(K) Life-cycle cost per baseline vessel and each alternative vessel.

(L) Life-cycle cost per specified quantity of baseline vessels and alternative vessels.

(M) Technology readiness assessment of baseline and each alternative. Assessment.

(N) Analysis of alternatives, including relative cost and capability performance of baseline and alternative vessels.

(O) Trade-off analysis.

(P) Sensitivity analysis.

(Q) Conclusions and recommendations, which if the Secretary of Defense deems it appropriate, shall include the determination required under subsection (d)(1)(B). Recommendations.

(f) DEFINITIONS.—In this section:

(1) The term "critical mission, hull, mechanical, and electrical subsystems", with respect to a covered vessel, includes the following subsystems:

(A) Command, control, communications, computers, intelligence, surveillance, and reconnaissance.

(B) Autonomous vessel navigation, vessel control, contact management, and contact avoidance.

(C) Communications security, including cryptopgraphy, encryption, and decryption.

(D) Main engines, including the lube oil, fuel oil, and other supporting systems.

(E) Electrical generation and distribution, including supporting systems.

(F) Military payloads.

(G) Any other subsystem identified as critical by the Senior Technical Authority for the class of naval vessels that includes the covered vessel.

(2) The term "Senior Technical Authority" means, with respect to a class of naval vessels, the Senior Technical Authority designated for that class of naval vessels under section 8669b of title 10, United States Code.

Subtitle C—Artificial Intelligence and Emerging Technology

SEC. 231. MODIFICATION OF BIANNUAL REPORT ON THE JOINT ARTIFICIAL INTELLIGENCE CENTER.

Section 260(b) of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1293) is amended by adding at the end the following new paragraphs:

"(11) The results of an assessment, conducted biannually, on the efforts of the Center and the Department of Defense to develop or contribute to the development of standards for artificial intelligence, including— Assessments. Time period.

"(A) a description of such efforts;

"(B) an evaluation of the need to incorporate standards for artificial intelligence into the strategies and doctrine of the Department and a description of any efforts undertaken to further the development and adoption of such standards; Evaluation.

"(C) an explanation of any collaboration on artificial intelligence standards development with—

"(i) other organizations and elements of the Department of Defense (including the Defense Agencies and the military departments);

"(ii) agencies of the Federal Government;

"(iii) the intelligence community;

"(iv) representatives of the defense industrial base and other sectors of private industry; and

"(v) any other agencies, entities, organizations, or persons the Secretary considers appropriate; and

"(D) an explanation of any participation by the Center and the Department of Defense in international or other multi-stakeholder standard-setting bodies.

Time periods.

"(12) For each member of the Armed Forces who concluded a formal assignment supporting the Center in the period of six months preceding the date of the report, a position description of the billet that the member transitioned into, as provided to the Center by the Armed Force of the member within 30 days of reassignment.

Time period. Updates. Consultation.

"(13) An annual update, developed in consultation with the Armed Forces, on the status of active duty members of the Armed Forces assigned to the Center. This update shall include the following:

Assessment.

"(A) An assessment of the effectiveness of such assignments in strengthening the ties between the Center and the Armed Forces for the purposes of—

"(i) identifying tactical and operational use cases for artificial intelligence;

"(ii) improving data collection relating to artificial intelligence; and

"(iii) establishing effective lines of communication between the Center and the Armed Forces to identify and address concerns from the Armed Forces relating to the widespread adoption and dissemination of artificial intelligence.

"(B) A description of any efforts undertaken to create opportunities for additional nontraditional broadening assignments at the Center for members of the Armed Forces on active duty.

Analysis.

"(C) An analysis of the career trajectories of active duty members of the Armed Forces assigned to the Center, including any potential negative effects of such assignment on the career trajectories of such members.".

SEC. 232. MODIFICATION OF JOINT ARTIFICIAL INTELLIGENCE RESEARCH, DEVELOPMENT, AND TRANSITION ACTIVITIES.

Section 238 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2358 note) is amended—

(1) in subsection (a)—

(A) in paragraph (1), by inserting "acquire," before "develop"; and

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

"(2) EMPHASIS.—The set of activities established under paragraph (1) shall include—

"(A) acquisition and development of mature artificial intelligence technologies in support of defense missions;

"(B) applying artificial intelligence and machine learning solutions to operational problems by directly delivering artificial intelligence capabilities to the Armed Forces and other organizations and elements of the Department of Defense;

"(C) accelerating the development, testing, and fielding of new artificial intelligence and artificial intelligence-enabling capabilities; and

"(D) coordinating and deconflicting activities involving artificial intelligence and artificial intelligence-enabled capabilities within the Department.";

(2) by striking subsection (e);

(3) by redesignating subsections (c) and (d) as subsections (d) and (e), respectively;

(4) by inserting after subsection (b) the following new subsection:

"(c) ORGANIZATION AND ROLES.—

"(1) ASSIGNMENT OF ROLES AND RESPONSIBILITIES.—

"(A) IN GENERAL.—In addition to designating an official under subsection (b), the Secretary of Defense shall assign to appropriate officials within the Department of Defense roles and responsibilities relating to the research, development, prototyping, testing, procurement of, requirements for, and operational use of artificial intelligence technologies.

"(B) APPROPRIATE OFFICIALS.—The officials assigned roles and responsibilities under subparagraph (A) shall include—

"(i) the Under Secretary of Defense for Research and Engineering;

"(ii) the Under Secretary of Defense for Acquisition and Sustainment;

"(iii) the Director of the Joint Artificial Intelligence Center;

"(iv) one or more officials in each military department;

"(v) officials of appropriate Defense Agencies; and

"(vi) such other officials as the Secretary of Defense determines appropriate.

"(2) ROLE OF DIRECTOR OF THE JOINT ARTIFICIAL INTELLIGENCE CENTER.—

"(A) DIRECT REPORT TO DEPUTY SECRETARY OF DEFENSE.—During the covered period, the Director of the Joint Artificial Intelligence Center shall report directly to the Deputy Secretary of Defense without intervening authority.

"(B) CONTINUATION.—The Director of the Joint Artificial Intelligence Center shall continue to report to the Deputy Secretary of Defense as described in subparagraph (A) after the expiration of the covered period if, not later than 30 days before such period expires, the Deputy Secretary— Deadline.

"(i) determines that the Director should continue to report to Deputy Secretary without intervening authority; and Determination.

"(ii) transmits notice of such determination to the congressional defense committees. Notice.

"(C) COVERED PERIOD DEFINED.—In this paragraph, the term 'covered period' means the period of two years beginning on the date of the enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.";

(5) in subsection (d), as so redesignated—

(A) in paragraph (1), in the matter preceding subparagraph (A), by inserting "acquire," before "develop";

(B) in the heading of paragraph (2), by striking "DEVELOPMENT" and inserting "ACQUISITION, DEVELOPMENT"; and

(C) in paragraph (2)—

(i) in the matter preceding subparagraph (A), by striking "To the degree practicable, the designated official" and inserting "The official designated under subsection (b)";

(ii) in subparagraph (A), by striking "development" and inserting "acquisition";

(iii) by redesignating subparagraphs (H) and (I) as subparagraphs (J) and (K), respectively; and

(iv) by inserting after subparagraph (G), the following new subparagraphs:

"(H) develop standard data formats for the Department that—

"(i) aid in defining the relative maturity of datasets; and

"(ii) inform best practices for cost and schedule computation, data collection strategies aligned to mission outcomes, and dataset maintenance practices;

"(I) establish data and model usage agreements and collaborative partnership agreements for artificial intelligence product development with each organization and element of the Department, including each of the Armed Forces;";

(6) in subsection (e), as so redesignated—

Deadline. Regulations.

