To authorize appropriations for fiscal year 2021 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 8, 2020

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

A BILL

To authorize appropriations for fiscal year 2021 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the “Intelligence Authorization Act for Fiscal Year 2021”.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,
(b) **TABLE OF CONTENTS.**—The table of contents for this Act is as follows:

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

**TITLE I—INTELLIGENCE ACTIVITIES**
Sec. 101. Authorization of appropriations.
Sec. 102. Classified Schedule of Authorizations.
Sec. 103. Intelligence Community Management Account.

**TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM**
Sec. 201. Authorization of appropriations.

**TITLE III—INTELLIGENCE COMMUNITY MATTERS**
Subtitle A—General Intelligence Community Matters
Sec. 301. Restriction on conduct of intelligence activities.
Sec. 302. Increase in employee compensation and benefits authorized by law.
Sec. 304. Continuity of operations plans for certain elements of the intelligence community in the case of a national emergency.
Sec. 305. Application of Executive Schedule level III to positions of Director of National Security Agency and Director of National Reconnaissance Office.
Sec. 306. National Intelligence University.
Sec. 307. Requiring facilitation of establishment of Social Media Data and Threat Analysis Center.
Sec. 308. Data collection on attrition in intelligence community.
Sec. 309. Limitation on delegation of responsibility for program management of information-sharing environment.
Sec. 310. Improvements to provisions relating to intelligence community information technology environment.
Sec. 311. Requirements and authorities for Director of the Central Intelligence Agency to improve education in science, technology, engineering, arts, and mathematics.

Subtitle B—Inspector General of the Intelligence Community
Sec. 321. Prohibition against disclosure of whistleblower identity as reprisal against whistleblower disclosure by employees and contractors in intelligence community.
Sec. 322. Clarification of standards regarding whistleblower complaints and information of urgent concern received by Inspector General of the Intelligence Community.
Sec. 323. Clarification regarding submittal of complaints and information by whistleblowers in the intelligence community to Congress.
Sec. 324. Limitation on sharing of intelligence community whistleblower complaints with persons named in such complaints.
Subtitle C—Reports and Assessments Pertaining to Intelligence Community

Sec. 331. Assessment by the Comptroller General of the United States on efforts of the intelligence community and the Department of Defense to identify and mitigate risks posed to the intelligence community and the Department by the use of direct-to-consumer genetic testing by the Government of the People’s Republic of China.

Sec. 332. Report on use by intelligence community of hiring flexibilities and expedited human resources practices to assure quality and diversity in the workforce of the intelligence community.

Sec. 333. Report on signals intelligence priorities and requirements.

Sec. 334. Assessment of demand for student loan repayment program benefit.

Sec. 335. Assessment of intelligence community demand for child care.

Sec. 336. Open source intelligence strategies and plans for the intelligence community.

Sec. 337. Plan for establishing an element of the intelligence community within the United States Space Force.

TITLE IV—SECURITY CLEARANCES AND TRUSTED WORKFORCE

Sec. 401. Exclusivity, consistency, and transparency in security clearance procedures, and right to appeal.

Sec. 402. Establishing process parity for security clearance revocations.

Sec. 403. Federal policy on sharing of derogatory information pertaining to contractor employees in the trusted workforce.

TITLE V—REPORTS AND OTHER MATTERS

Sec. 501. Secure and trusted technology.

Sec. 502. Report on attempts by foreign adversaries to build telecommunications and cybersecurity equipment and services for, or to provide such equipment and services to, certain allies of the United States.

Sec. 503. Report on threats posed by use by foreign governments and entities of commercially available cyber intrusion and surveillance technology.

Sec. 504. Reports on recommendations of the Cyberspace Solarium Commission.

Sec. 505. Assessment of critical technology trends relating to artificial intelligence, microchips, and semiconductors and related supply chains.

Sec. 506. Duty to report counterintelligence threats to campaigns.

Sec. 507. Combating Chinese influence operations in the United States and strengthening civil liberties protections.

Sec. 508. Annual report on corrupt activities of senior officials of the Chinese Communist Party.

Sec. 509. Report on corrupt activities of Russian and other Eastern European oligarchs.


Sec. 512. Report on Iranian activities relating to nuclear nonproliferation.

Sec. 513. Sense of Congress on Third Option Foundation.
SEC. 2. DEFINITIONS.

In this Act:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term "congressional intelligence committees" has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

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

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2021 for the conduct of the intelligence and intelligence-related activities of the following elements of the United States Government:

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

(2) The Central Intelligence Agency.

(3) The Department of Defense.

(4) The Defense Intelligence Agency.


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

(8) The Department of State.

(9) The Department of the Treasury.

(10) The Department of Energy.

(11) The Department of Justice.


(13) The Drug Enforcement Administration.

(14) The National Reconnaissance Office.

(15) The National Geospatial-Intelligence Agency.


SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) Specifications of Amounts.—The amounts authorized to be appropriated under section 101 for the conduct of the intelligence activities of the elements listed in paragraphs (1) through (16) of section 101, are those specified in the classified Schedule of Authorizations prepared to accompany this Act.

(b) Availability of Classified Schedule of Authorizations.—

(1) Availability.—The classified Schedule of Authorizations referred to in subsection (a) shall be made available to the Committee on Appropriations of the Senate, the Committee on Appropriations of the House of Representatives, and to the President.
(2) Distribution by the President.—Subject to paragraph (3), the President shall provide for suitable distribution of the classified Schedule of Authorizations referred to in subsection (a), or of appropriate portions of such Schedule, within the executive branch of the Federal Government.

(3) Limits on Disclosure.—The President shall not publicly disclose the classified Schedule of Authorizations or any portion of such Schedule except—

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

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

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) Authorization of Appropriations.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2021 the sum of $731,200,000.

(b) Classified Authorization of Appropriations.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Ac-
count by subsection (a), there are authorized to be appro-
priated for the Intelligence Community Management Ac-
count for fiscal year 2021 such additional amounts as are
specified in the classified Schedule of Authorizations re-
ferred to in section 102(a).

**TITLE II—CENTRAL INTEL-
LIGENCE AGENCY RETIRE-
MENT AND DISABILITY SYS-
TEM**

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

There is authorized to be appropriated for the Cen-
tral Intelligence Agency Retirement and Disability Fund
$514,000,000 for fiscal year 2021.

**TITLE III—INTELLIGENCE
COMMUNITY MATTERS**

**Subtitle A—General Intelligence
Community Matters**

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

The authorization of appropriations by this Act shall
not be deemed to constitute authority for the conduct of
any intelligence activity which is not otherwise authorized
by the Constitution or the laws of the United States.
SEC. 302. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY LAW.

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

SEC. 303. CLARIFICATION OF AUTHORITIES AND RESPONSIBILITIES OF NATIONAL MANAGER FOR NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY.

(a) Delegation of Authorities and Responsibilities.—

(1) In general.—The National Manager for National Security Telecommunications and Information Systems Security, as designated by National Security Directive 42 (signed by the President on July 5, 1990), may delegate the authorities and responsibilities assigned the National Manager under such Directive to a Deputy National Manager for National Security Telecommunications and Information Systems Security.

(2) Limitation.—The authority to delegate under paragraph (1) may not be further delegated below the Deputy National Manager.

(b) Scope of Responsibilities.—
(1) National Manager.—

(A) In general.—In carrying out the authorities and responsibilities of the National Manager under National Security Directive 42, the National Manager may supervise, oversee, or execute, either directly or indirectly, the Information Systems Security Program.

(B) Limitation.—In carrying out the authorities and responsibilities of the National Manager under National Security Directive 42, the National Manager shall not supervise, oversee, or execute, either directly or indirectly, any aspect of the National Intelligence Program or the Military Intelligence Program, except to the degree that doing so is necessary to supervise, oversee, or execute the Information Systems Security Program as described in subparagraph (A).

(2) Deputy National Manager.—

(A) In general.—In a case in which the National Manager delegates authorities and responsibilities to a Deputy National Manager under subsection (a)(1), the Deputy National Manager may supervise, oversee, or execute, ei-
ther directly or indirectly, the Information Systems Security Program.

(B) LIMITATION.—In a case described in subparagraph (A), the Deputy National Manager shall not supervise, oversee, or execute, either directly or indirectly, any aspect of the National Intelligence Program or the Military Intelligence Program, except to the degree that doing so is necessary to supervise, oversee, or execute the Information Systems Security Program as described in subparagraph (A).

SEC. 304. CONTINUITY OF OPERATIONS PLANS FOR CERTAIN ELEMENTS OF THE INTELLIGENCE COMMUNITY IN THE CASE OF A NATIONAL EMERGENCY.

(a) Definition of Covered National Emergency.—In this section, the term “covered national emergency” means the following:

(1) A major disaster declared by the President under section 401 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5170).

(2) An emergency declared by the President under section 501 of the Robert T. Stafford Disaster
Relief and Emergency Assistance Act (42 U.S.C. 5191).

(3) A national emergency declared by the President under the National Emergencies Act (50 U.S.C. 1601 et seq.).

(4) A public health emergency declared under section 319 of the Public Health Service Act (42 U.S.C. 247d).

(b) IN GENERAL.—The Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the National Reconnaissance Office, the Director of the Defense Intelligence Agency, the Director of the National Security Agency, and the Director of the National Geospatial-Intelligence Agency shall each establish continuity of operations plans for use in the case of covered national emergencies for the element of the intelligence community concerned.

(c) SUBMISSION TO CONGRESS.—

(1) DIRECTOR OF NATIONAL INTELLIGENCE AND DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY.—Not later than 7 days after the date on which a covered national emergency is declared, the Director of National Intelligence and the Director of the Central Intelligence Agency shall each submit to the congressional intelligence committees the plan
established under subsection (b) for that emergency for the element of the intelligence community concerned.

(2) **DIRECTOR OF NATIONAL RECONNAISSANCE OFFICE, DIRECTOR OF DEFENSE INTELLIGENCE AGENCY, DIRECTOR OF NATIONAL SECURITY AGENCY, AND DIRECTOR OF NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY.**—Not later than 7 days after the date on which a covered national emergency is declared, the Director of the National Reconnaissance Office, the Director of the Defense Intelligence Agency, the Director of the National Security Agency, and the Director of the National Geospatial-Intelligence Agency shall each submit the plan established under subsection (b) for that emergency for the element of the intelligence community concerned to the following:

(A) The congressional intelligence committees.

(B) The Committee on Armed Services of the Senate.

(C) The Committee on Armed Services of the House of Representatives.

(d) **UPDATES.**—During a covered national emergency, the Director of National Intelligence, the Director
of the Central Intelligence Agency, the Director of the National Reconnaissance Office, the Director of the Defense Intelligence Agency, the Director of the National Security Agency, and the Director of the National Geospatial-Intelligence Agency shall each submit any updates to the plans submitted under subsection (c)—

(1) in accordance with that subsection; and

(2) in a timely manner consistent with section 501 of the National Security Act of 1947 (50 U.S.C. 3091).

SEC. 305. APPLICATION OF EXECUTIVE SCHEDULE LEVEL III TO POSITIONS OF DIRECTOR OF NATIONAL SECURITY AGENCY AND DIRECTOR OF NATIONAL RECONNAISSANCE OFFICE.

Section 5314 of title 5, United States Code, is amended by adding at the end the following:

“Director of the National Security Agency/Central Security Service.

“Director of the National Reconnaissance Office.”.

SEC. 306. NATIONAL INTELLIGENCE UNIVERSITY.

(a) IN GENERAL.—Title X of the National Security Act of 1947 (50 U.S.C. 3191 et seq.) is amended by adding at the end the following:
“Subtitle D—National Intelligence University

“SEC. 1031. TRANSFER DATE.

“In this subtitle, the term ‘transfer date’ means the date on which the National Intelligence University is transferred from the Defense Intelligence Agency to the Director of National Intelligence under section 5324(a) of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92).

“SEC. 1032. DEGREE-GRANTING AUTHORITY.

“(a) IN GENERAL.—Beginning on the transfer date, under regulations prescribed by the Director of National Intelligence, the President of the National Intelligence University may, upon the recommendation of the faculty of the University, confer appropriate degrees upon graduates who meet the degree requirements.

“(b) LIMITATION.—A degree may not be conferred under this section unless—

“(1) the Secretary of Education has recommended approval of the degree in accordance with the Federal Policy Governing Granting of Academic Degrees by Federal Agencies; and

“(2) the University is accredited by the appropriate academic accrediting agency or organization
to award the degree, as determined by the Secretary
of Education.

“(c) CONGRESSIONAL NOTIFICATION REQUIRE-
MENTS.—

“(1) ACTIONS ON NONACREDITATION.—Begin-
ning on the transfer date, the Director shall prompt-
ly—

“(A) notify the congressional intelligence
committees of any action by the Middle States
Commission on Higher Education, or other ap-
propriate academic accrediting agency or orga-
nization, to not accredit the University to award
any new or existing degree; and

“(B) submit to such committees a report
containing an explanation of any such action.

“(2) MODIFICATION OR REDESIGNATION OF DE-
GREE GRANTING AUTHORITY.—Beginning on the
transfer date, upon any modification or redesigna-
tion of existing degree-granting authority, the Direc-
tor shall submit to the congressional intelligence
committees a report containing—

“(A) the rationale for the proposed modi-
fication or redesignation; and
“(B) any subsequent recommendation of
the Secretary of Education with respect to the
proposed modification or redesignation.

"SEC. 1033. FACULTY MEMBERS, EMPLOYMENT AND COM-
PENSATION.

“(a) Authority of Director.—Beginning on the
transfer date, the Director of National Intelligence may
employ as many professors, instructors, and lecturers at
the National Intelligence University as the Director con-
siders necessary.

“(b) Compensation of Faculty Members.—The
compensation of persons employed under this section shall
be as prescribed by the Director.

“(c) Compensation Plan.—The Director shall pro-
vide each person employed as a professor, instructor, or
lecturer at the University on the transfer date an oppor-
tunity to elect to be paid under the compensation plan in
effect on the day before the transfer date (with no reduc-
tion in pay) or under the authority of this section.

