiscal years” after “fiscal year”.

3 (b) CLARIFICATION ON DISAGGREGATION OF
4 DATA.—Subsection (b) of such section is amended, in the
5 matter before paragraph (1), by striking “disaggregated
6 data by category of covered person from each element of
7 the intelligence community” and inserting “data,
8 disaggregated by category of covered person and by ele-
9 ment of the intelligence community,”.

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

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

14 (1) there should be established, through the
15 issuing of an Intelligence Community Directive or
16 otherwise, an intelligence community-wide program
17 for student loan repayment, student loan forgive-
18 ness, financial counseling, and related matters, for
19 employees of the intelligence community;

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

1 (3) such a program, including with respect to
2 eligibility requirements, should be designed so as to
3 maximize the ability of the elements of the intel-
4 ligence community to recruit, hire, and retain highly
5 qualified personnel, including with respect to mis-
6 sion-critical and hard-to-fill positions; and

7 (4) to the extent possible, such a program
8 should be uniform throughout the intelligence com-
9 munity and publicly promoted by each element of
10 the intelligence community to both current employ-
11 ees of the element as well as to prospective employ-
12 ees of the element.

13 (b) REPORT ON POTENTIAL INTELLIGENCE COMMU-
14 NITY-WIDE PROGRAM.—

15 (1) IN GENERAL.—Not later than 180 days
16 after the date of the enactment of this Act, the Di-
17 rector of National Intelligence, in cooperation with
18 the heads of the elements of the intelligence commu-
19 nity and the heads of any other appropriate depart-
20 ment or agency of the Federal Government, shall
21 submit to the congressional intelligence committees a
22 report on potentially establishing and carrying out
23 an intelligence community-wide program for student
24 loan repayment, student loan forgiveness, financial

1 counseling, and related matters, as described in sub-
2 section (a).

3 (2) MATTERS INCLUDED.—The report under
4 paragraph (1) shall include, at a minimum, the fol-
5 lowing:

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

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

12 (C) The identification of any legislative ac-
13 tion the Director determines necessary to estab-
14 lish and carry out such a program.

15 (c) ANNUAL REPORTS ON ESTABLISHED PRO-
16 GRAMS.—

17 (1) COVERED PROGRAMS DEFINED.—In this
18 subsection, the term “covered programs” means any
19 loan repayment program, loan forgiveness program,
20 financial counseling program, or similar program,
21 established pursuant to title X of the National Secu-
22 rity Act of 1947 (50 U.S.C. 3191 et seq.) or any
23 other provision of law that may be administered or
24 used by an element of the intelligence community.

1 (2) ANNUAL REPORTS REQUIRED.—Not less
2 frequently than once each year, the Director of Na-
3 tional Intelligence shall submit to the congressional
4 intelligence committees a report on the covered pro-
5 grams. Each such report shall include, with respect
6 to the period covered by the report, the following:

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

10 (B) The total amount of funds each ele-
11 ment expended for each such program.

12 (C) A description of the efforts made by
13 each element to promote each covered program
14 pursuant to both the personnel of the element
15 of the intelligence community and to prospec-
16 tive personnel.

17 **SEC. 728. REPEAL OF CERTAIN REPORTING REQUIRE-**
18 **MENTS.**

19 (a) CORRECTING LONG-STANDING MATERIAL WEAK-
20 NESSES.—Section 368 of the Intelligence Authorization
21 Act for Fiscal Year 2010 (Public Law 110–259; 50 U.S.C.
22 3051 note) is hereby repealed.

23 (b) INTERAGENCY THREAT ASSESSMENT AND CO-
24 ORDINATION GROUP.—Section 210D of the Homeland Se-
25 curity Act of 2002 (6 U.S.C. 124k) is amended—

1 (1) by striking subsection (c);

2 (2) by redesignating subsections (d) through (i)

3 as subsections (c) through (h), respectively; and

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

5 (A) in paragraph (8), by striking “; and”

6 and inserting a period; and

7 (B) by striking paragraph (9).

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

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

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

14 **SEC. 729. INSPECTOR GENERAL OF THE INTELLIGENCE**
15 **COMMUNITY REPORT ON SENIOR EXECU-**
16 **TIVES OF THE OFFICE OF THE DIRECTOR OF**
17 **NATIONAL INTELLIGENCE.**

18 (a) SENIOR EXECUTIVE SERVICE POSITION DE-
19 FINED.—In this section, the term “Senior Executive Serv-
20 ice position” has the meaning given that term in section
21 3132(a)(2) of title 5, United States Code, and includes
22 any position above the GS–15, step 10, level of the Gen-
23 eral Schedule under section 5332 of such title.