(A) by striking "The Secretary shall" and inserting "Not later than 180 days after the date of the enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, the Secretary of Defense shall issue regulations to";

(B) by striking "the coordination described in subsection (b) and the duties set forth in subsection (c)" and inserting "the duties set forth in subsection (d)"; and

(C) by adding at the end the following new sentence: "At a minimum, such access shall ensure that the Director of the Joint Artificial Intelligence Center has the ability to discover, access, share, and appropriately reuse data and models of the Armed Forces and other organizations and elements of the Department of Defense, build and maintain artificial intelligence capabilities for the Department, and execute the duties assigned to the Director by the Secretary."; and

(7) by adding at the end the following new subsection:

"(h) JOINT ARTIFICIAL INTELLIGENCE CENTER DEFINED.—In this section, term 'Joint Artificial Intelligence Center' means the Joint Artificial Intelligence Center of the Department of Defense established pursuant to the memorandum of the Secretary of Defense

dated June 27, 2018, and titled 'Establishment of the Joint Artificial Intelligence Center', or any successor to such Center.".

SEC. 233. BOARD OF ADVISORS FOR THE JOINT ARTIFICIAL INTELLIGENCE CENTER. 10 USC 4001 note.

(a) ESTABLISHMENT.—The Secretary of Defense shall establish a board of advisors for the Joint Artificial Intelligence Center.

(b) DUTIES.—The duties of the board of advisors shall include the following:

(1) Provide independent strategic advice and technical expertise to the Secretary and the Director on matters relating to the development and use of artificial intelligence by the Department of Defense.

(2) Evaluate and advise the Secretary and the Director on ethical matters relating to the development and use of artificial intelligence by the Department.

(3) Conduct long-term and long-range studies on matters relating to artificial intelligence, as required.

(4) Evaluate and provide recommendations to the Secretary and the Director regarding the Department's development of a robust workforce proficient in artificial intelligence.

(5) Assist the Secretary and the Director in developing strategic level guidance on artificial intelligence-related hardware procurement, supply-chain matters, and other technical matters relating to artificial intelligence.

(c) MEMBERSHIP.—The board of advisors shall be composed of appropriate experts from academic or private sector organizations outside the Department of Defense, who shall be appointed by the Secretary. Appointments.

(d) CHAIRPERSON.—The chairperson of the board of advisors shall be selected by the Secretary.

(e) MEETINGS.—The board of advisors shall meet not less than once each fiscal quarter and may meet at other times at the call of the chairperson or a majority of its members. Time period.

(f) REPORTS.—Not later than September 30 of each year through September 30, 2024, the board of advisors shall submit to the congressional defense committees a report that summarizes the activities of the board over the preceding year. Time period.

(g) DEFINITIONS.—In this section:

(1) The term "artificial intelligence" has the meaning given that term in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2358 note).

(2) The term "Director" means the Director of the Joint Artificial Intelligence Center.

(3) The term "Joint Artificial Intelligence Center" means the Joint Artificial Intelligence Center of the Department of Defense established pursuant to the memorandum of the Secretary of Defense dated June 27, 2018, and titled "Establishment of the Joint Artificial Intelligence Center", or any successor to such Center.

(4) The term "Secretary" means the Secretary of Defense.

SEC. 234. APPLICATION OF ARTIFICIAL INTELLIGENCE TO THE DEFENSE REFORM PILLAR OF THE NATIONAL DEFENSE STRATEGY. 10 USC 113 note.

(a) IDENTIFICATION OF USE CASES.—The Secretary of Defense, acting through such officers and employees of the Department of

Defense as the Secretary considers appropriate, including the chief data officers and chief management officers of the military departments, shall identify a set of no fewer than five use cases of the application of existing artificial intelligence enabled systems to support improved management of enterprise acquisition, personnel, audit, or financial management functions, or other appropriate management functions, that are consistent with reform efforts that support the National Defense Strategy.

Coordination.

(b) PROTOTYPING ACTIVITIES ALIGNED TO USE CASES.—The Secretary, acting through the Under Secretary of Defense for Research and Engineering and in coordination with the Director of the Joint Artificial Intelligence Center and such other officers and employees as the Secretary considers appropriate, shall pilot technology development and prototyping activities that leverage commercially available technologies and systems to demonstrate new artificial intelligence enabled capabilities to support the use cases identified under subsection (a).

Deadline.

(c) BRIEFING.—Not later than October 1, 2021, the Secretary shall provide to the congressional defense committees a briefing summarizing the activities carried out under this section.

SEC. 235. ACQUISITION OF ETHICALLY AND RESPONSIBLY DEVELOPED ARTIFICIAL INTELLIGENCE TECHNOLOGY.

(a) ASSESSMENT REQUIRED.—

Deadline.

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, shall conduct an assessment to determine—

(A) whether the Department of Defense has the ability, requisite resourcing, and sufficient expertise to ensure that any artificial intelligence technology acquired by the Department is ethically and responsibly developed; and

(B) how the Department can most effectively implement ethical artificial intelligence standards in acquisition processes and supply chains.

(2) ELEMENTS.—The assessment conducted under paragraph (1) shall address the following:

(A) Whether there are personnel occupying relevant roles within the Department of Defense who have sufficient expertise, across multiple disciplines (including ethical, legal, and technical expertise)—

(i) to advise on the acquisition of artificial intelligence technology; and

(ii) to ensure the acquisition of ethically and responsibly developed artificial intelligence technology.

(B) The feasibility and advisability of retaining outside experts as consultants to assist the Department in strengthening capacity and filling any gaps in expertise identified under subparagraph (A).

(C) The extent to which existing acquisition processes encourage or require consultation with relevant experts across multiple disciplines within the Department to ensure that artificial intelligence technology acquired by the Department is ethically and responsibly developed.

(D) Quantitative and qualitative standards for assessing the extent to which experts across multiple disciplines are engaged in the acquisition of artificial intelligence technology by the department.

(b) BRIEFING REQUIRED.—

(1) IN GENERAL.—Not later than 30 days after the date on which the Secretary of Defense completes the assessment under subsection (a), the Secretary shall provide to the congressional defense committees a briefing on the results of the assessment. Deadline.

(2) ELEMENTS.—The briefing under paragraph (1) shall include, based on the results of the assessment—

(A) an explanation of whether the Department of Defense has personnel, in the proper roles and with sufficient expertise across multiple disciplines, to ensure the acquisition of ethically and responsibly developed artificial intelligence technology;

(B) an explanation of whether the Department has adequate procedures to encourage or require the consultation of such experts as part of the acquisition process for artificial intelligence technology;

(C) an explanation of any procedures the Department has in place to ensure that activities involving artificial intelligence are consistent with the Department's ethical artificial intelligence standards; and

(D) with respect to any deficiencies identified under subparagraph (A), (B), or (C), a description of any measures that have been taken, and any additional resources that may be needed, to mitigate such deficiencies.