"SEC. 1034. ACCEPTANCE OF FACULTY RESEARCH GRANTS.

“The Director of National Intelligence may authorize
the President of the National Intelligence University to
accept qualifying research grants in the same manner and
to the same degree as the President of the National De-
S 3905 RS

fense University under section 2165(e) of title 10, United States Code.

“SEC. 1035. CONTINUED APPLICABILITY OF THE FEDERAL ADVISORY COMMITTEE ACT TO THE BOARD OF VISITORS.

“The Federal Advisory Committee Act (5 U.S.C. App.) shall continue to apply to the Board of Visitors of the National Intelligence University on and after the transfer date.”.

(b) CONFORMING AMENDMENTS.—Section 5324 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92) is amended—

(1) in subsection (b)(1)(C), by striking “subsection (e)(2)” and inserting “section 1032(b) of the National Security Act of 1947”;

(2) by striking subsections (e) and (f); and

(3) by redesignating subsections (g) and (h) as subsections (e) and (f), respectively.

(c) CLERICAL AMENDMENT.—The table of contents of the National Security Act of 1947 is amended by inserting after the item relating to section 1024 the following:

“Subtitle D—National Intelligence University

Sec. 1031. Transfer date.
Sec. 1032. Degree-granting authority.
Sec. 1033. Faculty members; employment and compensation.
Sec. 1034. Acceptance of faculty research grants.
Sec. 1035. Continued applicability of the Federal Advisory Committee Act to the Board of Visitors.”.
SEC. 307. REQUIRING FACILITATION OF ESTABLISHMENT OF SOCIAL MEDIA DATA AND THREAT ANALYSIS CENTER.

(a) Requirement to Facilitate Establishment.—Subsection (c)(1) of section 5323 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92) is amended, by striking “may” and inserting “shall”.

(b) Deadline to Facilitate Establishment.—Such subsection is further amended by striking “The Director” and inserting “Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2021, the Director”.

(c) Conforming Amendments.—

(1) Reporting.—Subsection (d) of such section is amended—

(A) in the matter before paragraph (1), by striking “If the Director” and all that follows through “the Center, the” and inserting “The”; and

(B) in paragraph (1), by striking “180 days after the date of the enactment of this Act” and inserting “180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2021”.

S 3905 RS
(2) FUNDING.—Subsection (f) of such section is amended by striking “fiscal year 2020 and 2021” and inserting “fiscal year 2021 and 2022”.

(3) CLERICAL.—Subsection (c) of such section is amended—

(A) in the subsection heading, by striking “AUTHORITY” and inserting “REQUIREMENT”;

and

(B) in paragraph (1), in the paragraph heading, by striking “AUTHORITY” and inserting “REQUIREMENT”.

SEC. 308. DATA COLLECTION ON ATTRITION IN INTELLIGENCE COMMUNITY.

(a) STANDARDS FOR DATA COLLECTION.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall establish standards for collecting data relating to attrition in the intelligence community workforce across demographics, specialties, and length of service.

(2) INCLUSION OF CERTAIN CANDIDATES.—The Director shall include, in the standards established under paragraph (1), standards for collecting data from candidates who accepted conditional offers of employment but chose to withdraw from the hiring
process before entering into service, including data
with respect to the reasons such candidates chose to
withdraw.

(b) COLLECTION OF DATA.—Not later than 120 days
after the date of the enactment of this Act, each element
of the intelligence community shall begin collecting data
on workforce and candidate attrition in accordance with
the standards established under subsection (a).

(c) ANNUAL REPORT.—Not later than 1 year after
the date of the enactment of this Act, and annually there-
after, the Director shall submit to the congressional intel-
ligence committees a report on workforce and candidate
attrition in the intelligence community that includes—

(1) the findings of the Director based on the
data collected under subsection (b);

(2) recommendations for addressing any issues
identified in those findings; and

(3) an assessment of timeliness in processing
hiring applications of individuals previously em-
ployed by an element of the intelligence community,
consistent with the Trusted Workforce 2.0 initiative
sponsored by the Security Clearance, Suitability, and
Credentialing Performance Accountability Council.
SEC. 309. LIMITATION ON DELEGATION OF RESPONSIBILITY FOR PROGRAM MANAGEMENT OF INFORMATION-SHARING ENVIRONMENT.

(a) In General.—Section 1016(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485(b)), as amended by section 6402(a) of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92), is further amended—

(1) in paragraph (1), in the matter before subparagraph (A), by striking “Director of National Intelligence” and inserting “President”;

(2) in paragraph (2), by striking “Director of National Intelligence” both places it appears and inserting “President”; and

(3) by adding at the end the following:

“(3) Delegation.—

“(A) In General.—Subject to subparagraph (B), the President may delegate responsibility for carrying out this subsection.

“(B) Limitation.—The President may not delegate responsibility for carrying out this subsection to the Director of National Intelligence.”.

(b) Effective Date.—The amendments made by subsection (a) shall take effect on October 1, 2020.
SEC. 310. IMPROVEMENTS TO PROVISIONS RELATING TO

INTELLIGENCE COMMUNITY INFORMATION

TECHNOLOGY ENVIRONMENT.

Section 6312 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92) is amended by striking subsections (e) through (i) and inserting the following:

“(e) LONG-TERM ROADMAP.—Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2021, the Director of National Intelligence shall develop and maintain a long-term roadmap for the intelligence community information technology environment.

“(f) BUSINESS PLAN.—Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2021, the Director of National Intelligence shall develop and maintain a business plan to implement the long-term roadmap required by subsection (e).”.

SEC. 311. REQUIREMENTS AND AUTHORITIES FOR DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY TO IMPROVE EDUCATION IN SCIENCE, TECHNOLOGY, ENGINEERING, ARTS, AND MATHEMATICS.

The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.) is amended by adding the following:
"SEC. 24. IMPROVEMENT OF EDUCATION IN SCIENCE, TECHNOLOGY, ENGINEERING, ARTS, AND MATHEMATICS.

“(a) DEFINITIONS.—In this section:

“(1) ELIGIBLE ENTITY.—The term ‘eligible entity’ includes a department or agency of the Federal Government, a State, a political subdivision of a State, an individual, and a not-for-profit or other organization in the private sector.

“(2) EDUCATIONAL INSTITUTION.—The term ‘educational institution’ includes any public or private elementary school or secondary school, institution of higher education, college, university, or any other profit or nonprofit institution that is dedicated to improving science, technology, engineering, the arts, mathematics, business, law, medicine, or other fields that promote development and education relating to science, technology, engineering, the arts, or mathematics.

“(3) STATE.—The term ‘State’ means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and any other territory or possession of the United States.

“(b) REQUIREMENTS.—The Director shall, on a continuing basis—
“(1) identify actions that the Director may take to improve education in the scientific, technology, engineering, arts, and mathematics (known as ‘STEAM’) skills necessary to meet the long-term national security needs of the United States for personnel proficient in such skills; and

“(2) establish and conduct programs to carry out such actions.

“(e) Authori ties.—

“(1) In general.—The Director, in support of educational programs in science, technology, engineering, the arts, and mathematics, may—

“(A) award grants to eligible entities;

“(B) provide cash awards and other items to eligible entities;

“(C) accept voluntary services from eligible entities;

“(D) support national competition judging, other educational event activities, and associated award ceremonies in connection with such educational programs; and

“(E) enter into one or more education partnership agreements with educational institutions in the United States for the purpose of encouraging and enhancing study in science,
technology, engineering, the arts, and mathematics disciplines at all levels of education.

“(2) Education partnership agreements.—

“(A) Nature of assistance provided.—Under an education partnership agreement entered into with an educational institution under paragraph (1)(E), the Director may provide assistance to the educational institution by—

“(i) loaning equipment to the educational institution for any purpose and duration in support of such agreement that the Director considers appropriate;

“(ii) making personnel available to teach science courses or to assist in the development of science courses and materials for the educational institution;

“(iii) providing sabbatical opportunities for faculty and internship opportunities for students;

“(iv) involving faculty and students of the educational institution in Agency projects, including research and technology transfer or transition projects;
“(v) cooperating with the educational institution in developing a program under which students may be given academic credit for work on Agency projects, including research and technology transfer for transition projects; and

“(vi) providing academic and career advice and assistance to students of the educational institution.

“(B) PRIORITIES.—In entering into education partnership agreements under paragraph (1)(E), the Director shall prioritize entering into education partnership agreements with the following:

“(i) Historically Black colleges and universities and other minority-serving institutions, as described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

“(ii) Educational institutions serving women, members of minority groups, and other groups of individuals who traditionally are involved in the science, technology, engineering, arts, and mathematics professions in disproportionately low numbers.
“(d) DESIGNATION OF ADVISOR.—The Director shall designate one or more individuals within the Agency to advise and assist the Director regarding matters relating to science, technology, engineering, the arts, and mathematics education and training.”.

Subtitle B—Inspector General of the Intelligence Community

SEC. 321. PROHIBITION AGAINST DISCLOSURE OF WHISTLEBLOWER IDENTITY AS REPRISAL AGAINST WHISTLEBLOWER DISCLOSURE BY EMPLOYEES AND CONTRACTORS IN INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—Paragraph (3) of subsection (a) of section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subparagraph (I), by striking “; or” and inserting a semicolon;

(2) by redesignating subparagraph (J) as subparagraph (K); and

(3) by inserting after subparagraph (I) the following:

“(J) a knowing and willful or negligent disclosure revealing the identity or other personally identifiable information of an employee or contractor employee without the express
written consent of the employee or contractor
employee or if the Inspector General determines
it is necessary for the exclusive purpose of in-
vestigating a complaint or information received
under section 8H of the Inspector General Act
of 1978 (5 U.S.C. App. 8H); or”.

(b) Applicability to Detailees.—Such subsection
is amended by adding at the end the following:

“(5) EMPLOYEE.—The term ‘employee’, with
respect to an agency or a covered intelligence com-
pany element, includes an individual who has been
detailed to such agency or covered intelligence com-
pany element.”.

(e) Private Right of Action for Unlawful Disclo-
sure of Whistleblower Identity.—Subsection
(d) of such section is amended to read as follows:

“(d) Enforcement.—

“(1) In General.—Except as otherwise pro-
vided in this subsection, the President shall provide
for the enforcement of this section.

“(2) Private Right of Action for Unlaw-
ful, Willful Disclosure of Whistleblower
Identity.—In a case in which an employee of an
agency takes a personnel action described in sub-
section (a)(3)(J) against an employee of a covered
intelligence community element as a reprisal in violation of subsection (b) or in a case in which a contractor employee takes a personnel action described in such subsection against another contractor employee as a reprisal in violation of subsection (c), the employee or contractor employee against whom the personnel action was taken may bring a private action for all appropriate remedies, including injunctive relief and compensatory and punitive damages, against the employee or contractor employee who took the personnel action, in a Federal district court of competent jurisdiction within 180 days of when the employee or contractor employee first learned of or should have learned of the violation.’’.

SEC. 322. CLARIFICATION OF STANDARDS REGARDING WHISTLEBLOWER COMPLAINTS AND INFORMATION OF URGENT CONCERN RECEIVED BY INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.

(a) Clarification Regarding Definitions of URGENT CONCERN.—Clause (i) of section 103H(k)(5)(G) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)(G)) is amended to read as follows:

“(i) A serious or flagrant—

“(I) problem;
“(II) abuse;
“(III) violation of law;
“(IV) violation of an Executive order; or
“(V) deficiency—
“(aa) relating to the funding, administration, or operation of the Federal Government; and
“(bb) that is a matter of national security and not a difference of opinion concerning public policy matters.”.

(b) Authority to Determine Matters of Urgent Concern.—Section 103H(k)(5)(G) of such Act (50 U.S.C. 3033(k)(5)(G)) is amended—

(1) in clause (i), as amended by subsection (a)—

(A) in subclause (V), by redesignating items (aa) and (bb) as subitems (AA) and (BB), respectively; and

(B) by redesignating subclauses (I) through (V) as items (aa) through (ee), respectively;

(2) by redesignating clauses (i) through (iii) as subclauses (I) through (III), respectively;
(3) in the matter before subclause (I), as redesignated by paragraph (2), by inserting “(i)” before “In this”; and

(4) by adding at the end the following:

“(ii) The Inspector General shall have sole authority to determine whether any complaint or information reported to the Inspector General is a matter of urgent concern under this paragraph.”.

(e) SCOPE OF AUTHORITY OF INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—Section 103H(k)(5) of such Act (50 U.S.C. 3033(k)(5)) is amended by adding at the end the following:

“(J) The Inspector General shall have authority over any complaint or information submitted to the Inspector General from an employee, detailee, or contractor of the intelligence community.”.

(d) REQUIREMENTS RELATING TO BASIS AND DERIVATION OF COMPLAINTS AND INFORMATION REPORTED.—

(1) IN REPORT TO INSPECTOR GENERAL.—Subparagraph (A) of section 103H(k)(5) of such Act (50 U.S.C. 3033(k)(5)) is amended—

(A) by inserting “(i)” before “An employee”; and

(B) by adding at the end the following:
“(ii) An employee who reports a complaint or information under clause (i) shall include in such report a statement of the following:

“(I) The basis upon which such complaint or information is derived.

“(II) How such complaint or information was discovered.”.

(2) TRANSMITTAL TO DIRECTOR.—Subparagraph (B) of such section is amended by inserting before the period the following: “and the statement included under subparagraph (A)(ii), except that the Inspector General shall modify such statement as the Inspector General considers appropriate and in accordance with applicable provisions of law to protect the anonymity of the employee if the employee chooses to maintain the employee’s anonymity”.

SEC. 323. CLARIFICATION REGARDING SUBMITTAL OF COMPLAINTS AND INFORMATION BY WHISTLEBLOWERS IN THE INTELLIGENCE COMMUNITY TO CONGRESS.