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

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

5 (c) MATTERS INCLUDED.—The report under sub-
6 section (b) shall include the following:

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

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

12 (3) A discussion of how the number of the Sen-
13 ior Executive Service positions in the Office compare
14 to the number of senior positions at comparable or-
15 ganizations.

16 (d) COOPERATION.—The Director of National Intel-
17 ligence shall provide to the Inspector General of the Intel-
18 ligence Community any information requested by the In-
19 spector General of the Intelligence Community that is nec-
20 essary to carry out this section by not later than 14 cal-
21 endar days after the date on which the Inspector General
22 of the Intelligence Community makes such request.

1 **SEC. 730. BRIEFING ON FEDERAL BUREAU OF INVESTIGA-**
2 **TION OFFERING PERMANENT RESIDENCE TO**
3 **SOURCES AND COOPERATORS.**

4 Not later than 30 days after the date of the enact-
5 ment of this Act, the Director of the Federal Bureau of
6 Investigation shall provide to the congressional intelligence
7 committees a briefing on the ability of the Federal Bureau
8 of Investigation to offer, as an inducement to assisting the
9 Bureau, permanent residence within the United States to
10 foreign individuals who are sources or cooperators in coun-
11 terintelligence or other national security-related investiga-
12 tions. The briefing shall address the following:

13 (1) The extent to which the Bureau may make
14 such offers, whether independently or in conjunction
15 with other agencies and departments of the United
16 States Government, including a discussion of the au-
17 thorities provided by section 101(a)(15)(S) of the
18 Immigration and Nationality Act (8 U.S.C.
19 1101(a)(15)(S)), section 7 of the Central Intel-
20 ligence Agency Act (50 U.S.C. 3508), and any other
21 provision of law under which the Bureau may make
22 such offers.

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

1 (3) The sufficiency of such policies and prac-
2 tices with respect to inducing individuals to cooper-
3 ate with, serve as sources for such investigations, or
4 both.

5 (4) Whether the Director recommends any leg-
6 islative actions to improve such policies and prac-
7 tices, particularly with respect to the counterintel-
8 ligence efforts of the Bureau.

9 **SEC. 731. INTELLIGENCE ASSESSMENT OF NORTH KOREA**
10 **REVENUE SOURCES.**

11 (a) **ASSESSMENT REQUIRED.**—Not later than 180
12 days after the date of the enactment of this Act, the Direc-
13 tor of National Intelligence, in coordination with the As-
14 sistant Secretary of State for Intelligence and Research
15 and the Assistant Secretary of the Treasury for Intel-
16 ligence and Analysis, shall produce an intelligence assess-
17 ment of the revenue sources of the North Korean regime.
18 Such assessment shall include revenue from the following
19 sources:

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

21 (2) The provision of fishing rights to North Ko-
22 rean territorial waters.

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

1 (4) Trade in textiles.

2 (5) Sales of conventional defense articles and
3 services.

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

6 (7) Other types of manufacturing for export, as
7 the Director of National Intelligence considers ap-
8 propriate.

9 (8) The exportation of workers from North
10 Korea in a manner intended to generate significant
11 revenue, directly or indirectly, for use by the govern-
12 ment of North Korea.

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

16 (10) The provision of services, including bank-
17 ing and other support, including by entities located
18 in the Russian Federation, China, and Iran.

19 (11) Online commercial activities of the Govern-
20 ment of North Korea, including online gambling.

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

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

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

2 (2) Financial and non-financial networks, in-
3 cluding supply chain management, transportation,
4 and facilitation, through which North Korea accesses
5 the United States and international financial sys-
6 tems and repatriates and exports capital, goods, and
7 services.

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

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

15 **SEC. 732. REPORT ON POSSIBLE EXPLOITATION OF VIR-**
16 **TUAL CURRENCIES BY TERRORIST ACTORS.**

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

19 (b) REPORT.—Not later than 1 year after the date
20 of the enactment of this Act, the Director of National In-
21 telligence, in consultation with the Secretary of the Treas-
22 ury, shall submit to Congress a report on the possible ex-
23 ploitation of virtual currencies by terrorist actors. Such
24 report shall include the following elements:

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

4 (2) An assessment of the use by terrorist orga-
5 nizations and State sponsors of terrorism of virtual
6 currencies compared to the use by such organiza-
7 tions and States of other forms of financing to sup-
8 port operations, including an assessment of the col-
9 lection posture of the intelligence community on the
10 use of virtual currencies by such organizations and
11 States.