SEC. 236. STEERING COMMITTEE ON EMERGING TECHNOLOGY. 10 USC 4001 note.

(a) ESTABLISHMENT.—The Secretary of Defense may establish a steering committee on emerging technology and national security threats (referred to in this section as the "Steering Committee").

(b) MEMBERSHIP.—The Steering Committee shall be composed of the following:

(1) The Deputy Secretary of Defense.

(2) The Vice Chairman of the Joint Chiefs of Staff.

(3) The Under Secretary of Defense for Intelligence and Security.

(4) The Under Secretary of Defense for Research and Engineering.

(5) The Under Secretary of Defense for Personnel and Readiness.

(6) The Under Secretary of Defense for Acquisition and Sustainment.

(7) The Chief Information Officer.

(8) Such other officials of the Department of Defense as the Secretary of Defense determines appropriate.

(c) RESPONSIBILITIES.—The Steering Committee shall be responsible for—

(1) developing a strategy for the organizational change, concept and capability development, and technology investments in emerging technologies that are needed to maintain the technological superiority of the United States military as outlined in the National Defense Strategy;

(2) providing assessments of emerging threats and identifying investments and advances in emerging technology areas undertaken by adversaries of the United States;

(3) making recommendations to the Secretary of Defense on—

(A) the implementation of the strategy developed under paragraph (1);

(B) steps that may be taken to address the threats identified under paragraph (2);

(C) any changes to a program of record that may be required to achieve the strategy under paragraph (1);

(D) any changes to the Defense Planning Guidance required by section 113(g)(2)(A) of title 10, United States Code, that may be required to achieve the strategy under paragraph (1); and

(E) whether sufficient resources are available for the research activities, workforce, and infrastructure of the Department of Defense to support the development of capabilities to defeat emerging threats to the United States; and

(4) carrying out such other activities as are assigned to the Steering Committee by the Secretary of Defense.

(d) EMERGING TECHNOLOGY DEFINED.—In this section, the term "emerging technology" means technology determined to be in an emerging phase of development by the Secretary, including quantum information science and technology, data analytics, artificial intelligence, autonomous technology, advanced materials, software, high performance computing, robotics, directed energy, hypersonics, biotechnology, medical technologies, and such other technology as may be identified by the Secretary.

(e) SUNSET.—This section shall terminate on October 1, 2024.

Subtitle D—Education and Workforce Development

10 USC 501 note prec.

SEC. 241. MEASURING AND INCENTIVIZING PROGRAMMING PROFICIENCY.

Deadline.

(a) IN GENERAL.—Not later than two years after the date of the enactment of this Act, the Secretary of Defense shall carry out the following activities:

(1) Leverage existing civilian software development and software architecture certification programs to implement coding language proficiency and artificial intelligence competency tests within the Department of Defense that—

(A) measure an individual's competency in using machine learning tools, in a manner similar to the way the Defense Language Proficiency Test measures competency in foreign language skills;

(B) enable the identification of members of the Armed Forces and civilian employees of the Department of Defense who have varying levels of quantified coding comprehension and skills and a propensity to learn new programming paradigms, algorithms, and data analytics; and

(C) include hands-on coding demonstrations and challenges.

Update. Records.

(2) Update existing recordkeeping systems to track artificial intelligence and programming certification testing results in a manner that is comparable to the system used for tracking and documenting foreign language competency, and use that recordkeeping system to ensure that workforce coding and

artificial intelligence comprehension and skills are taken into consideration when making assignments.

(3) Implement a system of rewards, including appropriate incentive pay and retention incentives, for members of the Armed Forces and civilian employees of the Department of Defense who perform successfully on specific language coding proficiency and artificial intelligence competency tests and make their skills available to the Department.

(b) INFORMATION SHARING WITH OTHER FEDERAL AGENCIES.— Determination.
The Secretary of Defense shall share information on the activities carried out under subsection (a) with the Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the heads of such other organizations of the intelligence community as the Secretary determines appropriate, for purposes of—

(1) making information about the coding language proficiency and artificial intelligence competency tests developed under such subsection available to other Federal national security agencies; and

(2) encouraging the heads of such agencies to implement tracking and reward systems that are comparable to those implemented by the Department of Defense pursuant to such subsection.

(c) SPECIAL PAY FOR PROGRAMMING LANGUAGE PROFICIENCY BENEFICIAL FOR NATIONAL SECURITY INTERESTS.—

(1) IN GENERAL.—Chapter 81 of title 10, United States Code, is amended by inserting after section 1596b the following new section:

"§ 1596c. Programming language proficiency: special pay for proficiency beneficial for national security interests 10 USC 1596c.

"(a) AUTHORITY.—The Secretary of Defense, under the sole and exclusive discretion of the Secretary, may pay special pay under this section to an employee of the Department of Defense who—

"(1) has been certified by the Secretary to be proficient in a computer or digital programming language identified by the Secretary as being a language in which proficiency by civilian personnel of the Department is necessary because of national security interests; and Certification.

"(2) is assigned duties requiring proficiency in that programming language.

"(b) RATE.—The rate of special pay for an employee under this section shall be prescribed by the Secretary, but may not exceed 20 percent of the employee's rate of basic pay.

"(c) RELATIONSHIP TO OTHER PAY AND ALLOWANCES.—Special pay under this section is in addition to any other pay or allowances to which the employee is entitled.

"(d) REGULATIONS.—The Secretary of Defense shall prescribe regulations to carry out this section.".

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 81 of such title is amended by inserting 10 USC 1580 prec.

after the item relating to section 1596b the following new item:

"1596c. Programming language proficiency: special pay for proficiency beneficial for national security interests.".

SEC. 242. MODIFICATION OF SCIENCE, MATHEMATICS, AND RESEARCH FOR TRANSFORMATION (SMART) DEFENSE EDUCATION PROGRAM.

Section 2192a of title 10, United States Code, is amended—

(1) in subsection (c)(1)(B)(i), by inserting ", including by serving on active duty in the Armed Forces" after "Department";

(2) in subsection (d)—

(A) in paragraph (1), by striking "; and" and inserting a semicolon;

(B) in paragraph (2), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new paragraph:

"(3) may establish arrangements so that participants may participate in a paid internship for an appropriate period with an industry sponsor."; and

(3) in subsection (f)—

(A) by inserting "(1)" before "The Secretary"; and

(B) by adding at the end the following new paragraph:

"(2) The Secretary of Defense shall seek to enter into partnerships with minority institutions of higher education and appropriate public and private sector organizations to diversify the participants in the program under subsection (a).".

SEC. 243. IMPROVEMENTS TO TECHNOLOGY AND NATIONAL SECURITY FELLOWSHIP OF DEPARTMENT OF DEFENSE.