(a) Clarification of Right to Report Directly to Congress.—Subsection (a) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App. 8H) is amended by adding at the end the following:
“(4)(A) Subject to subparagraph (C), an employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community who intends to report to Congress a complaint or information may report such complaint or information directly to Congress, regardless of whether the complaint or information is with respect to an urgent concern, by contacting directly—

“(i) the Chairman and Vice Chairman of the Select Committee on Intelligence of the Senate, or a nonpartisan member of the staff of such Committee who has been designated by the Committee for purposes of receiving complaints or information under this paragraph; or

“(ii) the Chairman and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives, or a nonpartisan member of the staff of such Committee who has been designated by the Committee for purposes of receiving complaints or information under this paragraph; and

“(B) In the case of a complaint or information that is with respect to an urgent concern, the employee may report such complaint or information directly to Congress as described in subparagraph (A)—
“(i) in lieu of reporting such complaint or information under paragraph (1); or

“(ii) in addition to reporting such complaint or information under paragraph (1).

“(C)(i) In the case of a complaint or information containing classified information, an employee may contact Congress directly as described in subparagraph (A) of this paragraph only if the employee contacts designated nonpartisan staff of an intelligence committee and obtains and follows from the Director of National Intelligence, through the Inspector General, or from a security officer appointed under section 103H(j)(5) of the National Security Act of 1947 (50 U.S.C. 3033(j)(5)) guidance and direction on how to report to Congress under subparagraph (A) of this paragraph in accordance with appropriate security practices.

“(ii) If an employee contacts designated nonpartisan staff and seeks guidance and direction under clause (i) and does not receive the guidance and direction sought within 30 calendar days or fewer, the employee may contact Congress directly as described in subparagraph (A) without obtaining and following guidance and direction under clause (i) of this subparagraph.

“(D) If an employee described in subparagraph (A) reports a complaint or information to Congress as de-
scribed in such subparagraph, such employee shall provide testimony or an interview to an intelligence committee if—

“(i) such testimony or interview is requested by the Chairman, Vice Chairman, or Ranking Member of such intelligence committee;

“(ii) not later than 48 hours after making the request described in clause (i) and not fewer than 7 days before the testimony or interview is provided, the Chairman, Vice Chairman, or Ranking Member who made the request notifies the Chairman, Vice Chairman, or Ranking Member of such committee who did not make the request; and

“(iii) such testimony or interview is held in a closed session in accordance with appropriate classification guidelines and requisite protections for individual safety.”.

(b) APPOINTMENT OF PERMANENT SECURITY OFFICERS.—Section 103H(j) of the National Security Act of 1947 (50 U.S.C. 3033(j)) is amended by adding at the end the following:

“(5) The Inspector General shall appoint within the office of the Inspector General security officers to provide, on a permanent basis, confidential, security-related guidance and direction to an employee of an element of the intelligence community, an employee assigned or detailed
to an element of the intelligence community, or an em-
ployee of a contractor of an element of the intelligence community who intends to report to Congress a complaint or information so that such employee can obtain direction on how to report to Congress in accordance with appro-
priate security practices.”.

(c) CONFORMING AMENDMENTS.—

(1) NATIONAL SECURITY ACT OF 1947.—Section 103H(k)(5)(D) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)(D)) is amended—

(A) in clause (i), by striking “by con-
tacting” and all that follows and inserting the following: “by contacting, directly—

“(I) the Chairman and Vice Chairman of the Select Committee on Intelligence of the Senate, or a nonpartisan member of the staff of such Committee who has been designated by the Committee for pur-
poses of receiving complaints or information under this subparagraph; or

“(II) the Chairman and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives, or a nonpartisan member of the staff of such Committee who has been designated by the Committee for purposes of
receiving complaints or information under this sub-
paragraph.”;
(B) by amending clause (ii) to read as fol-
 lows:
“(ii)(I) In the case of a complaint or information con-
taining classified information, an employee may contact
Congress as described in clause (i) of this paragraph only
if the employee contacts designated nonpartisan staff of
a congressional intelligence committee and obtains and fol-
lows from the Director of National Intelligence, through
the Inspector General, or from a security officer appointed
under subsection (j)(5) guidance and direction on how to
report to Congress under clause (i) of this subparagraph
in accordance with appropriate security practices.
“(II) If an employee contacts designated nonpartisan
staff and seeks guidance and direction under subclause (I)
and does not receive the guidance and direction sought
within 30 calendar days or fewer, the employee may con-
tact Congress directly as described in clause (i) without
obtaining and following guidance and direction under sub-
clause (I) of this clause.”; and
(C) by adding at the end the following:
“(iv) If an employee described in clause (i) reports
a complaint or information to Congress as described in
such clause, such employee shall provide testimony or an
interview to a congressional intelligence committee if—

“(I) such testimony or interview is requested by
the Chairman, Vice Chairman, or Ranking Member
of such congressional intelligence committee;

“(II) not later than 48 hours after making the
request described in subclause (I) and not fewer
than 7 days before the testimony or interview is pro-
vided, the Chairman, Vice Chairman, or Ranking
Member who made the request notifies the Chair-
man, Vice Chairman, or Ranking Member of such
committee who did not make the request; and

“(III) such testimony or interview is held in a
closed session in accordance with appropriate classi-
fication guidelines and requisite protections for indi-
vidual safety.”.

(2) Central Intelligence Agency Act of
1949.—Section 17(d)(5)(D) of the Central Intel-
ligence Agency Act of 1949 (50 U.S.C.
3517(d)(5)(D)) is amended—

(A) in clause (i), by striking “by con-
tacting” and all that follows and inserting the
following: “by contacting, directly—

“(I) the Chairman and Vice Chairman of the
Select Committee on Intelligence of the Senate, or a
nonpartisan member of the staff of such Committee who has been designated by the Committee for purposes of receiving complaints or information under this subparagraph; or

“(II) the Chairman and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives, or a nonpartisan member of the staff of such Committee who has been designated by the Committee for purposes of receiving complaints or information under this subparagraph.”;

(B) by amending clause (ii) to read as follows:

“(ii)(I) In the case of a complaint or information containing classified information, the employee may contact Congress as described in clause (i) of this paragraph only if the employee contacts designated nonpartisan staff of an intelligence committee and obtains and follows from the Director, through the Inspector General, or from a security officer appointed under section 103H(j)(5) of the National Security Act of 1947 (50 U.S.C. 3033(j)(5)) guidance and direction on how to report to Congress under clause (i) of this subparagraph in accordance with appropriate security practices.
“(II) If an employee contacts designated nonpartisan staff and seeks guidance and direction under subclause (I) and does not receive the guidance and direction sought within 30 calendar days or fewer, the employee may contact Congress directly as described in clause (i) without obtaining and following guidance and direction under subclause (I) of this clause.”; and

(C) by adding at the end the following:

“(iv) If an employee described in clause (i) reports a complaint or information to Congress as described in such clause, such employee shall provide testimony or an interview to an intelligence committee if—

“(I) such testimony or interview is requested by the Chairman, Vice Chairman, or Ranking Member of such intelligence committee;

“(II) not later than 48 hours after making the request described in subclause (I) and not fewer than 7 days before the testimony or interview is provided, the Chairman, Vice Chairman, or Ranking Member who made the request notifies the Chairman, Vice Chairman, or Ranking Member of such committee who did not make the request; and

“(III) such testimony or interview is held in a closed session in accordance with appropriate classi-

(A) in paragraph (1), by striking “by contacting” and all that follows and inserting the following: “by contacting, directly—

“(A) the Chairman and Vice Chairman of the Select Committee on Intelligence of the Senate, or a nonpartisan member of the staff of such Committee who has been designated by the Committee for purposes of receiving complaints or information under this paragraph; or

“(B) the Chairman and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives, or a nonpartisan member of the staff of such Committee who has been designated by the Committee for purposes of receiving complaints or information under this paragraph.”;

(B) by amending paragraph (2) to read as follows:

“(2)(A) Subject to subparagraph (B), the employee may contact Congress directly as described in paragraph (1) of this subsection only if the employee contacts des-
ignated nonpartisan staff of an intelligence committee and obtains and follows from the head of the establishment, through the Inspector General, or from a security officer appointed under section 103H(j)(5) of the National Security Act of 1947 (50 U.S.C. 3033(j)(5)) guidance and direction on how to report to Congress in accordance with appropriate security practices.

“(B) If an employee contacts designated nonpartisan staff and seeks guidance and direction under subgraph (A) and does not receive the guidance and direction sought within 30 days or fewer, the employee may contact Congress directly as described in paragraph (1) without obtaining and following guidance and direction under subparagraph (A) of this paragraph.”; and

(C) by adding at the end the following:

“(4) If an employee described in paragraph (1) reports a complaint or information to Congress as described in such paragraph, such employee shall provide testimony or an interview to an intelligence committee if—

“(A) such testimony or interview is requested by the Chairman, Vice Chairman, or Ranking Member of such intelligence committee;

“(B) not later than 48 hours after making the request described in subparagraph (A) and not fewer than 7 days before the testimony or interview is pro-
vided, the Chairman, Vice Chairman, or Ranking
Member who made the request notifies the Chair-
man, Vice Chairman, or Ranking Member of such
committee who did not make the request; and

“(C) such testimony or interview is held in a
closed session in accordance with appropriate classi-
fication guidelines and requisite protections for indi-
vidual safety.”.

SEC. 324. LIMITATION ON SHARING OF INTELLIGENCE
COMMUNITY WHISTLEBLOWER COMPLAINTS
WITH PERSONS NAMED IN SUCH COM-
PLAINTS.

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

(1) by redesignating subsection (h) as sub-
section (i); and

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

“(h)(1) It shall be unlawful for an employee or agent
of the Federal Government to share any complaint or in-
formation submitted to an Inspector General under this
section with any person named as a subject of the com-
plaint or information, unless—
“(A) the person who submitted the complaint or
information consents, in writing, to such sharing;
and

“(B) such sharing is part of an investigation of
an alleged violation of section 1104 of the National
Security Act of 1947 (50 U.S.C. 3234) that involves
a personnel action described in subsection (a)(3)(J)
of such section.

“(2) Any person who violates paragraph (1) shall be
fined in accordance with title 18, United States Code, im-
prisoned for not more than 2 years, or both.

“(3) In any case in which an Inspector General under
this section learns of a violation of paragraph (1), such
Inspector General shall notify the congressional intel-
ligence committees of such violation.”.
Subtitle C—Reports and Assessments Pertaining to Intelligence Community


(a) Assessment Required.—The Comptroller General of the United States shall assess the efforts of the intelligence community and the Department of Defense to identify and mitigate the risks posed to the intelligence community and the Department by the use of direct-to-consumer genetic testing by the Government of the People’s Republic of China.

(b) Report Required.—

(1) Definition of United States Direct-to-Consumer Genetic Testing Company.—In this subsection, the term “United States direct-to-consumer genetic testing company” means a private entity that—
(A) carries out direct-to-consumer genetic testing; and

(B) is organized under the laws of the United States or any jurisdiction within the United States.

(2) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General shall submit to Congress a report on the assessment required by subsection (a).

(3) ELEMENTS.—The report required by paragraph (2) shall include the following:

(A) A description of key national security risks and vulnerabilities associated with direct-to-consumer genetic testing, including—

(i) how the Government of the People’s Republic of China may be using data provided by personnel of the intelligence community and the Department through direct-to-consumer genetic tests; and

(ii) how ubiquitous technical surveillance may amplify those risks.

(B) An assessment of the extent to which the intelligence community and the Department have identified risks and vulnerabilities posed by direct-to-consumer genetic testing and have
sought to mitigate such risks and vulnerabilities, or have plans for such mitigation, including the extent to which the intelligence community has determined—

(i) in which United States direct-to-consumer genetic testing companies the Government of the People’s Republic of China or entities owned or controlled by the Government of the People’s Republic of China have an ownership interest; and

(ii) which United States direct-to-consumer genetic testing companies may have sold data to the Government of the People’s Republic of China or entities owned or controlled by the Government of the People’s Republic of China.

(C) Such recommendations as the Comptroller General may have for action by the intelligence community and the Department to improve the identification and mitigation of risks and vulnerabilities posed by the use of direct-to-consumer genetic testing by the Government of the People’s Republic of China.
(4) Form.—The report required by paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

(c) Cooperation.—The heads of relevant elements of the intelligence community and components of the Department shall—

(1) fully cooperate with the Comptroller General in conducting the assessment required by subsection (a); and

(2) provide any information and data required by the Comptroller General to conduct the assessment.

SEC. 332. REPORT ON USE BY INTELLIGENCE COMMUNITY OF HIRING FLEXIBILITIES AND EXPEDITED HUMAN RESOURCES PRACTICES TO ASSURE QUALITY AND DIVERSITY IN THE WORKFORCE OF THE INTELLIGENCE COMMUNITY.

(a) In General.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on how elements of the intelligence community are exercising hiring flexibilities and expedited human resources practices afforded under section 3326 of title 5, United States Code, and subpart D of part 315 of title 5, Code of Federal Regulations, or successor regu-
lation, to assure quality and diversity in the workforce of the intelligence community.

(b) OBSTACLES.—The report submitted under subsection (a) shall include identification of any obstacles encountered by the intelligence community in exercising the authorities described in such subsection.

SEC. 333. REPORT ON SIGNALS INTELLIGENCE PRIORITIES AND REQUIREMENTS.

(a) REPORT REQUIRED.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on signals intelligence priorities and requirements subject to Presidential Policy Directive 28.

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

(1) The implementation of the annual process for advising the Director on signals intelligence priorities and requirements described in section 3 of Presidential Policy Directive 28.

(2) The signals intelligence priorities and requirements as of the most recent annual process.

(3) The application of such priorities and requirements to the signals intelligence collection efforts of the intelligence community.

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

SEC. 334. ASSESSMENT OF DEMAND FOR STUDENT LOAN REPAYMENT PROGRAM BENEFIT.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the head of each element of the intelligence community shall—

   (1) calculate the number of personnel of that element who qualify for a student loan repayment program benefit;

   (2) compare the number calculated under paragraph (1) to the number of personnel who apply for such a benefit;

   (3) provide recommendations for how to structure such a program to optimize participation and enhance the effectiveness of the benefit as a retention tool, including with respect to the amount of the benefit offered and the length of time an employee receiving a benefit is required to serve under a continuing service agreement; and
(4) identify any shortfall in funds or authorities needed to provide such a benefit.