12 (3) A description of any existing legal impedi-
13 ments that inhibit or prevent the intelligence com-
14 munity from collecting information on or helping
15 prevent the use of virtual currencies by international
16 terrorist organizations and State sponsors of ter-
17 rorism and an identification of any gaps in existing
18 law that could be exploited for illicit funding by such
19 organizations and States.

20 (c) FORM OF REPORT.—The report required by sub-
21 section (b) shall be submitted in unclassified form, but
22 may include a classified annex.

1 **SEC. 733. INCLUSION OF DISCIPLINARY ACTIONS IN AN-**
 2 **NUAL REPORT RELATING TO SECTION 702 OF**
 3 **THE FOREIGN INTELLIGENCE SURVEIL-**
 4 **LANCE ACT OF 1978.**

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

11 **Subtitle C—Other Matters**

12 **SEC. 741. PUBLIC INTEREST DECLASSIFICATION BOARD.**

13 Section 710(b) of the Public Interest Declassification
 14 Act of 2000 (Public Law 106–567; 50 U.S.C. 3161 note)
 15 is amended by striking “December 31, 2018” and insert-
 16 ing “December 31, 2028”.

17 **SEC. 742. SECURING ENERGY INFRASTRUCTURE.**

18 (a) DEFINITIONS.—In this section:

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

22 (A) the congressional intelligence commit-
 23 tees;

24 (B) the Committee on Homeland Security
 25 and Governmental Affairs and the Committee

1 on Energy and Natural Resources of the Sen-
2 ate; and

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

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

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

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

24 (5) NATIONAL LABORATORY.—The term “Na-
25 tional Laboratory” has the meaning given the term

1 in section 2 of the Energy Policy Act of 2005 (42
2 U.S.C. 15801).

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

5 (7) SECRETARY.—Except as otherwise specifi-
6 cally provided, the term “Secretary” means the Sec-
7 retary of Energy.

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

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

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

22 (2) evaluating technology and standards, in
23 partnership with covered entities, to isolate and de-
24 fend industrial control systems of covered entities

1 from security vulnerabilities and exploits in the most
2 critical systems of the covered entities, including—

- 3 (A) analog and nondigital control systems;
- 4 (B) purpose-built control systems; and
- 5 (C) physical controls.

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

8 (1) ESTABLISHMENT.—The Secretary shall es-
9 tablish a working group—

10 (A) to evaluate the technology and stand-
11 ards used in the Program under subsection
12 (b)(2); and

13 (B) to develop a national cyber-informed
14 engineering strategy to isolate and defend cov-
15 ered entities from security vulnerabilities and
16 exploits in the most critical systems of the cov-
17 ered entities.

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

23 (A) The Department of Energy.

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

4 (C)(i) The Department of Homeland Secu-
5 rity; or

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

8 (D) The North American Electric Reli-
9 ability Corporation.

10 (E) The Nuclear Regulatory Commission.

11 (F)(i) The Office of the Director of Na-
12 tional Intelligence; or

13 (ii) the intelligence community (as defined
14 in section 3 of the National Security Act of
15 1947 (50 U.S.C. 3003)).

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

17 (ii) the Assistant Secretary of Defense for
18 Homeland Security and America's Security Af-
19 fairs.

20 (H) A State or regional energy agency.

21 (I) A national research body or academic
22 institution.

23 (J) The National Laboratories.

24 (d) REPORTS ON THE PROGRAM.—

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

6 (A) describes the results of the Program;

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

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

12 (2) FINAL REPORT.—Not later than 2 years
13 after the date on which funds are first disbursed
14 under the Program, the Secretary shall submit to
15 the appropriate congressional committees a final re-
16 port that—

17 (A) describes the results of the Program;

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

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

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

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

3 (2) shall be exempt from disclosure under sec-
4 tion 552 of title 5, United States Code, or any provi-
5 sion of any State, Tribal, or local freedom of infor-
6 mation law, open government law, open meetings
7 law, open records law, sunshine law, or similar law
8 requiring the disclosure of information or records;
9 and

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

15 (f) PROTECTION FROM LIABILITY.—

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

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

21 (B) shall be promptly dismissed by the ap-
22 plicable court.