(a) MODIFICATION REGARDING BASIC PAY.—Subparagraph (A) of section 235(a)(4) of National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 10 U.S.C. 1580 note prec.) is amended to read as follows:

"(A) shall be compensated at a rate of basic pay that is not less than the minimum rate of basic pay payable for a position at GS–10 of the General Schedule (subchapter III of chapter 53 of title 5, United States Code) and not more than the maximum rate of basic pay payable for a position at GS–15 of such Schedule; and".

(b) BACKGROUND CHECKS.—Subsection (b) of such section is amended by adding at the end the following new paragraph:

"(3) BACKGROUND CHECK REQUIREMENT.—No individual may participate in the fellows program without first undergoing a background check that the Secretary of Defense considers appropriate for participation in the program.".

SEC. 244. MODIFICATION OF MECHANISMS FOR EXPEDITED ACCESS TO TECHNICAL TALENT AND EXPERTISE AT ACADEMIC INSTITUTIONS.

Section 217 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2358 note) is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking "National Defense Authorization Act for Fiscal Year 2020" and inserting "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021"; and

(ii) by striking "not fewer than three" and inserting "not fewer than four";

(B) by redesignating paragraph (2) as paragraph (3);

(C) by inserting after paragraph (1) the following new paragraph:

"(2) COORDINATION.—In carrying out paragraph (1), the Secretary of Defense may act through the Defense Advanced Research Projects Agency or any other organization or element of the Department of Defense the Secretary considers appropriate."; and

(D) in paragraph (3), as so redesignated, by inserting "training," after "management,";

(2) in subsection (e)—

(A) in paragraph (28) by striking "Infrastructure resilience" and inserting "Additive manufacturing";

(B) by redesignating paragraph (30) as paragraph (31); and

(C) by inserting after paragraph (29) the following new paragraph:

"(30) 3D and virtual technology training platforms.";

(3) by redesignating subsections (f) and (g) as subsection (g) and (h), respectively;

(4) by inserting after subsection (e) the following new subsection:

"(f) REQUIREMENT TO ESTABLISH CONSORTIA.—

"(1) IN GENERAL.—In carrying out subsection (a)(1)—

"(A) the Secretary of Defense shall seek to establish at least one multi-institution consortium through the Office of the Secretary of Defense;

"(B) the Secretary of the Army shall seek to establish at least one multi-institution consortium through the Army;

"(C) the Secretary of the Navy shall seek to establish at least one multi-institution consortium through the Navy; and

"(D) the Secretary of the Air Force shall seek to establish at least one multi-institution consortium through the Air Force.

"(2) REPORT REQUIRED.—Not later than September 30, 2022, the Secretary of Defense shall submit to the congressional defense committees a report on the status of the efforts to establish consortia under paragraph (1)."; and

(5) in subsection (g), as so redesignated, by striking "2022" and inserting "2026".

SEC. 245. ENCOURAGEMENT OF CONTRACTOR SCIENCE, TECHNOLOGY, ENGINEERING, AND MATHEMATICS (STEM) PROGRAMS.

10 USC 2191 note prec.

(a) IN GENERAL.—The Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Acquisition and Sustainment, shall develop programs and incentives to ensure that Department of Defense contractors take appropriate steps to—

Coordination.

(1) enhance undergraduate, graduate, and doctoral programs in science, technology, engineering, and mathematics (in this section referred to as "STEM");

(2) make investments, such as programming and curriculum development, in STEM programs within elementary schools and secondary schools;

(3) encourage employees to volunteer in elementary schools and secondary schools, including schools that the Secretary of Defense determines serve high numbers or percentages of students from low-income families or that serve significant populations of military dependents, in order to enhance STEM education and programs;

(4) establish partnerships with appropriate entities, including institutions of higher education for the purpose of training students in technical disciplines;

(5) make personnel available to advise and assist in STEM educational activities aligned with functions of the Department of Defense;

(6) award scholarships and fellowships, and establish work-based learning programs in scientific disciplines;

(7) conduct recruitment activities to enhance the diversity of the STEM workforce; or

(8) make internships available to students of secondary schools, undergraduate, graduate, and doctoral programs in STEM disciplines.

Procedures.

(b) AWARD PROGRAM.—The Secretary of Defense shall establish procedures to recognize defense industry contractors that demonstrate excellence in supporting STEM education, partnerships, programming, and other activities to enhance participation in STEM fields.

Reports.

(c) IMPLEMENTATION.—Not later than 270 days after the date of the enactment of this Act, the Under Secretary of Defense for Research and Engineering shall submit to the congressional defense committees a report on the steps taken to implement the requirements of this section.

(d) DEFINITIONS.—In this section:

(1) The terms "elementary school" and "secondary school" have the meanings given those terms in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(2) The term "institution of higher education" has the meaning given such term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

(e) CONFORMING REPEAL.—Section 862 of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112–81; 10 U.S.C. note prec. 2191) is repealed.

10 USC 2001 note prec.

SEC. 246. TRAINING PROGRAM FOR HUMAN RESOURCES PERSONNEL IN BEST PRACTICES FOR TECHNICAL WORKFORCE.

(a) PILOT TRAINING PROGRAM.—

Deadline.

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense, acting through the Under Secretary of Defense for Personnel and Readiness and the Under Secretary of Defense for Research and Engineering, shall develop and implement a pilot program to provide covered human resources personnel with training in public and private sector best practices for attracting and retaining technical talent.

Procedures.

(2) TRAINING AREAS.—The pilot program shall include training in the authorities and procedures that may be used to recruit technical personnel for positions in the Department of Defense, including—

(A) appropriate direct hiring authorities;

(B) excepted service authorities;

(C) personnel exchange authorities;

(D) authorities for hiring special government employees and highly qualified experts;

(E) special pay authorities; and

(F) private sector best practices to attract and retain technical talent.

(3) METRICS.—The Secretary of Defense shall develop metrics to evaluate the effectiveness of the pilot program in contributing to the ability of the Department of Defense to attract and retain technical talent.

(4) PLAN REQUIRED.—The Secretary of Defense shall develop a plan for the implementation of the pilot program.

(b) REPORTS.—

(1) REPORT ON PLAN.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report that sets forth the plan required under subsection (a)(4).

(2) REPORT ON PILOT PROGRAM.—Not later than three years after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report on the results of the pilot program.

(c) DEFINITIONS.—In this section:

(1) The term "covered human resources personnel" means members of the Armed Forces and civilian employees of the Department of Defense, including human resources professionals, hiring managers, and recruiters, who are responsible for hiring technical talent.

(2) The term "technical talent" means individuals with expertise in high priority technical disciplines.

(d) TERMINATION.—The requirement to carry out the pilot program under this section shall terminate five years after the date of the enactment of this Act.

SEC. 247. PILOT PROGRAM ON THE USE OF ELECTRONIC PORTFOLIOS TO EVALUATE CERTAIN APPLICANTS FOR TECHNICAL POSITIONS.

10 USC 1580 note prec.

(a) PILOT PROGRAM.—Beginning not later than one year after the date of the enactment of this Act, the Secretary of Defense shall carry out a pilot program under which certain applicants for technical positions within the Department of Defense will be evaluated, in part, based on electronic portfolios of the applicant's work, as described in subsection (b).