(b) INCLUSION IN FISCAL YEAR 2022 BUDGET SUBMISSION.—The Director of National Intelligence shall include in the budget justification materials submitted to Congress in support of the budget for the intelligence community for fiscal year 2022 (as submitted with the budget of the President under section 1105(a) of title 31, United States Code) a report on the findings of the elements of the intelligence community under subsection (a).

SEC. 335. ASSESSMENT OF INTELLIGENCE COMMUNITY DEMAND FOR CHILD CARE.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the heads of the elements of the intelligence community specified in subsection (b), shall submit to the congressional intelligence committees a report that includes—

1. a calculation of the total annual demand for child care by employees of such elements, at or near the workplaces of such employees, including a calculation of the demand for early morning and evening child care;

2. an identification of any shortfall between the demand calculated under paragraph (1) and the
child care supported by such elements as of the date of the report;

(3) an assessment of options for addressing any such shortfall, including options for providing child care at or near the workplaces of employees of such elements;

(4) an identification of the advantages, disadvantages, security requirements, and costs associated with each such option;

(5) a plan to meet, by the date that is 5 years after the date of the report—

(A) the demand calculated under paragraph (1); or

(B) an alternative standard established by the Director for child care available to employees of such elements; and

(6) an assessment of needs of specific elements of the intelligence community, including any Government-provided child care that could be collocated with a workplace of employees of such an element and any available child care providers in the proximity of such a workplace.

(b) ELEMENTS SPECIFIED.—The elements of the intelligence community specified in this subsection are the following:
SEC. 336. OPEN SOURCE INTELLIGENCE STRATEGIES AND PLANS FOR THE INTELLIGENCE COMMUNITY.

(a) Requirement for Survey and Evaluation of Customer Feedback.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the head of each element of the intelligence community, shall—

(1) conduct a survey of the open source intelligence requirements, goals, monetary and property investments, and capabilities for each element of the intelligence community; and

(2) evaluate the usability and utility of the Open Source Enterprise by soliciting customer feedback and evaluating such feedback.

(b) Requirement for Overall Strategy and Plan for Improving Usability of Open Source Enterprise, and Risk
ANALYSIS OF CREATING OPEN SOURCE CENTER.—Not later than 180 days after the date of the enactment of this Act, the Director, in coordination with the head of each element of the intelligence community and using the findings of the Director with respect to the survey conducted under subsection (a), shall—

(1) develop a strategy for open source intelligence collection, analysis, and production that defines the overarching goals, roles, responsibilities, and processes for such collection, analysis, and production for the intelligence community;

(2) develop a plan for improving usability and utility of the Open Source Enterprise based on the customer feedback solicited under subsection (a)(2); and

(3) conduct a risk and benefit analysis of creating an open source center independent of any current intelligence community element.

(c) REQUIREMENT FOR PLAN FOR CENTRALIZED DATA REPOSITORY.—Not later than 270 days after the date of the enactment of this Act and using the findings of the Director with respect to the survey and evaluation conducted under subsection (a), the strategy and plan developed under subsection (b), and the risk and benefit analysis conducted under such subsection, the Director
shall develop a plan for a centralized data repository of open source intelligence that enables all elements of the intelligence community—

(1) to use such repository for their specific requirements; and

(2) to derive open source intelligence advantages.

(d) REQUIREMENT FOR COST-SHARING MODEL.—Not later than 1 year after the date of the enactment of this Act and using the findings of the Director with respect to the survey and evaluation conducted under subsection (a), the strategy and plan developed under subsection (b), the risk and benefit analysis conducted under such subsection, and the plan developed under subsection (c), the Director shall develop a cost-sharing model that leverages the open source intelligence investments of each element of the intelligence community for the beneficial use of the entire intelligence community.

(e) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date of the enactment of this Act, the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the Defense Intelligence Agency, the Director of the National Geospatial-Intelligence Agency, and the Director of the National Se-
security Agency shall jointly brief the congressional intelligence committees on—

(1) the strategy developed under paragraph (1) of subsection (b);

(2) the plan developed under paragraph (2) of such subsection;

(3) the plan developed under subsection (c); and

(4) the cost-sharing model developed under subsection (d).

SEC. 337. PLAN FOR ESTABLISHING AN ELEMENT OF THE INTELLIGENCE COMMUNITY WITHIN THE UNITED STATES SPACE FORCE.

Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence and the Under Secretary of Defense for Intelligence and Security, in coordination with the Secretary of the Air Force and the Chief of Space Operations, shall submit to the congressional intelligence committees, the Committee on Armed Services of the Senate, and the Committee on Armed Services of the House of Representatives a plan for establishing an element of the intelligence community within the United States Space Force.
TITLE IV—SECURITY CLEARANCES AND TRUSTED WORKFORCE

SEC. 401. EXCLUSIVITY, CONSISTENCY, AND TRANSPARENCY IN SECURITY CLEARANCE PROCEDURES, AND RIGHT TO APPEAL.

(a) Exclusivity of Procedures.—Section 801 of the National Security Act of 1947 (50 U.S.C. 3161) is amended by adding at the end the following:

“(c) Exclusivity.—Except as provided in subsection (b) and subject to sections 801A and 801B, the procedures established pursuant to subsection (a) and promulgated and set forth under subpart A of title 32, Code of Federal Regulations, or successor regulations, shall be the exclusive procedures by which decisions about eligibility for access to classified information are governed.”.

(b) Transparency.—Such section is further amended by adding at the end the following:

“(d) Publication.—

“(1) In general.—Not later than 180 days after the date of the enactment of this subsection, the President shall—

“(A) publish in the Federal Register the procedures established pursuant to subsection (a); or
“(B) submit to Congress a certification that the procedures currently in effect that govern access to classified information as described in subsection (a)—

“(i) are published in the Federal Register; and

“(ii) comply with the requirements of subsection (a).

“(2) UPDATES.—Whenever the President makes a revision to a procedure established pursuant to subsection (a), the President shall publish such revision in the Federal Register not later than 30 days before the date on which the revision becomes effective.”.

(c) CONSISTENCY.—

(1) IN GENERAL.—Title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.) is amended by inserting after section 801 the following:

“SEC. 801A. DECISIONS RELATING TO ACCESS TO CLASSIFIED INFORMATION.

“(a) DEFINITIONS.—In this section:

“(1) AGENCY.—The term ‘agency’ has the meaning given the term ‘Executive agency’ in section 105 of title 5, United States Code.
“(2) Classified information.—The term ‘classified information’ includes sensitive compartmented information, restricted data, restricted handling information, and other compartmented information.

“(3) Eligibility for access to classified information.—The term ‘eligibility for access to classified information’ has the meaning given such term in the procedures established pursuant to section 801(a).

“(b) In general.—Each head of an agency that makes a determination regarding eligibility for access to classified information shall ensure that in making the determination, the head of the agency or any person acting on behalf of the head of the agency—

“(1) does not violate any right or protection enshrined in the Constitution of the United States, including rights articulated in the First, Fifth, and Fourteenth Amendments;

“(2) does not discriminate for or against an individual on the basis of race, ethnicity, color, religion, sex, national origin, age, or handicap;

“(3) is not carrying out—

“(A) retaliation for political activities or beliefs; or
“(B) a coercion or reprisal described in section 2302(b)(3) of title 5, United States Code; and

“(4) does not violate section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)).”.

(2) CLERICAL AMENDMENT.—The table of contents in the matter preceding section 2 of the National Security Act of 1947 (50 U.S.C. 3002) is amended by inserting after the item relating to section 801 the following:

“Sec. 801A. Decisions relating to access to classified information.”.

(d) RIGHT TO APPEAL.—

(1) IN GENERAL.—Such title, as amended by subsection (c), is further amended by inserting after section 801A the following:

“SEC. 801B. RIGHT TO APPEAL.

“(a) DEFINITIONS.—In this section:

“(1) AGENCY.—The term ‘agency’ has the meaning given the term ‘Executive agency’ in section 105 of title 5, United States Code.

“(2) COVERED PERSON.—The term ‘covered person’ means a person, other than the President and Vice President, currently or formerly employed in, detailed to, assigned to, or issued an authorized conditional offer of employment for a position that
requires access to classified information by an agency, including the following:

“(A) A member of the Armed Forces.

“(B) A civilian.

“(C) An expert or consultant with a contractual or personnel obligation to an agency.

“(D) Any other category of person who acts for or on behalf of an agency as determined by the head of the agency.

“(3) Eligibility for access to classified information.—The term ‘eligibility for access to classified information’ has the meaning given such term in the procedures established pursuant to section 801(a).

“(4) Need for access.—The term ‘need for access’ has such meaning as the President may define in the procedures established pursuant to section 801(a).

“(5) Reciprocity of clearance.—The term ‘reciprocity of clearance’, with respect to a denial by an agency, means that the agency, with respect to a covered person—

“(A) failed to accept a security clearance background investigation as required by paragraph (1) of section 3001(d) of the Intelligence...
Reform and Terrorism Prevention Act of 2004
(50 U.S.C. 3341(d));

“(B) failed to accept a transferred security
clearance background investigation required by
paragraph (2) of such section;

“(C) subjected the covered person to an
additional investigative or adjudicative require-
ment in violation of paragraph (3) of such sec-
tion; or

“(D) conducted an investigation in viola-
tion of paragraph (4) of such section.

“(6) SECURITY EXECUTIVE AGENT.—The term
‘Security Executive Agent’ means the officer serving
as the Security Executive Agent pursuant to section
803.

“(b) AGENCY REVIEW.—

“(1) IN GENERAL.—Not later than 180 days
after the date of the enactment of the Intelligence
Authorization Act for Fiscal Year 2021, each head
of an agency shall, consistent with the interest of
national security, establish and publish in the Fed-
eral Register a process by which a covered person to
whom eligibility for access to classified information
was denied or revoked by the agency or for whom
reciprocity of clearance was denied by the agency
can appeal that denial or revocation within the agency.

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

“(A) In the case of a covered person to whom eligibility for access to classified information or reciprocity of clearance is denied or revoked by an agency, the following:

“(i) The head of the agency shall provide the covered person with a written—

“(I) detailed explanation of the basis for the denial or revocation as the head of the agency determines is consistent with the interests of national security and as permitted by other applicable provisions of law; and

“(II) notice of the right of the covered person to a hearing and appeal under this subsection.

“(ii) Not later than 30 days after receiving a request from the covered person for copies of the documents that formed the basis of the agency’s decision to revoke or deny, including the investigative file, the
head of the agency shall provide to the covered person copies of such documents as—

“(I) the head of the agency determines is consistent with the interests of national security; and

“(II) permitted by other applicable provisions of law, including—

“(aa) section 552 of title 5, United States Code (commonly known as the ‘Freedom of Information Act’);

“(bb) section 552a of such title (commonly known as the ‘Privacy Act of 1974’); and

“(cc) such other provisions of law relating to the protection of confidential sources and privacy of individuals.

“(iii)(I) The covered person shall have the opportunity to retain counsel or other representation at the covered person’s expense.

“(II) Upon the request of the covered person, and a showing that the ability to review classified information is essential to
the resolution of an appeal under this subsection, counsel or other representation retained under this clause shall be considered for access to classified information for the limited purposes of such appeal.

“(iv)(I) The head of the agency shall provide the covered person an opportunity, at a point in the process determined by the agency head—

“(aa) to appear personally before an adjudicative or other authority, other than the investigating entity, and to present to such authority relevant documents, materials, and information, including evidence that past problems relating to the denial or revocation have been overcome or sufficiently mitigated; and

“(bb) to call and cross-examine witnesses before such authority, unless the head of the agency determines that calling and cross-examining witnesses is not consistent with the interests of national security.
“(II) The head of the agency shall make, as part of the security record of the covered person, a written summary, transcript, or recording of any appearance under item (aa) of subclause (I) or of any calling or cross-examining of witnesses under item (bb) of such subclause.

“(v) On or before the date that is 30 days after the date on which the covered person receives copies of documents under clause (ii), the covered person may request a hearing of the decision to deny or revoke by filing a written appeal with the head of the agency.

“(B) A requirement that each review of a decision under this subsection is completed on average not later than 180 days after the date on which a hearing is requested under subparagraph (A)(v).

“(3) AGENCY REVIEW PANELS.—

“(A) IN GENERAL.—Each head of an agency shall establish a panel to hear and review appeals under this subsection.

“(B) MEMBERSHIP.—
“(i) COMPOSITION.—Each panel established by the head of an agency under subparagraph (A) shall be composed of at least three employees of the agency selected by the agency head, two of whom shall not be members of the security field.

“(ii) TERMS.—A term of service on a panel established by the head of an agency under subparagraph (A) shall not exceed 2 years.

“(C) DECISIONS.—

“(i) WRITTEN.—Each decision of a panel established under subparagraph (A) shall be in writing and contain a justification of the decision.

“(ii) CONSISTENCY.—Each head of an agency that establishes a panel under subparagraph (A) shall ensure that each decision of the panel is consistent with the interests of national security and applicable provisions of law.

“(iii) OVERTURN.—The head of an agency may overturn a decision of the panel if, not later than 30 days after the date on which the panel issues the deci-
sion, the agency head personally exercises
the authority granted by this clause to
overturn such decision.

“(iv) Finality.—Each decision of a
panel established under subparagraph (A)
or overturned pursuant to clause (iii) of
this subparagraph shall be final but sub-
ject to appeal and review under subsection
(c).

“(D) ACCESS TO CLASSIFIED INFORMA-
tion.—The head of an agency that establishes
a panel under subparagraph (A) shall afford ac-
cess to classified information to the members of
the panel as the agency head determines—

“(i) necessary for the panel to hear
and review an appeal under this sub-
section; and

“(ii) consistent with the interests of
national security.