23 (2) VOLUNTARY ACTIVITIES.—Nothing in this
24 section subjects any covered entity to liability for not

1 engaging in the voluntary activities authorized under
2 subsection (b).

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

7 (h) AUTHORIZATION OF APPROPRIATIONS.—

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

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

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

17 **SEC. 743. BUG BOUNTY PROGRAMS.**

18 (a) DEFINITIONS.—In this section:

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

22 (A) the congressional intelligence commit-
23 tees;

1 (B) the Committee on Armed Services and
2 the Committee on Homeland Security and Gov-
3 ernmental Affairs of the Senate; and

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

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

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

17 (b) BUG BOUNTY PROGRAM PLAN.—

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

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

3 (A) an assessment of—

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

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

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

17 **SEC. 744. MODIFICATION OF AUTHORITIES RELATING TO**
18 **THE NATIONAL INTELLIGENCE UNIVERSITY.**

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

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

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

1 (2) COMPENSATION PLAN.—The Secretary of
2 Defense shall provide each person employed as a
3 full-time professor, instructor, or lecturer at the Na-
4 tional Intelligence University on the date of the en-
5 actment of this Act an opportunity to elect to be
6 paid under the compensation plan in effect on the
7 day before the date of the enactment of this Act
8 (with no reduction in pay) or under the authority of
9 section 1595 of title 10, United States Code, as
10 amended by paragraph (1).

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

14 “(d) ACCEPTANCE OF FACULTY RESEARCH
15 GRANTS.—The Secretary of Defense may authorize the
16 President of the National Intelligence University to accept
17 qualifying research grants in the same manner and to the
18 same degree as the President of the National Defense Uni-
19 versity under section 2165(e) of this title.”.

20 (c) PILOT PROGRAM ON ADMISSION OF PRIVATE
21 SECTOR CIVILIANS TO RECEIVE INSTRUCTION.—

22 (1) PILOT PROGRAM REQUIRED.—

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

1 carrying out a pilot program to assess the
2 feasibility and advisability of permitting eligible
3 private sector employees who work in organiza-
4 tions relevant to national security to receive in-
5 struction at the National Intelligence Univer-
6 sity.

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

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

15 (D) NUMBER OF PARTICIPANTS.—No more
16 than the equivalent of 35 full-time student posi-
17 tions may be filled at any one time by private
18 sector employees enrolled under the pilot pro-
19 gram.

20 (E) DIPLOMAS AND DEGREES.—Upon suc-
21 cessful completion of the course of instruction
22 in which enrolled, any such private sector em-
23 ployee may be awarded an appropriate diploma
24 or degree under section 2161 of title 10, United
25 States Code.

1 (2) ELIGIBLE PRIVATE SECTOR EMPLOYEES.—

2 (A) IN GENERAL.—For purposes of this
3 subsection, an eligible private sector employee is
4 an individual employed by a private firm that is
5 engaged in providing to the Department of De-
6 fense, the intelligence community, or other Gov-
7 ernment departments or agencies significant
8 and substantial intelligence or defense-related
9 systems, products, or services or whose work
10 product is relevant to national security policy or
11 strategy.

12 (B) LIMITATION.—Under this subsection,
13 a private sector employee admitted for instruc-
14 tion at the National Intelligence University re-
15 mains eligible for such instruction only so long
16 as that person remains employed by the same
17 firm, holds appropriate security clearances, and
18 complies with any other applicable security pro-
19 tocols.

20 (3) ANNUAL CERTIFICATION BY SECRETARY OF
21 DEFENSE.—Under the pilot program, private sector
22 employees may receive instruction at the National
23 Intelligence University during any academic year
24 only if, before the start of that academic year, the
25 Secretary of Defense determines, and certifies to the

1 Committee on Armed Services of the Senate and the
2 Committee on Armed Services of the House of Rep-
3 resentatives, that providing instruction to private
4 sector employees under this section during that year
5 will further the national security interests of the
6 United States.

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

9 (A) the curriculum in which private sector
10 employees may be enrolled under the pilot pro-
11 gram is not readily available through other
12 schools and concentrates on national security-
13 relevant issues; and

14 (B) the course offerings at the National
15 Intelligence University are determined by the
16 needs of the Department of Defense and the in-
17 telligence community.