Deadline.

(b) ACTIVITIES.—Under the pilot program, the human resources manager of each organization of the Department of Defense participating in the program, in consultation with relevant subject matter experts, shall—

Consultation.

(1) identify a subset of technical positions for which the evaluation of electronic portfolios would be appropriate as part of the hiring process; and

(2) as appropriate, assess applicants for such positions by reviewing electronic portfolios of the applicants' best work, as selected by the applicant concerned.

Assessment.

(c) SCOPE OF PROGRAM.—The Secretary of Defense shall carry out the pilot program under subsection (a) in—

(1) the Joint Artificial Intelligence Center;

(2) the Defense Digital Service;

(3) at least one activity of each military department, as identified by the Secretary of the department concerned; and

(4) such other organizations and elements of the Department of Defense as the Secretary determines appropriate.

(d) REPORT.—Not later than two years after the commencement of the pilot program under subsection (a), the Secretary of Defense shall submit to the congressional defense committees a report on the results of the program. At a minimum, the report shall—

(1) describe how the use of electronic portfolios in the hiring process affected the timeliness of the hiring process for technical positions in organizations of the Department of Defense participating in the program;

Assessment.

(2) assess the level of satisfaction of organization leaders, hiring authorities, and subject matter experts with the quality of applicants who were hired based on evaluations of electronic portfolios;

(3) identify other job series that could benefit from the use of electronic portfolios in the hiring process;

Recommendations.

(4) recommend whether the use of electronic portfolios in the hiring process should be expanded or made permanent; and

Recommendations.

(5) recommend any statutory, regulatory, or policy changes required to support the goals of the pilot program under subsection (a).

(e) TECHNICAL POSITION DEFINED.—In this section, the term "technical position" means a position in the Department of Defense that—

(1) requires expertise in artificial intelligence, data science, or software development; and

(2) is eligible for direct hire authority under section 9905 of title 5, United States Code, or section 2358a of title 10, United States Code.

(f) TERMINATION.—The authority to carry out the pilot program under subsection (a) shall terminate 5 years after the date of the enactment of this Act.

10 USC 2001 note prec.

SEC. 248. PILOT PROGRAM ON SELF-DIRECTED TRAINING IN ADVANCED TECHNOLOGIES.

List.

(a) ONLINE COURSES.—The Secretary of Defense shall carry out a pilot program under which the Secretary makes available a list of approved online courses relating to advanced technologies that may be taken by civilian employees of the Department of Defense and members of the Armed Forces on a voluntary basis while not engaged in the performance of their duties.

(b) PROCEDURES.—The Secretary shall establish procedures for the development, selection, approval, adoption, and evaluation of online courses under subsection (a) to ensure that such courses are supportive of the goals of this section and overall goals for the training and education of the civilian and military workforce of the Department of Defense.

(c) DOCUMENTATION OF COMPLETION.—The Secretary of Defense shall develop and implement a system—

(1) to confirm whether a civilian employee of the Department of Defense or member of the Armed Forces has completed an online course approved by the Secretary under subsection (a); and

(2) to document the completion of such course by such employee or member.

(d) INCENTIVES.—The Secretary of Defense shall develop and implement incentives to encourage civilian employees of the Department of Defense and members of the Armed Forces to complete online courses approved by the Secretary under subsection (a).

(e) METRICS.—The Secretary of Defense shall develop metrics to evaluate whether, and to what extent, the pilot program under this section improves the ability of participants—

(1) to perform job-related functions; and

(2) to execute relevant missions of the Department of Defense.

(f) ADVANCED TECHNOLOGIES DEFINED.—In this section, the term "advanced technologies" means technologies that the Secretary of Defense determines to be in high-demand within the Department of Defense and to which significant research and development efforts are devoted, including technologies such as artificial intelligence, data science, machine learning, fifth-generation telecommunications technology, and biotechnology.

(g) DEADLINE.—The Secretary of Defense shall carry out the activities described in subsections (a) through (e) not later than one year after the date of the enactment of this Act.

(h) SUNSET.—This section shall terminate on October 1, 2024.

SEC. 249. PART-TIME AND TERM EMPLOYMENT OF UNIVERSITY FACULTY AND STUDENTS IN THE DEFENSE SCIENCE AND TECHNOLOGY ENTERPRISE.

10 USC 4001 note.

(a) PROGRAM REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall establish a program under which opportunities for part-time and term employment are made available in the Defense science and technology enterprise for faculty and students of institutions of higher education for the purpose of enabling such faculty and students to carry out research projects in accordance with subsection (b).

Deadline.

(b) RESEARCH PROJECTS.—

(1) FACULTY.—A faculty member who is employed in position made available under subsection (a) shall, in the course of such employment, carry out a research project that—

(A) relates to a topic in the field of science, technology, engineering, or mathematics; and

(B) contributes to the objectives of the Department of Defense, as determined by the Secretary of Defense.

(2) STUDENTS.—A student employed in position made available under subsection (a) shall assist a faculty member with a research project described in paragraph (1).

(c) SELECTION OF PARTICIPANTS.—The Secretary of Defense, acting through the heads of participating organizations in the Defense science and technology enterprise, shall select individuals for participation in the program under subsection (a) as follows:

(1) Faculty members shall be selected for participation on the basis of—

(A) the academic credentials and research experience of the faculty member; and

(B) the extent to which the research proposed to be carried out by the faculty member will contribute to the objectives of the Department of Defense.

(2) Students shall be selected to assist with a research project under the program on the basis of—

(A) the academic credentials and other qualifications of the student; and

(B) the student's ability to fulfill the responsibilities assigned to the student as part of the project.

(d) MINIMUM NUMBER OF POSITIONS.—

(1) IN GENERAL.—During the first year of the program under subsection (a), the Secretary of Defense shall establish not fewer than 10 part-time or term positions for faculty.

(2) ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING.—Of the positions established under paragraph (1), not fewer than five such positions shall be reserved for faculty who will conduct research in the area of artificial intelligence and machine learning.

(e) AUTHORITIES.—In carrying out the program under subsection (a), the Secretary of Defense, or the head of an organization in the Defense science and technology enterprise, as applicable, may—

(1) use any hiring authority available to the Secretary or the head of such organization, including—

(A) any hiring authority available under a laboratory demonstration program, including the hiring authority provided under section 2358a of title 10, United States Code;

(B) direct hiring authority under section 1599h of title 10, United States Code; and

(C) expert hiring authority under section 3109 of title 5, United States Code;

Contracts.

(2) enter into cooperative research and development agreements under section 12 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3710a) to enable the sharing of research and expertise with institutions of higher education and the private sector; and

Referral bonuses.

(3) pay referral bonuses to faculty or students participating in the program who identify—

(A) students to assist in a research project under the program; or

(B) students or recent graduates to participate in other programs in the Defense science and technology enterprise, including internships at Department of Defense laboratories and in the Pathways Program of the Department.