“(4) REPRESENTATION BY COUNSEL.—

“(A) IN GENERAL.—Each head of an
agency shall ensure that, under this subsection,
a covered person appealing a decision of the
head’s agency under this subsection has an op-
portunity to retain counsel or other representation at the covered person’s expense.

“(B) ACCESS TO CLASSIFIED INFORMATION.—

“(i) IN GENERAL.—Upon the request of a covered person appealing a decision of an agency under this subsection and a showing that the ability to review classified information is essential to the resolution of the appeal under this subsection, the head of the agency shall sponsor an application by the counsel or other representation retained under this paragraph for access to classified information for the limited purposes of such appeal.

“(ii) EXTENT OF ACCESS.—Counsel or another representative who is cleared for access under this subparagraph may be afforded access to relevant classified materials to the extent consistent with the interests of national security.

“(5) CORRECTIVE ACTION.—

“(A) IN GENERAL.—If, in the course of proceedings under this subsection, the head of an agency or a panel established by the agency
head under paragraph (3) decides that a covered person’s eligibility for access to classified information was improperly denied or revoked by the agency, the agency shall take corrective action to return the covered person, as nearly as practicable and reasonable, to the position such covered person would have held had the improper denial or revocation not occurred.

“(B) COMPENSATION.—Corrective action under subparagraph (A) may include compensation, in an amount not to exceed $300,000, for any loss of wages or benefits suffered, or expenses otherwise incurred, by reason of such improper denial or revocation.

“(6) PUBLICATION OF DECISIONS.—

“(A) IN GENERAL.—Each head of an agency shall publish each final decision on an appeal under this subsection.

“(B) REQUIREMENTS.—In order to ensure transparency, oversight by Congress, and meaningful information for those who need to understand how the clearance process works, each publication under subparagraph (A) shall be—

“(i) made in a manner that is consistent with section 552 of title 5, United
71 States Code, as amended by the Electronic Freedom of Information Act Amendments of 1996 (Public Law 104–231);

“(ii) published to explain the facts of the case, redacting personally identifiable information and sensitive program information; and

“(iii) made available on a website that is searchable by members of the public.

“(c) HIGHER LEVEL REVIEW.—

“(1) PANEL.—

“(A) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2021, the Security Executive Agent shall establish a panel to review decisions made on appeals pursuant to the processes established under subsection (b).

“(B) SCOPE OF REVIEW AND JURISDICTION.—After the initial review to verify grounds for appeal, the panel established under subparagraph (A) shall review such decisions only—

“(i) as they relate to violations of section 801A(b); or
“(ii) to the extent to which an agency properly conducted a review of an appeal under subsection (b).

“(C) COMPOSITION.—The panel established pursuant to subparagraph (A) shall be composed of three individuals selected by the Security Executive Agent for purposes of the panel, of whom at least one shall be an attorney.

“(2) APPEALS AND TIMELINESS.—

“(A) APPEALS.—

“(i) INITIATION.—On or before the date that is 30 days after the date on which a covered person receives a written decision on an appeal under subsection (b), the covered person may initiate oversight of that decision by filing a written appeal with the Security Executive Agent.

“(ii) FILING.—A written appeal filed under clause (i) relating to a decision of an agency shall be filed in such form, in such manner, and containing such information as the Security Executive Agent may require, including—

“(I) a description of—
“(aa) any alleged violations
of section 801A(b) relating to the
denial or revocation of the covered person’s eligibility for access
to classified information; and

“(bb) any allegations of how
the decision may have been the result of the agency failing to properly conduct a review under subsection (b); and

“(II) supporting materials and information for the allegations described under subclause (I).

“(B) Timeliness.—The Security Executive Agent shall ensure that, on average, review of each appeal filed under this subsection is completed not later than 180 days after the date on which the appeal is filed.

“(3) Decisions and Remands.—

“(A) In General.—If, in the course of reviewing under this subsection a decision of an agency under subsection (b), the panel established under paragraph (1) decides that there is sufficient evidence of a violation of section 801A(b) to merit a new hearing or decides that
the decision of the agency was the result of an improperly conducted review under subsection (b), the panel shall vacate the decision made under subsection (b) and remand to the agency by which the covered person shall be eligible for a new appeal under subsection (b).

“(B) WRITTEN DECISIONS.—Each decision of the panel established under paragraph (1) shall be in writing and contain a justification of the decision.

“(C) CONSISTENCY.—The panel under paragraph (1) shall ensure that each decision of the panel is consistent with the interests of national security and applicable provisions of law.

“(D) FINALITY.—

“(i) IN GENERAL.—Except as provided in clause (ii), each decision of the panel established under paragraph (1) shall be final.

“(ii) OVERTURN.—The Security Executive Agent may overturn a decision of the panel if, not later than 30 days after the date on which the panel issues the decision, the Security Executive Agent person-
ally exercises the authority granted by this clause to overturn such decision.

“(E) NATURE OF REMANDS.—In remanding a decision under subparagraph (A), the panel established under paragraph (1) may not direct the outcome of any further appeal under subsection (b).

“(F) NOTICE OF DECISIONS.—For each decision of the panel established under paragraph (1) regarding a covered person, the Security Executive Agent shall provide the covered person with a written notice of the decision that includes a detailed description of the reasons for the decision, consistent with the interests of national security and applicable provisions of law.

“(4) REPRESENTATION BY COUNSEL.—

“(A) IN GENERAL.—The Security Executive Agent shall ensure that, under this subsection, a covered person appealing a decision under subsection (b) has an opportunity to retain counsel or other representation at the covered person’s expense.

“(B) ACCESS TO CLASSIFIED INFORMATION.—
“(i) IN GENERAL.—Upon the request of the covered person and a showing that the ability to review classified information is essential to the resolution of an appeal under this subsection, the Security Executive Agent shall sponsor an application by the counsel or other representation retained under this paragraph for access to classified information for the limited purposes of such appeal.

“(ii) EXTENT OF ACCESS.—Counsel or another representative who is cleared for access under this subparagraph may be afforded access to relevant classified materials to the extent consistent with the interests of national security.

“(5) ACCESS TO DOCUMENTS AND EMPLOYEES.—

“(A) AFFORDING ACCESS TO MEMBERS OF PANEL.—The Security Executive Agent shall afford access to classified information to the members of the panel established under paragraph (1)(A) as the Security Executive Agent determines—
“(i) necessary for the panel to review a decision described in such paragraph; and

“(ii) consistent with the interests of national security.

“(B) AGENCY COMPLIANCE WITH REQUESTS OF PANEL.—Each head of an agency shall comply with each request by the panel for a document and each request by the panel for access to employees of the agency necessary for the review of an appeal under this subsection, to the degree that doing so is, as determined by the head of the agency and permitted by applicable provisions of law, consistent with the interests of national security.

“(6) PUBLICATION OF DECISIONS.—

“(A) IN GENERAL.—For each final decision on an appeal under this subsection, the head of the agency with respect to which the appeal pertains and the Security Executive Agent shall each publish the decision, consistent with the interests of national security.

“(B) REQUIREMENTS.—In order to ensure transparency, oversight by Congress, and meaningful information for those who need to under-
stand how the clearance process works, each publication under subparagraph (A) shall be—

“(i) made in a manner that is consistent with section 552 of title 5, United States Code, as amended by the Electronic Freedom of Information Act Amendments of 1996 (Public Law 104–231);

“(ii) published to explain the facts of the case, redacting personally identifiable information and sensitive program information; and

“(iii) made available on a website that is searchable by members of the public.

“(d) Period of Time for the Right to Appeal.—

“(1) In general.—Except as provided in paragraph (2), any covered person who has been the subject of a decision made by the head of an agency to deny or revoke eligibility for access to classified information shall retain all rights to appeal under this section until the conclusion of the appeals process under this section.

“(2) Waiver of Rights.—

“(A) Persons.—Any covered person may voluntarily waive the covered person’s right to
appeal under this section and such waiver shall be conclusive.

“(B) AGENCIES.—The head of an agency may not require a covered person to waive the covered person’s right to appeal under this section for any reason.

“(e) WAIVER OF AVAILABILITY OF PROCEDURES FOR NATIONAL SECURITY INTEREST.—

“(1) IN GENERAL.—If the head of an agency determines that a procedure established under subsection (b) cannot be made available to a covered person in an exceptional case without damaging a national security interest of the United States by revealing classified information, such procedure shall not be made available to such covered person.

“(2) FINALITY.—A determination under paragraph (1) shall be final and conclusive and may not be reviewed by any other official or by any court.

“(3) REPORTING.—

“(A) CASE-BY-CASE.—

“(i) IN GENERAL.—In each case in which the head of an agency determines under paragraph (1) that a procedure established under subsection (b) cannot be made available to a covered person, the
agency head shall, not later than 30 days after the date on which the agency head makes such determination, submit to the Security Executive Agent and to the congressional intelligence committees a report stating the reasons for the determination.

“(ii) FORM.—A report submitted under clause (i) may be submitted in classified form as necessary.

“(B) ANNUAL REPORTS.—

“(i) IN GENERAL.—Not less frequently than once each fiscal year, the Security Executive Agent shall submit to the congressional intelligence committees a report on the determinations made under paragraph (1) during the previous fiscal year.

“(ii) CONTENTS.—Each report submitted under clause (i) shall include, for the period covered by the report, the following:

“(I) The number of cases and reasons for determinations made under paragraph (1), disaggregated by agency.
“(II) Such other matters as the Security Executive Agent considers appropriate.

“(f) Denials and Revocations Under Other Provisions of Law.—

“(1) Rule of Construction.—Nothing in this section shall be construed to limit or affect the responsibility and power of the head of an agency to deny or revoke eligibility for access to classified information or to deny reciprocity of clearance in the interest of national security.

“(2) Denials and Revocation.—The power and responsibility to deny or revoke eligibility for access to classified information or to deny reciprocity of clearance pursuant to any other provision of law or Executive order may be exercised only when the head of an agency determines that an applicable process established under this section cannot be invoked in a manner that is consistent with national security.

“(3) Finality.—A determination under paragraph (2) shall be final and conclusive and may not be reviewed by any other official or by any court.

“(4) Reporting.—

“(A) Case-by-Case.—
“(i) In general.—In each case in which the head of an agency determines under paragraph (2) that a determination relating to a denial or revocation of eligibility for access to classified information or denial of reciprocity of clearance could not be made pursuant to a process established under this section, the agency head shall, not later than 30 days after the date on which the agency head makes such a determination under paragraph (2), submit to the Security Executive Agent and to the congressional intelligence committees a report stating the reasons for the determination.

“(ii) Form.—A report submitted under clause (i) may be submitted in classified form as necessary.

“(B) Annual reports.—

“(i) In general.—Not less frequently than once each fiscal year, the Security Executive Agent shall submit to the congressional intelligence committees a report on the determinations made under
paragraph (2) during the previous fiscal year.

“(ii) CONTENTS.—Each report submitted under clause (i) shall include, for the period covered by the report, the following:

“(I) The number of cases and reasons for determinations made under paragraph (2), disaggregated by agency.

“(II) Such other matters as the Security Executive Agent considers appropriate.

“(g) RELATIONSHIP TO SUITABILITY.—No person may use a determination of suitability under part 731 of title 5, Code of Federal Regulations, or successor regulation, for the purpose of denying a covered person the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information or a denial of reciprocity of clearance.

“(h) PRESERVATION OF ROLES AND RESPONSIBILITIES UNDER EXECUTIVE ORDER 10865 AND OF THE DEFENSE OFFICE OF HEARINGS AND APPEALS.—Nothing in this section shall be construed to diminish or otherwise affect the procedures in effect on the day before the date
of the enactment of this Act for denial and revocation pro-
cedures provided to individuals by Executive Order 10865
(50 U.S.C. 3161 note; relating to safeguarding classified
information within industry), or successor order, including
those administered through the Defense Office of Hear-
ings and Appeals of the Department of Defense under De-
partment of Defense Directive 5220.6, or successor direc-
tive.

"(i) Rule of Construction Relating to Cer-
tain Other Provisions of Law.—This section and the
processes and procedures established under this section
shall not be construed to apply to paragraphs (6) and (7)
of section 3001(j) of the Intelligence Reform and Ter-
rorism Prevention Act of 2004 (50 U.S.C. 3341(j)).”.

(2) Clerical Amendment.—The table of con-
tents in the matter preceding section 2 of the Na-
tional Security Act of 1947 (50 U.S.C. 3002), as
amended by subsection (c), is further amended by
inserting after the item relating to section 801A the
following:

"Sec. 801B. Right to appeal.”.

SEC. 402. ESTABLISHING PROCESS PARITY FOR SECURITY
CLEARANCE REVOCATIONS.
Subparagraph (C) of section 3001(j)(4) of the Intel-
ligence Reform and Terrorism Prevention Act of 2004 (50
U.S.C. 3341(j)(4)) is amended to read as follows:
“(C) Burdens of proof.—

“(i) In general.—Subject to clause (iii), in determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if the individual has demonstrated that a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual.

“(ii) Circumstantial evidence.—

An individual under clause (i) may demonstrate that the disclosure was a contributing factor in the adverse security clearance or access determination taken against the individual through circumstantial evidence, such as evidence that—

“(I) the official making the determination knew of the disclosure; and

“(II) the determination occurred within a period such that a reasonable person could conclude that the disclo-
sure was a contributing factor in the
determination.

“(iii) Defense.—In determining
whether the adverse security clearance or
access determination violated paragraph
(1), the agency shall not find that para-
graph (1) was violated if, after a finding
that a disclosure was a contributing factor,
the agency demonstrates by clear and con-
vincing evidence that it would have made
the same security clearance or access de-
termination in the absence of such disclo-
sure.”.

SEC. 403. FEDERAL POLICY ON SHARING OF DEROGATORY
INFORMATION PERTAINING TO CONTRACTOR
EMPLOYEES IN THE TRUSTED WORKFORCE.

(a) Policy Required.—Not later than 180 days
after the date of the enactment of this Act, the Security
Executive Agent, in coordination with the principal mem-
ers of the Performance Accountability Council and the
Attorney General, shall issue a policy for the Federal Gov-
ernment on sharing of derogatory information pertaining
to contractor employees engaged by the Federal Govern-
ment.