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

21 (A) is at least the rate charged for employ-
22 ees of the United States outside the Depart-
23 ment of Defense, less infrastructure costs; and

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

1 (6) STANDARDS OF CONDUCT.—While receiving
2 instruction at the National Intelligence University,
3 students enrolled under the pilot program, to the ex-
4 tent practicable, are subject to the same regulations
5 governing academic performance, attendance, norms
6 of behavior, and enrollment as apply to Government
7 civilian employees receiving instruction at the univer-
8 sity.

9 (7) USE OF FUNDS.—

10 (A) IN GENERAL.—Amounts received by
11 the National Intelligence University for instruc-
12 tion of students enrolled under the pilot pro-
13 gram shall be retained by the university to de-
14 fray the costs of such instruction.

15 (B) RECORDS.—The source, and the dis-
16 position, of such funds shall be specifically iden-
17 tified in records of the university.

18 (8) REPORTS.—

19 (A) ANNUAL REPORTS.—Each academic
20 year in which the pilot program is carried out,
21 the Secretary shall submit to the congressional
22 intelligence committees, the Committee on
23 Armed Services of the Senate, and the Com-
24 mittee on Armed Services of the House of Rep-
25 resentatives a report on the number of eligible

1 private sector employees participating in the
2 pilot program.

3 (B) FINAL REPORT.—Not later than 90
4 days after the date of the conclusion of the pilot
5 program, the Secretary shall submit to the con-
6 gressional intelligence committees, the Com-
7 mittee on Armed Services of the Senate, and
8 the Committee on Armed Services of the House
9 of Representatives a report on the findings of
10 the Secretary with respect to the pilot program.

11 Such report shall include—

12 (i) the findings of the Secretary with
13 respect to the feasibility and advisability
14 of permitting eligible private sector em-
15 ployees who work in organizations relevant
16 to national security to receive instruction
17 at the National Intelligence University;
18 and

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

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

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

1 (1) by inserting after the item relating to sec-
2 tion 2 the following new item:

“Sec. 3. Definitions.”;

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

4 (3) by striking the item relating to section
5 113B and inserting the following new item:

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

6 (4) by striking the items relating to sections
7 202, 203, 204, 208, 209, 210, 211, 212, 213, and
8 214; and

9 (5) by inserting after the item relating to sec-
10 tion 311 the following new item:

“Sec. 312. Repealing and saving provisions.”.

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

13 (1) in section 102A—

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

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

20 (2) in section 106—

21 (A) by inserting “**SEC. 106.**” before “(a)”;

22 and

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

4 (3) by striking section 107;

5 (4) in section 108(c), by striking “in both a
6 classified and an unclassified form” and inserting
7 “to Congress in classified form, but may include an
8 unclassified summary”;

9 (5) in section 112(c)(1), by striking “section
10 103(c)(7)” and inserting “section 102A(i)”;

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

12 **“SEC. 201. DEPARTMENT OF DEFENSE.**

13 “Except to the extent inconsistent with the provisions
14 of this Act or other provisions of law, the provisions of
15 title 5, United States Code, shall be applicable to the De-
16 partment of Defense.”;

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

19 (8) in section 206, by striking “(a)”;

20 (9) in section 207, by striking “(c)”;

21 (10) in section 308(a), by striking “this Act”
22 and inserting “sections 2, 101, 102, 103, and 303
23 of this Act”;

24 (11) by redesignating section 411 as section
25 312;

1 (12) in section 503—

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

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

5 (ii) by moving the margins of sub-
6 paragraph (B) of such paragraph 2 ems to
7 the left; and

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

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

14 **SEC. 746. TECHNICAL AMENDMENTS RELATED TO THE DE-**
15 **PARTMENT OF ENERGY.**

16 (a) NATIONAL NUCLEAR SECURITY ADMINISTRATION
17 ACT.—

18 (1) CLARIFICATION OF FUNCTIONS OF THE AD-
19 MINISTRATOR FOR NUCLEAR SECURITY.—Subsection
20 (b) of section 3212 of the National Nuclear Security
21 Administration Act (50 U.S.C. 2402(b)) is amend-
22 ed—

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

1 (B) by redesignating paragraphs (13)
2 through (19) as paragraphs (11) through (17),
3 respectively.

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

7 (A) by striking “Administration” and in-
8 serting “Department”; and

9 (B) by inserting “Intelligence and” after
10 “the Office of”.