(f) ANNUAL REPORTS.—

(1) INITIAL REPORT.—Not later than 30 days after the conclusion of the first year of the program under subsection (a), the Secretary of Defense shall submit to the congressional defense committees a report on the status of the program. The report shall include—

(A) identification of the number of faculty and students employed under the program;

(B) identification of the organizations in the Defense science and technology enterprise that employed such individuals; and

(C) a description of the types of research conducted by such individuals.

(2) SUBSEQUENT REPORTS.—Not later than 30 days after the conclusion of the second and third years of the program under subsection (a), the Secretary of Defense shall submit

Subtitle A—Acquisition Policy and Management

SEC. 801. REPORT ON ACQUISITION RISK ASSESSMENT AND MITIGATION AS PART OF ADAPTIVE ACQUISITION FRAMEWORK IMPLEMENTATION.

(a) IN GENERAL.—Each service acquisition executive shall submit to the Secretary of Defense, the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Research and Engineering, and the Chief Information Officer of the Department of Defense a report on how such service acquisition executive is, with respect to the risks in acquisition programs described in subsection (b)—

(1) assessing such risks;

(2) mitigating such risks; and

(3) reporting within the Department of Defense and to Congress on such risks.

(b) ACQUISITION PROGRAM RISKS.—The risks in acquisition programs described in this subsection are the following:

(1) Technical risks in engineering, software, manufacturing and testing.

(2) Integration and interoperability risks, including complications related to systems working across multiple domains while using machine learning and artificial intelligence capabilities to continuously change and optimize system performance.

(3) Operations and sustainment risks, including as mitigated by appropriate sustainment planning earlier in the lifecycle of a program, access to technical data, and intellectual property rights.

(4) Workforce and training risks, including consideration of the role of contractors as part of the total workforce.

(5) Supply chain risks, including cybersecurity, foreign control and ownership of key elements of supply chains, and the consequences that a fragile and weakening defense industrial base, combined with barriers to industrial cooperation with allies and partners, pose for delivering systems and technologies in a trusted and assured manner.

(c) REPORT TO CONGRESS.—Not later than March 31, 2021, the Under Secretary of Defense for Acquisition and Sustainment shall submit to the congressional defense committees a report including—

(1) the input received from the service acquisition executives pursuant to subsection (a); and

(2) the views of the Under Secretary with respect to the matters described in paragraphs (1) through (5) of subsection (b).

SEC. 802. IMPROVING PLANNING, EXECUTION, AND OVERSIGHT OF LIFE CYCLE SUSTAINMENT ACTIVITIES.

(a) PLANNING FOR LIFE CYCLE SUSTAINMENT.—Section 2337 of title 10, United States Code, is amended—

(1) by striking "major weapon system" each place it appears and inserting "covered system";

(2) by striking "major weapon systems" each place it appears and inserting "covered systems";

(3) by striking "weapon system" each place it appears and inserting "covered system";

(4) by redesignating subsections (b) and (c) as subsections (c) and (d), respectively;

(5) by inserting after subsection (a) the following new subsection:

"(b) LIFE CYCLE SUSTAINMENT PLAN.—Before granting Milestone B approval (or the equivalent), the milestone decision authority shall ensure that each covered system has an approved life cycle sustainment plan. The life cycle sustainment plan shall include—

"(1) a comprehensive product support strategy; Strategy.

"(2) performance goals, including key performance parameters for sustainment, key system attributes of the covered system, and other appropriate metrics;

"(3) an approved life-cycle cost estimate for the covered system; Cost estimate.

"(4) affordability constraints and key cost factors that could affect the operating and support costs of the covered system;

"(5) sustainment risks and proposed mitigation plans for such risks;

"(6) engineering and design considerations that support cost-effective sustainment of the covered system;

"(7) a technical data and intellectual property management plan for product support; and Data.

"(8) major maintenance and overhaul requirements that will be required during the life cycle of the covered system."; Requirements.

(6) in subsection (c)(2), as so redesignated—

(A) by amending subparagraph (A) to read as follows:

"(A) develop, update, and implement a life cycle sustainment plan described in subsection (b);";

(B) in subparagraph (B), by striking "use" and inserting "ensure the life cycle sustainment plan is informed by"; and

(C) in subparagraph (C), by inserting "and life cycle sustainment plan" after "product support strategy";"; and

(7) in subsection (d), as so redesignated—

(A) by amending paragraph (5) to read as follows:

"(5) COVERED SYSTEM.—The term 'covered system' means— Definition.

"(A) a major defense acquisition program as defined in section 2430 of this title; or

"(B) an acquisition program or project that is carried out using the rapid fielding or rapid prototyping acquisition pathway under section 804 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 10 U.S.C. 2302 note) that is estimated by the Secretary of Defense to require an eventual total expenditure described in section 2430(a)(1)(B)."; and

(B) by adding at the end the following new paragraphs: Definitions.

"(6) MILESTONE B APPROVAL.—The term 'Milestone B approval' has the meaning given that term in section 2366(e)(7) of this title.

"(7) MILESTONE DECISION AUTHORITY.—The term 'milestone decision authority' has the meaning given in section 2431a(e)(5) of this title.".

(b) ADDITIONAL REQUIREMENTS BEFORE MILESTONE B APPROVAL.—Section 2366b of title 10, United States Code is amended—

(1) in subsection (a)(3)—

(A) in subparagraph (N), by striking "and" at the end;

(B) in subparagraph (O), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new subparagraph:

"(P) has approved the life cycle sustainment plan required under section 2337(b) of this title."; and

(2) in subsection (c)(1)—

(A) by redesignating subparagraph (H) as subparagraph (I); and

(B) by inserting after subparagraph (G) the following new subparagraph:

"(H) A summary of the life cycle sustainment plan required under section 2337 of this title.".

(c) RECURRING SUSTAINMENT REVIEWS.—Section 2441 of title 10, United States Code, is amended—

(1) in subsection (a)—

(A) in the first sentence—

(i) by striking "major weapon system" and inserting "covered system";

(ii) by striking "and throughout the life cycle of the weapon system" and inserting ", and every five years thereafter throughout the life cycle of the covered system,"; and

(iii) by striking "costs of the weapon system" and inserting "costs of the covered system"; and

(B) by striking the second sentence;

(2) in subsection (b)—

(A) in the matter preceding paragraph (1), by inserting "assess execution of the life cycle sustainment plan of the covered system and" before "include the following elements:"; and

(B) by adding at the end the following new paragraph:

"(10) As applicable, information regarding any decision to restructure the life cycle sustainment plan for a covered system or any other action that will lead to critical operating and support cost growth."; and

(3) by adding at the end the following new subsections:

Deadlines. Reviews.

"(d) SUBMISSION TO CONGRESS.—(1) Not later than September 30 of each fiscal year, the Secretary of each military department shall annually submit to the congressional defense committees the sustainment reviews required by this section for such fiscal year.

Classified information.

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

Remediation plan. Certification.

"(3) For a covered system with critical operating and support cost growth, such submission shall include a remediation plan to

reduce operating and support costs or a certification by the Secretary concerned that such critical operating and support cost growth is necessary to meet national security requirements.

"(e) DEFINITIONS.—In this section:

"(1) COVERED SYSTEM.—The term 'covered system' shall have the meaning given in section 2337 of this title.