(b) Consent Requirement.—
(1) IN GENERAL.—The policy issued under subsection (a) shall require, as a condition of accepting a security clearance with the Federal Government, that a contractor employee provide prior written consent for the Federal Government to share covered derogatory information with the chief security officer of the contractor employer that employs the contractor employee.

(2) COVERED DEROGATORY INFORMATION.—For purposes of this section, covered derogatory information—

(A) is information that—


(ii) a Federal Government agency certifies is accurate and reliable;

(iii) is relevant to a contractor’s ability to protect against insider threats as required by section 1–202 of the National Industrial Security Program Operating Manual (NISPOM), or successor manual; and
(iv) may have a bearing on the contractor employee’s suitability for a position of public trust or to receive credentials to access certain facilities of the Federal Government; and

(B) shall include any negative information considered in the adjudicative process, including information provided by the contractor employee on forms submitted for the processing of the contractor employee’s security clearance.

(c) ELEMENTS.—The policy issued under subsection (a) shall—

(1) require Federal agencies, except under exceptional circumstances specified by the Security Executive Agent, to share with the contractor employer of a contractor employee engaged with the Federal Government the existence of potentially derogatory information and which National Security Adjudicative Guideline it falls under, with the exception that the Security Executive Agent may waive such requirement in circumstances the Security Executive Agent considers extraordinary;

(2) require that covered derogatory information shared with a contractor employer as described in subsection (b)(1) be used by the contractor employer
exclusively for risk mitigation purposes under section 1–202 of the National Industrial Security Program Operating Manual, or successor manual;

(3) require Federal agencies to share any mitigation measures in place to address the derogatory information;

(4) establish standards for timeliness for sharing the derogatory information;

(5) specify the methods by which covered derogatory information will be shared with the contractor employer of the contractor employee;

(6) allow the contractor employee, within a specified timeframe, the right—

(A) to contest the accuracy and reliability of covered derogatory information;

(B) to address or remedy any concerns raised by the covered derogatory information; and

(C) to provide documentation pertinent to subparagraph (A) or (B) for an agency to place in relevant security clearance databases;

(7) establish a procedure by which the contractor employer of the contractor employee may consult with the Federal Government prior to taking any remedial action under section 1–202 of the Na-
tional Industrial Security Program Operating Manual, or successor manual, to address the derogatory information the Federal agency has provided;

(8) stipulate that the chief security officer of the contractor employer is prohibited from sharing or discussing covered derogatory information with other parties, including nonsecurity professionals at the contractor employer; and

(9) require companies in the National Industrial Security Program to comply with the policy.

(d) CONSIDERATION OF LESSONS LEARNED FROM INFORMATION-SHARING PROGRAM FOR POSITIONS OF TRUST AND SECURITY CLEARANCES.—In developing the policy issued under subsection (a), the Director shall consider, to the extent available, lessons learned from actions taken to carry out section 6611(f) of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92).

TITLE V—REPORTS AND OTHER MATTERS

SEC. 501. SECURE AND TRUSTED TECHNOLOGY.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appropriate committees of Congress” means—
(A) the Select Committee on Intelligence of the Senate;

(B) the Committee on Foreign Relations of the Senate;

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

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

(E) the Committee on Commerce, Science, and Transportation of the Senate;

(F) the Permanent Select Committee on Intelligence of the House of Representatives;

(G) the Committee on Foreign Affairs of the House of Representatives;

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

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

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

(2) **Fifth-generation wireless network.**—The term “fifth-generation wireless network” means a radio network as described by the 3rd Generation Partnership Project (3GPP) Release 15 or higher.
(b) Supporting the Development and Adoption of Secure and Trusted Technologies Among Intelligence Allies and Partners.—

(1) Communications Technology Security and Innovation Fund.—

(A) Establishment of Fund.—

(i) In general.—There is established in the Treasury of the United States a fund to be known as the “Communications Technology Security and Innovation Fund” (referred to in this paragraph as the “Security Fund”).

(ii) Administration.—The Director of the Defense Advanced Research Projects Agency and the Director of the Intelligence Advanced Research Projects Activity shall jointly administer the Security Fund.

(iii) Contents of Fund.—

(I) In general.—The fund shall consist of—

(aa) amounts appropriated pursuant to the authorization of appropriations under paragraph (3)(A); and
(bb) such other amounts as
may be appropriated or otherwise
made available to the Director of
the Defense Advanced Research
Projects Agency and the Director
of the Intelligence Advanced Re-
search Projects Activity to be de-
posited in the Security Fund.

(II) AVAILABILITY.—

(aa) IN GENERAL.—

Amounts deposited in the Secu-
rity Fund shall remain available
through the end of the tenth fis-
cal year beginning after the date
of the enactment of this Act.

(bb) REMAINDER TO TREAS-
URY.—Any amounts remaining in
the Security Fund after the end
of the tenth fiscal year beginning
after the date of the enactment
of this Act shall be deposited in
the general fund of the Treasury.

(iv) USE OF AMOUNTS.—Amounts de-
posited in the Security Fund shall be avail-
able to the Director of the Defense Ad-
vanced Research Projects Agency and the
Director of the Intelligence Advanced Re-
search Projects Activity to award grants
under subparagraph (B).

(B) GRANTS.—

(i) IN GENERAL.—The Director of the
Defense Advanced Research Projects Agen-
cy and the Director of the Intelligence Ad-
vanced Research Projects Activity shall
award grants to support research and the
commercial application of such research,
including in the following areas:

(I) Promoting the development of
technology, including software, hard-
ware, and microprocessing technology,
that will enhance competitiveness in
fifth-generation (commonly known as
“5G”) and successor wireless tech-
nology supply chains.

(II) Accelerating development
and deployment of open interface,
standards-based compatible interoper-
able equipment, such as equipment
developed pursuant to the standards
set forth by organizations such as the
O–RAN Alliance, the Telecom Infra Project, 3GPP, the O–RAN Software Community, or any successor organizations.

(III) Promoting compatibility of new fifth-generation wireless network equipment with future open standards-based interoperable equipment.

(IV) Managing integration of multivendor network environments.

(V) Objective criteria to define equipment as compliant with open standards for multivendor network equipment interoperability.

(VI) Promoting development and inclusion of security features enhancing the integrity and availability of equipment in multivendor networks.

(VII) Promoting the application of network function virtualization to facilitate multivendor interoperability and a more diverse vendor market.

(ii) AMOUNT.—

(I) IN GENERAL.—Subject to subclause (II), a grant awarded under
clause (i) shall be in such amount as the Director of the Defense Advanced Research Projects Agency and the Director of the Intelligence Advanced Research Projects Activity consider appropriate.

(II) LIMITATION ON GRANT AMOUNTS.—The amount of a grant awarded under this paragraph to a recipient for a specific research focus area may not exceed $100,000,000.

(iii) CRITERIA.—The Director of the Defense Advanced Research Projects Agency and the Director of the Intelligence Advanced Research Projects Activity, in consultation with the Assistant Secretary of Commerce for Communications and Information, the Director of the National Institute of Standards and Technology, and the Secretary of Homeland Security, shall jointly establish criteria for grants awarded under clause (i).

(iv) TIMING.—Not later than 1 year after the date of the enactment of this Act, the Director of the Defense Advanced Re-
search Projects Agency and the Director of
the Intelligence Advanced Research
Projects Activity shall begin awarding
grants under clause (i).

(C) FEDERAL ADVISORY BODY.—

   (i) Establishment.—The Director

   of the Defense Advanced Research Projects

   Agency and the Director of the Intelligence

   Advanced Research Projects Activity shall

   establish a Federal advisory committee, in

   accordance with the Federal Advisory

   Committee Act (5 U.S.C. App.), composed

   of government and private sector experts,

   to advise the Director of the Defense Ad-

   vanced Research Projects Agency and the

   Director of the Intelligence Advanced Re-

   search Projects Activity on the administra-

   tion of the Security Fund.

   (ii) Composition.—The advisory

   committee established under clause (i)

   shall be composed of—

   (I) representatives from—

   (aa) the Federal Commu-

   nications Commission;
(bb) the National Institute of Standards and Technology;

(cc) the Department of State;

(dd) the National Science Foundation; and

(ee) the Department of Homeland Security; and

(II) other representatives from the private and public sectors, at the discretion of the Security Fund.

(iii) Duties.—The advisory committee established under clause (i) shall advise the Director of the Defense Advanced Research Projects Agency and the Director of the Intelligence Advanced Research Projects Activity on technology developments to help inform—

(I) the strategic direction of the Security Fund; and

(II) efforts of the Federal Government to promote a more secure, diverse, sustainable, and competitive supply chain.

(D) Reports to Congress.—
(i) Initial Report.—Not later than 180 days after the date of the enactment of this Act, the Director of the Defense Advanced Research Projects Agency and the Director of the Intelligence Advanced Research Projects Activity shall jointly submit to the appropriate committees of Congress a report with—

(I) additional recommendations on promoting the competitiveness and sustainability of trusted suppliers in the wireless supply chain; and

(II) any additional authorities needed to facilitate the timely adoption of open standards-based equipment, including authority to provide loans, loan guarantees, and other forms of credit extension that would maximize the use of designated funds.

(ii) Annual Report.—For each fiscal year for which amounts in the Security Fund are available under this paragraph, the Director of the Defense Advanced Research Projects Agency and the Director of the Intelligence Advanced Research
Projects Activity shall submit to Congress a report that—

(I) describes how, and to whom, grants have been awarded under sub-
paragraph (B);

(II) details the progress of the Director of the Defense Advanced Re-
search Projects Agency and the Director of the Intelligence Advanced Re-
search Projects Activity in meeting the objectives described in subpara-
graph (B)(i); and

(III) includes such other informa-
tion as the Director of the Defense Advanced Research Projects Agency and the Director of the Intelligence Advanced Research Projects Activity determine appropriate.

(2) MULTILATERAL TELECOMMUNICATIONS SE-
curity Fund.—

(A) Establishment of fund.—

(i) In general.—There is established in the Treasury of the United States a fund to be known as the “Multilateral Telecommunications Security Fund” (in
this section referred to as the “Multilateral Fund”).

(ii) **Administration.**—The Director of National Intelligence and the Secretary of Defense shall jointly administer the Multilateral Fund.

(iii) **Use of Amounts.**—Amounts in the Multilateral Fund shall be used to establish the common funding mechanism required by subparagraph (B).

(iv) **Contents of Fund.**—

(I) **In general.**—The Multilateral Fund shall consist of amounts appropriated pursuant to the authorization of appropriations under paragraph (3)(B) and such other amounts as may be appropriated or otherwise made available to the Director and the Secretary to be deposited in the Multilateral Fund.

(II) **Availability.**—

(aa) **In general.**—

Amounts deposited in the Multilateral Fund shall remain available through fiscal year 2031.
(bb) **Remainder to Treasury.**—Any amounts remaining in the Fund after fiscal year 2031 shall be deposited in the General Fund of the Treasury.

(B) **Multilateral Common Funding Mechanism.**—

(i) **In General.**—The Director and the Secretary shall jointly, in coordination with foreign partners, establish a common funding mechanism that uses amounts from the Multilateral Fund to support the development and adoption of secure and trusted telecommunications technologies in key markets globally.

(ii) **Consultation Required.**—The Director and the Secretary shall carry out clause (i) in consultation with the following:

(I) The Federal Communications Commission.

(II) The Secretary of State.

(III) The Assistant Secretary of Commerce for Communications and Information.
(IV) The Director of the Defense Advanced Research Projects Agency.

(V) The Director of the Intelligence Advanced Research Projects Activity.

(VI) The Under Secretary of Commerce for Standards and Technology.

(C) ANNUAL REPORT TO CONGRESS.—

(i) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act and not less frequently than once each fiscal year thereafter until fiscal year 2031, the Director and the Secretary shall jointly submit to the appropriate committees of Congress an annual report on the Multilateral Fund and the use of amounts under subparagraph (B).

(ii) CONTENTS.—Each report submitted under clause (i) shall include, for the fiscal year covered by the report, the following:

(I) Any funding commitments from foreign partners, including each specific amount committed.
(II) Governing criteria for use of the amounts in the Multilateral Fund.

(III) An account of—

(aa) how, and to whom, funds have been deployed;

(bb) amounts remaining in the Multilateral Fund; and

(cc) the progress of the Director and the Secretary in meeting the objective described in subparagraph (B)(i).

(IV) Such recommendations for legislative or administrative action as the Director and the Secretary may have to enhance the effectiveness of the Multilateral Fund in achieving the security goals of the United States.

(3) Authorization of Appropriations.—

(A) Communications Technology Security and Innovation Fund.—There is authorized to be appropriated to carry out paragraph (1) $750,000,000 for the period of fiscal years 2021 through 2031.

(B) Multilateral Telecommunications Security Fund.—There is authorized
to be appropriated to carry out paragraph (2) $750,000,000 for the period of fiscal years 2021 through 2031.

(c) Exposing Political Pressure in International Standards-setting Bodies That Set Standards for Fifth-generation Wireless Networks.—

(1) Report required.—

(A) In general.—Not later than 120 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report on political pressure within international forums that set standards for fifth-generation wireless networks and for future generations of wireless networks, including—

(i) the International Telecommunication Union (ITU);

(ii) the International Organization for Standardization (ISO);

(iii) the Inter-American Telecommunication Commission (CITEL); and

(iv) the voluntary standards organizations that develop protocols for wireless devices and other equipment, such as the 3rd
Generation Partnership Project (3GPP) and the Institute of Electrical and Electronics Engineers (IEEE).

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

(2) CONSULTATION REQUIRED.—The Director and the Secretary shall carry out paragraph (1) in consultation with the following:

(A) The Federal Communications Commission.

(B) The Secretary of State.

(C) The Assistant Secretary of Commerce for Communications and Information.

(D) The Director of the Defense Advanced Research Projects Agency.

(E) The Director of the Intelligence Advanced Research Projects Activity.