11 (b) ATOMIC ENERGY DEFENSE ACT.—Section
12 4524(b)(2) of the Atomic Energy Defense Act (50 U.S.C.
13 2674(b)(2)) is amended by inserting “Intelligence and”
14 after “The Director of”.

15 (c) NATIONAL SECURITY ACT OF 1947.—Paragraph
16 (2) of section 106(b) of the National Security Act of 1947
17 (50 U.S.C. 3041(b)(2)) is amended—

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

20 (2) by striking subparagraph (F);

21 (3) by redesignating subparagraphs (G), (H),
22 and (I) as subparagraphs (F), (G), and (H), respec-
23 tively; and

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

4 **SEC. 747. SENSE OF CONGRESS ON NOTIFICATION OF CER-**
5 **TAIN DISCLOSURES OF CLASSIFIED INFOR-**
6 **MATION.**

7 (a) DEFINITIONS.—In this section:

8 (1) ADVERSARY FOREIGN GOVERNMENT.—The
9 term “adversary foreign government” means the
10 government of any of the following foreign countries:

11 (A) North Korea.

12 (B) Iran.

13 (C) China.

14 (D) Russia.

15 (E) Cuba.

16 (2) COVERED CLASSIFIED INFORMATION.—The
17 term “covered classified information” means classi-
18 fied information that was—

19 (A) collected by an element of the intel-
20 ligence community; or

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

24 (3) ESTABLISHED INTELLIGENCE CHANNELS.—

25 The term “established intelligence channels” means

1 methods to exchange intelligence to coordinate for-
2 eign intelligence relationships, as established pursu-
3 ant to law by the Director of National Intelligence,
4 the Director of the Central Intelligence Agency, the
5 Director of the National Security Agency, or other
6 head of an element of the intelligence community.

7 (4) INDIVIDUAL IN THE EXECUTIVE BRANCH.—
8 The term “individual in the executive branch”
9 means any officer or employee of the executive
10 branch, including individuals—

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

13 (B) appointed to a position by an indi-
14 vidual described in subparagraph (A); or

15 (C) serving in the civil service or the Sen-
16 ior Executive Service (or similar service for sen-
17 ior executives of particular departments or
18 agencies).

19 (b) FINDINGS.—Congress finds that section 502 of
20 the National Security Act of 1947 (50 U.S.C. 3092) re-
21 quires elements of the intelligence community to keep the
22 congressional intelligence committees “fully and currently
23 informed” about all “intelligence activities” of the United
24 States, and to “furnish to the congressional intelligence
25 committees any information or material concerning intel-

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

4 (c) SENSE OF CONGRESS.—It is the sense of Con-
5 gress that—

6 (1) section 502 of the National Security Act of
7 1947 (50 U.S.C. 3092), together with other intel-
8 ligence community authorities, obligates an element
9 of the intelligence community to submit to the con-
10 gressional intelligence committees written notifica-
11 tion, by not later than 7 days after becoming aware,
12 that an individual in the executive branch has dis-
13 closed covered classified information to an official of
14 an adversary foreign government using methods
15 other than established intelligence channels; and

16 (2) each such notification should include—

17 (A) the date and place of the disclosure of
18 classified information covered by the notifica-
19 tion;

20 (B) a description of such classified infor-
21 mation;

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

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

3 **SEC. 748. SENSE OF CONGRESS ON CONSIDERATION OF ES-**
4 **PIONAGE ACTIVITIES WHEN CONSIDERING**
5 **WHETHER OR NOT TO PROVIDE VISAS TO**
6 **FOREIGN INDIVIDUALS TO BE ACCREDITED**
7 **TO A UNITED NATIONS MISSION IN THE**
8 **UNITED STATES.**

9 It is the sense of the Congress that the Secretary of
10 State, in considering whether or not to provide a visa to
11 a foreign individual to be accredited to a United Nations
12 mission in the United States, should consider—

13 (1) known and suspected intelligence activities,
14 espionage activities, including activities constituting
15 precursors to espionage, carried out by the indi-
16 vidual against the United States, foreign allies of the
17 United States, or foreign partners of the United
18 States; and

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

21 **SEC. 749. SENSE OF CONGRESS ON WIKILEAKS.**

22 It is the sense of Congress that WikiLeaks and the
23 senior leadership of WikiLeaks resemble a nonstate hostile

- 1 intelligence service often abetted by state actors and
- 2 should be treated as such a service by the United States.

○