"(2) CRITICAL OPERATING AND SUPPORT COST GROWTH.—The term 'critical operating and support cost growth' means operating and support cost growth—

"(A) of at least 25 percent more than the estimate documented in the most recent independent cost estimate for the covered system; or

"(B) of at least 50 percent more than the estimate documented in the original Baseline Estimate (as defined in section 2435(d) of this title) for the covered system.".

(d) COMPTROLLER GENERAL REVIEW.—

(1) IN GENERAL.—The Comptroller General of the United States shall—

(A) annually, select 10 covered systems for which a sustainment review has been submitted under section 2441(d) of title 10, United States Code; and

(B) submit to the congressional defense committees an assessment of the steps taken by Secretaries concerned to quantify and address critical operating and support cost growth with respect to such covered systems. Assessments.

(2) CONTENTS.—Each assessment described in paragraph (1) shall include—

(A) an evaluation of— Evaluations.

(i) the causes of critical operating and support cost growth for each such covered system;

(ii) the extent to which the Secretary concerned has mitigated critical operating and support cost growth of such covered system; and

(iii) any other issues related to potential critical operating and support cost growth the Comptroller General determines appropriate; and

(B) any recommendations, including steps the Secretaries concerned could take to reduce critical operating and support cost growth for covered systems and lessons learned to be incorporated in covered system acquisitions. Recommendations.

(3) TERMINATION.—The requirement under this subsection shall terminate on September 30, 2025.

(4) DEFINITIONS.—In this subsection, the terms "covered system" and "critical operating and support cost growth" have the meanings given, respectively, in section 2441 of title 10, United States Code.

(e) REPORT ON SUSTAINMENT PLANNING PROCESSES FOR NON-MAJOR DEFENSE ACQUISITION PROGRAM ACTIVITIES.—Not later than December 31, 2021, the Secretary of Defense shall submit to the congressional defense committees a report on the process for ensuring that timely and robust sustainment planning processes are in place for all acquisition activities. The report shall include a discussion of—

(1) sustainment planning processes for each—

(A) acquisition program or project that is carried out using the rapid fielding or rapid prototyping acquisition pathway under section 804 of the National Defense

Authorization Act for Fiscal Year 2016 (Public Law 114–92; 10 U.S.C. 2302 note);

(B) information technology and software program;

(C) services contract, including each services contract for information technologies and systems; and

(D) acquisition activity other than major defense acquisition programs (as defined in section 2430 of title 10, United States Code), as determined by the Secretary of Defense;

(2) methods to identify responsible individuals for sustainment planning;

Requirements.

(3) required elements of sustainment planning;

(4) timing of sustainment planning activities in the acquisition process;

Assessment. Compliance.

(5) measures and metrics to assess compliance with sustainment plans; and

(6) actions to continuously monitor, create incentives for, and ensure compliance with sustainment plans.

SEC. 803. DISCLOSURES FOR OFFERORS FOR CERTAIN SHIPBUILDING MAJOR DEFENSE ACQUISITION PROGRAM CONTRACTS.

(a) IN GENERAL.—Chapter 137 of title 10, United States Code, is amended by adding at the end the following new section:

10 USC 2339c.

"§ 2339c. Disclosures for offerors for certain shipbuilding major defense acquisition program contracts

Proposal.

"(a) IN GENERAL.—Any covered offeror seeking to be awarded a shipbuilding construction contract as part of a major defense acquisition program with funds from the Shipbuilding and Conversion, Navy account shall disclose along with the offer and any subsequent revisions of the offer (including the final proposal revision offer) if any part of the planned contract performance will or is expected to include foreign government subsidized performance, foreign financing, foreign financial guarantees, or foreign tax concessions.

"(b) REQUIREMENTS.—A disclosure required under subsection (a) shall be made in a form prescribed by the Secretary of the Navy and shall include a specific description of the extent to which the planned contract performance will include, with or without contingencies, any foreign government subsidized performance, foreign financing, foreign financial guarantees, or foreign tax concessions.

Deadline.

"(c) CONGRESSIONAL NOTIFICATION.—Not later than 5 days after awarding a contract described under subsection (a), the Secretary of the Navy shall notify the congressional defense committees and summarize the disclosure provided under such subsection.

"(d) DEFINITIONS.—In this section:

"(1) COVERED OFFEROR.—The term 'covered offeror' means any offeror that requires or may reasonably be expected to require, during the period of performance on a shipbuilding construction contract described in subsection (a), a method to mitigate or negate foreign ownership under section 2004.34(f)(6) of title 32, Code of Federal Regulations.

"(2) FOREIGN GOVERNMENT SUBSIDIZED PERFORMANCE.—The term 'foreign government subsidized performance' means any financial support, materiel, services, or guarantees of support,

services, supply, performance, or intellectual property concessions, that may be provided to or for the covered offeror or the customer of the offeror by a foreign government or entity effectively owned or controlled by a foreign government, which may have the effect of supplementing, supplying, servicing, or reducing the cost or price of an end item, or supporting, financing in whole or in part, or guaranteeing contract performance by the offeror.

"(3) MAJOR DEFENSE ACQUISITION PROGRAM.—The term 'major defense acquisition program' has the meaning given the term in section 2430 of this title.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 137 of title 10, United States Code, is amended by inserting after the item relating to section 2339b the following new item: 10 USC 2301 prec.

"2339c. Disclosures for offerors for certain shipbuilding major defense acquisition program contracts.".

SEC. 804. IMPLEMENTATION OF MODULAR OPEN SYSTEMS APPROACHES. 10 USC 4401 note.

(a) REQUIREMENTS FOR INTERFACE DELIVERY.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the Joint All-Domain Command and Control cross-functional team and the Director for Command, Control, Communications, and Computers/Cyber, shall issue regulations and guidance applicable to the military departments, Defense Agencies, Department of Defense Field Activities (as such terms are defined, respectively, in section 101 of title 10, United States Code), and combatant commands, as appropriate, to— Deadline. Coordination. Regulations. Applicability.

(A) facilitate the Department of Defense's access to and utilization of modular system interfaces;

(B) fully realize the intent of chapter 144B of title 10, United States Code, by facilitating the implementation of modular open system approaches across major defense acquisition programs (as defined in section 2430 of title 10, United States Code) and other relevant acquisition programs, including in the acquisition and sustainment of weapon systems, platforms, and components for which no common interface standard has been established, to enable communication between such weapon systems, platforms, and components; and

(C) advance the efforts of the Department to generate diverse and recomposable kill chains.