(F) The Under Secretary of Commerce for Standards and Technology.

(d) EXPANDING FIFTH-GENERATION WIRELESS NETWORK TESTBEDS TO INCREASE SUPPLIER DIVERSITY AND SECURITY USING OPEN-ARCHITECTURE STANDARDS.—
(1) REPORT REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence and the Secretary of Defense shall jointly submit to the appropriate committees of Congress a report on developing fifth-generation wireless network testbeds for development of military and dual-use applications that use open interface, standards-based compatible interoperable equipment, such as equipment developed pursuant to the standards set forth by organizations such as the O–RAN Alliance, the Telecom Infra Project, the 3rd Generation Partnership Project (3GPP), the O–RAN Software Community, or any successor organizations.

(2) FOREIGN EFFORTS.—The report submitted under paragraph (1) shall include information about ongoing efforts by China and the United Kingdom to build similar testbeds for virtualized telecommunications technologies.
SEC. 502. REPORT ON ATTEMPTS BY FOREIGN ADVERSARIES TO BUILD TELECOMMUNICATIONS AND CYBERSECURITY EQUIPMENT AND SERVICES FOR, OR TO PROVIDE SUCH EQUIPMENT AND SERVICES TO, CERTAIN ALLIES OF THE UNITED STATES.

(a) Definitions.—In this section:

(1) Appropriate committees of Congress.—The term “appropriate committees of Congress” means—

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

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

(2) Five Eyes country.—The term “Five Eyes country” means any of the following:

(A) Australia.

(B) Canada.

(C) New Zealand.

(D) The United Kingdom.

(E) The United States.

(b) Report Required.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency, the Director of the Na-
tional Security Agency, and the Director of the Defense Intelligence Agency shall jointly submit to the appropriate committees of Congress a report on attempts by foreign adversaries to build telecommunications and cybersecurity equipment and services for, or to provide such equipment and services to, Five Eyes countries.

(c) ELEMENTS.—The report submitted under subsection (b) shall include the following:

(1) An assessment of United States intelligence sharing and intelligence and military force posture in any Five Eyes country that currently uses or intends to use telecommunications or cybersecurity equipment or services provided by a foreign adversary of the United States, including China and Russia.

(2) A description and assessment of mitigation of any potential compromises or risks for any circumstance described in paragraph (1).

(d) FORM.—The report required by subsection (b) shall include an unclassified executive summary, and may include a classified annex.
SEC. 503. REPORT ON THREATS POSED BY USE BY FOREIGN GOVERNMENTS AND ENTITIES OF COMMERCIALLY AVAILABLE CYBER INTRUSION AND SURVEILLANCE TECHNOLOGY.

(a) Report Required.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the threats posed by the use by foreign governments and entities of commercially available cyber intrusion and other surveillance technology.

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

(1) Matters relating to threats described in subsection (a) as they pertain to the following:

(A) The threat posed to United States persons and persons inside the United States.

(B) The threat posed to United States personnel overseas.

(C) The threat posed to employees of the Federal Government, including through both official and personal accounts and devices.

(2) A description of which foreign governments and entities pose the greatest threats from the use of technology described in subsection (a) and the nature of those threats.
(3) An assessment of the source of the commercially available cyber intrusion and other surveillance technology that poses the threats described in subsection (a), including whether such technology is made by United States companies or companies in the United States or by foreign companies.

(4) An assessment of actions taken, as of the date of the enactment of this Act, by the Federal Government and foreign governments to limit the export of technology described in subsection (a) from the United States or foreign countries to foreign governments and entities in ways that pose the threats described in such subsection.

(5) Matters relating to how the Federal Government, Congress, and foreign governments can most effectively mitigate the threats described in subsection (a), including matters relating to the following:

(A) Working with the technology and telecommunications industry to identify and improve the security of consumer software and hardware used by United States persons and persons inside the United States that is targeted by commercial cyber intrusion and surveillance software.
(B) Export controls.

(C) Diplomatic pressure.

(D) Trade agreements.

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

SEC. 504. REPORTS ON RECOMMENDATIONS OF THE CYBERSPACE SOLARIUM COMMISSION.

(a) FINDINGS.—Congress makes the following findings:

(1) The report issued by the Cyberspace Solarium Commission under section 1652(k) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) is an important contribution toward better defending the United States against cyber attacks of catastrophic consequence.

(2) The recommendations in such report provide potentially important opportunities for the private and public sectors to implement critical changes that could harden United States defenses against cyber attacks.

(b) REPORTS REQUIRED.—Not later than 180 days after the date of the enactment of this Act, each head of an agency described in subsection (c) shall submit to Con-

(c) Agencies Described.—The agencies described in this subsection are the following:

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

(2) The Department of Homeland Security.

(3) The Department of Energy.

(4) The Department of Commerce.

(5) The Department of Defense.

(d) Contents.—Each report submitted under subsection (b) by the head of an agency described in subsection (c) shall include the following:

(1) An evaluation of the recommendations in the report described in subsection (b) that pertain to the agency.

(2) A description of the actions taken, or the actions that the head of the agency expects to take, to implement any of the recommendations included in such report.

(e) Actions Through Officers.—
(1) **Under Secretary of Homeland Security for Intelligence and Analysis.**—In submitting a report under subsection (b), the Secretary of Homeland Security shall do so by acting through the Under Secretary of Homeland Security for Intelligence and Analysis.

(2) **Director of Intelligence and Counterintelligence of Department of Energy.**—In submitting a report under subsection (b), the Secretary of Energy shall do so by acting through the Director of Intelligence and Counterintelligence of the Department of Energy.

**SEC. 505. ASSESSMENT OF CRITICAL TECHNOLOGY TRENDS RELATING TO ARTIFICIAL INTELLIGENCE, MICROCHIPS, AND SEMICONDUCTORS AND RELATED SUPPLY CHAINS.**

(a) **Assessment Required.**—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall complete a detailed assessment of critical technology trends relating to artificial intelligence, microchips, and semiconductors and related supply chains.

(b) **Elements.**—The assessment required by subsection (a) shall include the following:

(1) **Export Controls.**—
(A) **IN GENERAL.**—An assessment of efforts by partner countries to enact and implement export controls and other technology transfer measures with respect to artificial intelligence, microchips, advanced manufacturing equipment, and other artificial intelligence enabled technologies critical to United States supply chains.

(B) **IDENTIFICATION OF OPPORTUNITIES FOR COOPERATION.**—The assessment under subparagraph (A) shall identify opportunities for further cooperation with international partners on a multilateral and bilateral basis to strengthen export control regimes and address technology transfer threats.

(2) **SEMICONDUCTOR SUPPLY CHAINS.**—

(A) **IN GENERAL.**—An assessment of global semiconductor supply chains, including areas to reduce United States vulnerabilities and maximize points of leverage.

(B) **ANALYSIS OF POTENTIAL EFFECTS.**—The assessment under subparagraph (A) shall include an analysis of the potential effects of significant geopolitical shifts, including those related to Taiwan.
(C) Identification of opportunities for diversification.—The assessment under subparagraph (A) shall also identify opportunities for diversification of United States supply chains, including an assessment of cost, challenges, and opportunities to diversify manufacturing capabilities on a multinational basis.

(3) Computing power.—An assessment of trends relating to computing power and the effect of such trends on global artificial intelligence development and implementation, in consultation with the Director of the Intelligence Advanced Research Projects Activity, the Director of the Defense Advanced Research Projects Agency, and the Director of the National Institute of Standards and Technology, including forward-looking assessments of how computing resources may affect United States national security, innovation, and implementation relating to artificial intelligence.

e) Report.—

(1) Definition of appropriate committees of Congress.—In this subsection, the term “appropriate committees of Congress” means—

(A) the Select Committee on Intelligence, the Committee on Armed Services, the Com-
mittee on Banking, Housing, and Urban Affairs, and the Committee on Foreign Relations of the Senate; and

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

(2) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director shall submit to the appropriate committees of Congress a report on the findings of the Director with respect to the assessment completed under subsection (a).

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

SEC. 506. DUTY TO REPORT COUNTERINTELLIGENCE THREATS TO CAMPAIGNS.

(a) IN GENERAL.—Section 304 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30104) is amended by adding at the end the following new subsection:

“(j) DISCLOSURE OF REPORTABLE FOREIGN CONTACTS.—
“(1) COMMITTEE OBLIGATION.—Not later than 1 week after a reportable foreign contact, each authorized committee of a candidate for President shall notify the Federal Bureau of Investigation of the reportable foreign contact and provide a summary of the circumstances with respect to such reportable foreign contact.

“(2) INDIVIDUAL OBLIGATION.—Not later than 1 week after a reportable foreign contact—

“(A) each candidate for the office of President shall notify the treasurer or other designated official of the principal campaign committee of such candidate of the reportable foreign contact and provide a summary of the circumstances with respect to such reportable foreign contact; and

“(B) each official, employee, or agent of an authorized committee of a candidate for the office of President shall notify the treasurer or other designated official of the authorized committee of the reportable foreign contact and provide a summary of the circumstances with respect to such reportable foreign contact.

“(3) REPORTABLE FOREIGN CONTACT.—In this subsection:
“(A) IN GENERAL.—The term ‘reportable foreign contact’ means any direct or indirect contact or communication that—

“(i) is between—

“(I) a candidate for the office of President, an authorized committee of such a candidate, or any official, employee, or agent of such authorized committee; and

“(II) an individual that the person described in subclause (I) knows, has reason to know, or reasonably believes is a covered foreign national; and

“(ii) the person described in clause (i)(I) knows, has reason to know, or reasonably believes involves—

“(I) a contribution, donation, expenditure, disbursement, or solicitation described in section 319; or

“(II) coordination or collaboration with an offer or provision of information or services to or from, or persistent and repeated contact with a
covered foreign national in connection with an election.

“(B) EXCEPTION.—Such term shall not include any contact or communication with a covered foreign national by an elected official or an employee of an elected official solely in an official capacity as such an official or employee.

“(C) COVERED FOREIGN NATIONAL DEFINED.—

“(i) IN GENERAL.—In this paragraph, the term ‘covered foreign national’ means—

“(I) a foreign principal (as defined in section 1(b) of the Foreign Agents Registration Act of 1938 (22 U.S.C. 611(b)) that is a government of a foreign country or a foreign political party;

“(II) any person who acts as an agent, representative, employee, or servant, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign principal described in subclause (I) or of a person any of
whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in major part by a foreign principal described in subclause (I); or

“(III) any person included in the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury pursuant to authorities relating to the imposition of sanctions relating to the conduct of a foreign principal described in subclause (I).

“(ii) CLARIFICATION REGARDING APPLICATION TO CITIZENS OF THE UNITED STATES.—In the case of a citizen of the United States, subclause (II) of clause (i) applies only to the extent that the person involved acts within the scope of that person’s status as the agent of a foreign principal described in subclause (I) of clause (i).

“(4) CLARIFICATION REGARDING VOLUNTEERS.—For purposes of paragraphs (2)(B) and
(3)(A)(i)(I), an unpaid volunteer shall not be treated as an official, employee, or agent of an authorized committee unless such unpaid volunteer has a significant supervisory role or provides advice or input to the candidate or to senior officials of the authorized committee.”.

(b) FEDERAL CAMPAIGN FOREIGN CONTACT REPORTING COMPLIANCE SYSTEM.—Section 302(e) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30102(e)) is amended by adding at the end the following new paragraph:

“(6) REPORTABLE FOREIGN CONTACTS COMPLIANCE POLICY.—

“(A) REPORTING.—Each authorized committee of a candidate for the office of President shall establish a policy that requires all officials, employees, and agents of such committee to notify the treasurer or other appropriate designated official of the committee of any reportable foreign contact (as defined in section 304(j)) not later than 1 week after such contact was made.

“(B) RETENTION AND PRESERVATION OF RECORDS.—Each authorized committee of a candidate for the office of President shall estab-
lish a policy that provides for the retention and 
preservation of records and information related 
to reportable foreign contacts (as so defined) 
for a period of not less than 3 years.

“(C) CERTIFICATION.—Upon designation 
of a political committee as an authorized com-
mittee by a candidate for the office of Presi-
dent, and with each report filed by such com-
mittee under section 304(a), the candidate shall 
certify that—

“(i) the committee has in place poli-
cies that meet the requirements of sub-
paragraphs (A) and (B);

“(ii) the committee has designated an 
official to monitor compliance with such 
policies; and

“(iii) not later than 1 week after the 
beginning of any formal or informal affili-
ation with the committee, all officials, em-
ployees, and agents of such committee 
will—

“(I) receive notice of such poli-
cies;

“(II) be informed of the prohibi-
tions under section 319; and
“(III) sign a certification affirming their understanding of such policies and prohibitions.”.

(c) CRIMINAL PENALTIES.—Section 309(d)(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30109(d)(1)) is amended by adding at the end the following new subparagraphs:

“(E) Any person who knowingly and willfully commits a violation of section 304(j) or section 302(e)(6) shall be fined under title 18, United States Code, imprisoned for not more than 3 years, or both.

“(F) Any person who knowingly and willfully conceals or destroys any materials relating to a reportable foreign contact (as defined in section 304(j)) shall be fined under title 18, United States Code, imprisoned for not more than 3 years, or both.”.

(d) RULE OF CONSTRUCTION.—Nothing in this section or the amendments made by this section shall be construed—

(1) to impede legitimate journalistic activities;

or

(2) to impose any additional limitation on the right of any individual who is not a citizen of the
United States or a national of the United States (as defined in section 101(a)(22) of the Immigration and Nationality Act) and who is not lawfully admitted for permanent residence, as defined by section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(20)) to express political views or to participate in public discourse.

SEC. 507. COMBATING CHINESE INFLUENCE OPERATIONS IN THE UNITED STATES AND STRENGTHENING CIVIL LIBERTIES PROTECTIONS.

(a) Updates to Annual Reports on Influence Operations and Campaigns in the United States by the Chinese Communist Party.—Section 1107(b) of the National Security Act of 1947 (50 U.S.C. 3237(b)) is amended—

(1) by redesignating paragraph (8) as paragraph (9); and

(2) by inserting after paragraph (7) the following:

“(8) An identification of influence activities and operations employed by the Chinese Communist Party against the United States science and technology sectors, specifically employees of the United States Government, researchers, scientists, and stu-
(b) **Plan for Federal Bureau of Investigation to Increase Public Awareness and Detection of Influence Activities by the Government of the People’s Republic of China.**—

(1) **Plan Required.**—Not later than 90 days after the date of the enactment of this Act, the Director of the Federal Bureau of Investigation shall submit to the congressional intelligence committees a plan—

(A) to increase public awareness of influence activities by the Government of the People’s Republic of China; and

(B) to publicize mechanisms that members of the public can use—

(i) to detect such activities; and

(ii) to report such activities to the Bureau.

(2) **Consultation.**—In carrying out paragraph (1), the Director shall consult with the following:

(A) The Director of the Office of Science and Technology Policy.
(B) Such other stakeholders outside the intelligence community, including professional associations, institutions of higher education, businesses, and civil rights and multicultural organizations, as the Director determines relevant.

(e) **Recommendations of the Federal Bureau of Investigation to Strengthen Relationships and Build Trust With Communities of Interest.**—

(1) **In general.**—The Director of the Federal Bureau of Investigation, in consultation with the Assistant Attorney General for the Civil Rights Division and the Chief Privacy and Civil Liberties Officer of the Department of Justice, shall develop recommendations to strengthen relationships with communities targeted by influence activities of the Government of the People’s Republic of China and build trust with such communities through local and regional grassroots outreach.

(2) **Submittal to Congress.**—Not later than 1 year after the date of the enactment of this Act, the Director shall submit to Congress the recommendations developed under paragraph (1).

(d) **Technical Corrections.**—The National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended—
(1) in section 1107 (50 U.S.C. 3237)—

   (A) in the section heading, by striking "COMMUNIST PARTY OF CHINA" and inserting "CHINESE COMMUNIST PARTY"; and

   (B) by striking "Communist Party of China" both places it appears and inserting "Chinese Communist Party"; and

(2) in the table of contents before section 2 (50 U.S.C. 3002), by striking the item relating to section 1107 and inserting the following new item:

"Sec. 1107. Annual reports on influence operations and campaigns in the United States by the Chinese Communist Party."

SEC. 508. ANNUAL REPORT ON CORRUPT ACTIVITIES OF SENIOR OFFICIALS OF THE CHINESE COMMUNIST PARTY.

   (a) Definition of appropriate committees of Congress.—In this section, the term "appropriate committees of Congress" means—

   (1) the Committee on Banking, Housing, and Urban Affairs, the Committee on Finance, the Committee on Foreign Relations, and the Select Committee on Intelligence of the Senate; and

   (2) the Committee on Financial Services, the Committee on Foreign Affairs, the Committee on Ways and Means, and the Permanent Select Com-
mittee on Intelligence of the House of Representatives.

(b) **Annual Report Required.**—

(1) **In general.**—Not later than 90 days after the date of the enactment of this Act, and annually thereafter through 2025, the Director of the Central Intelligence Agency shall submit to the appropriate committees of Congress a report on the corruption and corrupt activities of senior officials of the Chinese Communist Party.

(2) **Elements.**—

(A) **In general.**—Each report under paragraph (1) shall include the following:

(i) A description of the wealth of, and corruption and corrupt activities among, senior officials of the Chinese Communist Party.

(ii) A description of any recent actions of the officials described in clause (i) that could be considered a violation, or potential violation, of United States law.

(iii) A description and assessment of targeted financial measures, including potential targets for designation of the officials described in clause (i) for the corrup-
tion and corrupt activities described in that clause and for the actions described in clause (ii).

(B) Scope of reports.—The first report under paragraph (1) shall include comprehensive information on the matters described in subparagraph (A). Any succeeding report under paragraph (1) may consist of an update or supplement to the preceding report under that subsection.

(3) Coordination.—In preparing each report, update, or supplement under this subsection, the Director of the Central Intelligence Agency shall coordinate as follows:

(A) In preparing the description required by clause (i) of paragraph (2)(A), the Director of the Central Intelligence Agency shall coordinate with the head of the Office of Intelligence and Analysis of the Department of the Treasury and the Director of the Federal Bureau of Investigation.

(B) In preparing the descriptions required by clauses (ii) and (iii) of such paragraph, the Director of the Central Intelligence Agency shall coordinate with the head of the Office of
Intelligence and Analysis of the Department of the Treasury.

(4) FORM.—Each report under paragraph (1) shall include an unclassified executive summary, and may include a classified annex.

(c) SENSE OF CONGRESS.—It is the sense of Congress that the United States should undertake every effort and pursue every opportunity to expose the corruption and illicit practices of senior officials of the Chinese Communist Party, including President Xi Jinping.

SEC. 509. REPORT ON CORRUPT ACTIVITIES OF RUSSIAN AND OTHER EASTERN EUROPEAN OLIGARCHS.

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

(1) the Committee on Banking, Housing, and Urban Affairs, the Committee on Finance, the Committee on Foreign Relations, and the Select Committee on Intelligence of the Senate; and

(2) the Committee on Financial Services, the Committee on Foreign Affairs, the Committee on Ways and Means, and the Permanent Select Committee on Intelligence of the House of Representa-
(b) Report Required.—Not later than 100 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall submit to the appropriate committees of Congress and the Undersecretary of State for Public Diplomacy and Public Affairs a report on the corruption and corrupt activities of Russian and other Eastern European oligarchs.

(c) Elements.—

(1) In general.—Each report under subsection (b) shall include the following:

(A) A description of corruption and corrupt activities among Russian and other Eastern European oligarchs who support the Government of the Russian Federation, including estimates of the total assets of such oligarchs.

(B) An assessment of the impact of the corruption and corrupt activities described pursuant to subparagraph (A) on the economy and citizens of Russia.

(C) A description of any connections to, or support of, organized crime, drug smuggling, or human trafficking by an oligarch covered by subparagraph (A).

(D) A description of any information that reveals corruption and corrupt activities in Rus-
sia among oligarchs covered by subparagraph (A).

(E) A description and assessment of potential sanctions actions that could be imposed upon oligarchs covered by subparagraph (A) who support the leadership of the Government of Russia, including President Vladimir Putin.

(2) **Scope of reports.**—The first report under subsection (a) shall include comprehensive information on the matters described in paragraph (1). Any succeeding report under subsection (a) may consist of an update or supplement to the preceding report under that subsection.

(d) **Coordination.**—In preparing each report, update, or supplement under this section, the Director of the Central Intelligence Agency shall coordinate as follows:

(1) In preparing the assessment and descriptions required by subparagraphs (A) through (D) of subsection (c)(1), the Director of the Central Intelligence Agency shall coordinate with the head of the Office of Intelligence and Analysis of the Department of the Treasury and the Director of the Federal Bureau of Investigation.

(2) In preparing the description and assessment required by subparagraph (E) of such subsection,
the Director of the Central Intelligence Agency shall
coordinate with the head of the Office of Intelligence
and Analysis of the Department of the Treasury.

(e) FORM.—

(1) IN GENERAL.—Subject to paragraph (2),
each report under subsection (b) shall include an un-
classified executive summary, and may include a
classified annex.

(2) UNCLASSIFIED FORM OF CERTAIN INFOR-
MATION.—The information described in subsection
(c)(1)(D) in each report under subsection (b) shall
be submitted in unclassified form.

SEC. 510. REPORT ON BIOSECURITY RISK AND
DISINFORMATION BY THE CHINESE COM-
MUNIST PARTY AND THE GOVERNMENT OF
THE PEOPLE'S REPUBLIC OF CHINA.

(a) DEFINITIONS.—In this section:

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

(A) the Select Committee on Intelligence,
the Committee on Armed Services, the Com-
mittee on Foreign Relations, the Committee on
Health, Education, Labor, and Pensions, and
the Committee on Homeland Security and Governmental Affairs of the Senate; and

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

(2) CRITICAL INFRASTRUCTURE.—The term “critical infrastructure” has the meaning given such term in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e)).

(b) REPORT REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report identifying whether and how officials of the Chinese Communist Party and the Government of the People’s Republic of China may have sought—

(1) to suppress information about—

(A) the outbreak of the novel coronavirus in Wuhan;
(B) the spread of the virus through China;

and

(C) the transmission of the virus to other countries;

(2) to spread disinformation relating to the pandemic; or

(3) to exploit the pandemic to advance their national security interests.

(e) Assessments.—The report required by subsection (b) shall include assessments of reported actions and the effect of those actions on efforts to contain the novel coronavirus pandemic, including each of the following:

(1) The origins of the novel coronavirus outbreak, the time and location of initial infections, and the mode and speed of early viral spread.

(2) Actions taken by the Government of China to suppress, conceal, or misinform the people of China and those of other countries about the novel coronavirus outbreak in Wuhan.

(3) The effect of disinformation or the failure of the Government of China to fully disclose details of the outbreak on response efforts of local governments in China and other countries.
(4) Diplomatic, political, economic, intelligence, or other pressure on other countries and international organizations to conceal information about the spread of the novel coronavirus and the response of the Government of China to the contagion, as well as to influence or coerce early responses to the pandemic by other countries.

(5) Efforts by officials of the Government of China to deny access to health experts and international health organizations to afflicted individuals in Wuhan, pertinent areas of the city, or laboratories of interest in China, including the Wuhan Institute of Virology.

(6) Efforts by the Government of China, or those acting at its direction or with its assistance, to conduct cyber operations against international, national, or private health organizations conducting research relating to the novel coronavirus or operating in response to the pandemic.

(7) Efforts to control, restrict, or manipulate relevant segments of global supply chains, particularly in the sale, trade, or provision of relevant medicines, medical supplies, or medical equipment as a result of the pandemic.
(8) Efforts to advance the economic, intelligence, national security, and political objectives of the Government of China by exploiting vulnerabilities of foreign governments, economies, and companies under financial duress as a result of the pandemic or to accelerate economic espionage and intellectual property theft.

(9) Efforts to exploit the disruption of the pharmaceutical and telecommunications industries as well as other industries tied to critical infrastructure and bilateral trade between China and the United States and between China and allies and partners of the United States in order to advance the economic and political objectives of the Government of China following the pandemic.

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

SEC. 511. REPORT ON EFFECT OF LIFTING OF UNITED NATIONS ARMS EMBARGO ON ISLAMIC REPUBLIC OF IRAN.

(a) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term “appropriate committees of Congress” means—
(1) the Select Committee on Intelligence, the Committee on Armed Services, and the Committee on Foreign Relations of the Senate; and

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

(b) REPORT REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of the Defense Intelligence Agency, in consultation with such heads of other elements of the intelligence community as the Director considers appropriate, shall submit to the appropriate committees of Congress a report on—

(1) the plans of the Government of the Islamic Republic of Iran to acquire military arms if the ban on arms transfers to or from such government under United Nations Security Council resolutions are lifted; and

(2) the effect such arms acquisitions may have on regional security and stability.

(c) CONTENTS.—The report submitted under subsection (b) shall include assessments relating to plans of the Government of the Islamic Republic of Iran to acquire additional weapons, the intention of other countries to provide such weapons, and the effect such acquisition and
provision would have on regional stability, including with respect to each of the following:

   (1) The type and quantity of weapon systems under consideration for acquisition.

   (2) The countries of origin of such systems.

   (3) Likely reactions of other countries in the region to such acquisition, including the potential for proliferation by other countries in response.

   (4) The threat that such acquisition could present to international commerce and energy supplies in the region, and the potential implications for the national security of the United States.

   (5) The threat that such acquisition could present to the Armed Forces of the United States, of countries allied with the United States, and of countries partnered with the United States stationed in or deployed in the region.

   (6) The potential that such acquisition could be used to deliver chemical, biological, or nuclear weapons.

   (7) The potential for the Government of the Islamic Republic of Iran to proliferate weapons acquired in the absence of an arms embargo to regional groups, including Shi’a militia groups backed by such government.
SEC. 512. REPORT ON IRANIAN ACTIVITIES RELATING TO NUCLEAR NONPROLIFERATION.

(a) Definition of Appropriate Committees of Congress.—In this section, the term “appropriate committees of Congress” means—

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

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

(b) Report Required.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate committees of Congress a report assessing—

(1) any relevant activities potentially relating to nuclear weapons research and development by the Islamic Republic of Iran; and

(2) any relevant efforts to afford or deny international access in accordance with international non-proliferation agreements.
(c) ASSESSMENTS.—The report required by subsection (b) shall include assessments, for the period beginning on January 1, 2018, and ending on the date of the submittal of the report, of the following:

(1) Activities to research, develop, or enrich uranium or reprocess plutonium with the intent or capability of creating weapons-grade nuclear material.

(2) Research, development, testing, or design activities that could contribute to or inform construction of a device intended to initiate or capable of initiating a nuclear explosion.

(3) Efforts to receive, transmit, store, destroy, relocate, archive, or otherwise preserve research, processes, products, or enabling materials relevant or relating to any efforts assessed under paragraph (1) or (2).

(4) Efforts to afford or deny international access, in accordance with international nonproliferation agreements, to locations, individuals, and materials relating to activities described in paragraph (1), (2), or (3).

(d) FORM.—The report required under subsection (b) shall be submitted in unclassified form, but may include a classified annex.
SEC. 513. SENSE OF CONGRESS ON THIRD OPTION FOUNDATION.

It is the sense of the Congress that—

(1) the work of the Third Option Foundation to heal, help, and honor members of the special operations community of the Central Intelligence Agency and their families is invaluable; and

A BILL

S. 3905

To authorize appropriations for fiscal year 2021 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

JUNE 8, 2020

Read twice and placed on the calendar

VerDate Sep 11 2014 00:27 Jun 09, 2020 Jkt 099200 PO 00000 Frm 00144 Fmt 6651 Sfmt 6651 E:\BILLS\S3905.RS S3905kjohnson on DSK79L0C42PROD with BILLS