(2) ELEMENTS.—The regulations and guidance required under paragraph (1) shall include requirements that—

(A) the program officer for each weapon system characterizes, in the acquisition strategy required under section 2431a of title 10, United States Code or in other documentation, the desired modularity of the weapon system for which the program officer is responsible, including—

(i) identification of—

(I) the modular systems that comprise the weapon system;

(II) the information that should be communicated between individual modular systems (such as tracking and targeting data or command and control instructions); and

(III) the desired function of the communication between modular systems (such as fire control functions); and

(ii) a default configuration specifying which modular systems should communicate with other modular systems, including modular systems of other weapon systems;

(B) each relevant Department of Defense contract entered into after the date on which the regulations and guidance required under paragraph (1) are implemented includes requirements for the delivery of modular system interfaces for modular systems deemed relevant in the acquisition strategy or documentation referred to in subparagraph (A), including—

(i) software-defined interface syntax and properties, specifically governing how values are validly passed and received between major subsystems and components, in machine-readable format;

(ii) a machine-readable definition of the relationship between the delivered interface and existing common standards or interfaces available in the interface repositories established pursuant to subsection (c); and

(iii) documentation with functional descriptions of software-defined interfaces, conveying semantic meaning of interface elements, such as the function of a given interface field;

(C) the relevant program offices, including those responsible for maintaining and upgrading legacy systems—

(i) that have not characterized the desired modularity of the systems nevertheless meet the requirements of paragraph (2)(A), if the program officers make an effort, to the extent practicable, to update the acquisition strategies required under section 2431a of title 10, United States Code, or to develop or update other relevant documentation; and

(ii) that have awarded contracts that do not include the requirements specified in subparagraph (B) of paragraph (2) nevertheless acquire, to the extent practicable, the items specified in clauses (i) through (iii) of such subparagraph, either through contractual updates, separate negotiations or contracts, or program management mechanisms; and

(D) the relevant program officers deliver modular system interfaces and the associated documentation to at least one of the repositories established pursuant to subsection (c).

(3) APPLICABILITY OF REGULATIONS AND GUIDANCE.—

(A) APPLICABILITY.—The regulations and guidance required under paragraph (1) shall apply to any program office responsible for the prototyping, acquisition, or sustainment of a new or existing weapon system.

(B) EXTENSION OF SCOPE.—Not earlier than 1 year before, and not later than 2 years after the regulations and guidance required under paragraph (1) are issued for weapon systems, the Under Secretary of Defense for Acquisition and Sustainment may extend such regulations and guidance to apply to software-based non-weapon systems, including business systems and cybersecurity systems. Time period.

(4) INCLUSION OF COMPONENTS.—For the purposes of paragraph (2)(A), each component that meets the following requirements shall be treated as a modular system:

(A) A component that is able to execute without requiring coincident execution of other weapon systems or components and can communicate across component boundaries and through interfaces.

(B) A component that can be separated from and recombined with other weapon systems or components to achieve various effects, missions, or capabilities.

(C) A component that is covered by a unique contract line item.

(5) MACHINE-READABLE DEFINITION.—Where appropriate and available, the requirement in paragraph (2)(B)(ii) for a machine-readable definition may be satisfied by using a covered technology.

(b) EXTENSION OF MODULAR OPEN SYSTEMS APPROACH AND RIGHTS IN INTERFACE SOFTWARE.—

(1) REQUIREMENT FOR MODULAR OPEN SYSTEM APPROACH.—Section 2446a of title 10, United States Code, is amended—

(A) in subsection (a), by adding at the end the following: "Other defense acquisition programs shall also be designed and developed, to the maximum extent practicable, with a modular open system approach to enable incremental development and enhance competition, innovation, and interoperability.";

(B) in subsection (b)—

(i) in paragraph (1)—

(I) in subparagraph (A), by striking "major system interfaces" and all that follows and inserting "modular system interfaces between major systems, major system components and modular systems;";

(II) in subparagraph (B), by striking "major system interfaces" and all that follows and inserting the following: "that relevant modular system interfaces—

"(i) comply with, if available and suitable, widely supported and consensus-based standards; or

"(ii) are delivered pursuant to the requirements established in subsection (a)(2)(B) of section 804 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, including the delivery of—

"(I) software-defined interface syntax and properties, specifically governing how values are validly passed and received between major subsystems and components, in machine-readable format;

"(II) a machine-readable definition of the relationship between the delivered interface and existing common standards or interfaces available in Department interface repositories; and

"(III) documentation with functional descriptions of software-defined interfaces, conveying semantic meaning of interface elements, such as the function of a given interface field;"; and

(III) in subparagraph (C), by inserting "and modular systems" after "severable major system components";

(ii) in paragraph (3)(A), by striking "well-defined major system interfaces" and inserting "modular system interfaces";

Definitions.

(iii) by amending paragraph (4) to read as follows:

"(4) The term 'modular system interface' means a shared boundary between major systems, major system components, or modular systems, defined by various physical, logical, and functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software elements.";

(iv) by redesignating paragraphs (5) through (8) as paragraphs (6) through (9), respectively; and

(v) by inserting after paragraph (4) the following new paragraph:

"(5) The term 'modular system' refers to a weapon system or weapon system component that—

"(A) is able to execute without requiring coincident execution of other specific weapon systems or components;

"(B) can communicate across component boundaries and through interfaces; and

"(C) functions as a module that can be separated, recombined, and connected with other weapon systems or weapon system components in order to achieve various effects, missions, or capabilities.".

(2) RIGHTS IN TECHNICAL DATA.—

(A) IN GENERAL.—Section 2320 of title 10, United States Code, is amended—

(i) in subsection (a)(2), by amending subparagraph (G) to read as follows:

Determination.

"(G) MODULAR SYSTEM INTERFACES DEVELOPED EXCLUSIVELY AT PRIVATE EXPENSE OR WITH MIXED FUNDING.—Notwithstanding subparagraphs (B) and (E), the United States shall have government purpose rights in technical data pertaining to a modular system interface developed exclusively at private expense or in part with Federal funds and in part at private expense and used in a modular open system approach pursuant to section 2446a of this title, except in any case in which the Secretary of Defense determines that negotiation of different rights in such technical data would be in the best interest of the United States. Such modular system interface shall be identified in the contract solicitation and the contract. For technical data pertaining to a modular system interface developed exclusively at private expense for which the United States asserts government purpose rights, the Secretary of Defense shall negotiate with the contractor the appropriate and reasonable compensation for such technical data."; and

(ii) in subsection (h), by striking ", 'major system interface'" and inserting ", 'modular system interface'".

(B) REGULATIONS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall update the regulations required by section 2320(a)(1) of title 10, United States Code, to reflect the amendments made by this paragraph. Deadline. Update.

(c) INTERFACE REPOSITORIES.—

(1) ESTABLISHMENT.—Not later than 90 days after the date of the enactment of this Act, the Under Secretary of Defense for Acquisition and Sustainment shall— Deadline.

(A) direct the Secretaries concerned and the heads of other appropriate Department of Defense components to establish and maintain repositories for interfaces, syntax and properties, documentation, and communication implementations delivered pursuant to the requirements established under subsection (a)(2)(B);

(B) establish and maintain a comprehensive index of interfaces, syntax and properties, documentation, and communication implementations delivered pursuant to the requirements established under subsection (a)(2)(B) and maintained in the repositories required under subparagraph (A); and

(C) if practicable, establish and maintain an alternate reference repository of interfaces, syntax and properties, documentation, and communication implementations delivered pursuant to the requirements established under subsection (a)(2)(B).

(2) DISTRIBUTION OF INTERFACES.—

(A) IN GENERAL.—Consistent with the requirements of section 2320 of title 10, United States Code, the Under Secretary of Defense for Acquisition and Sustainment shall, in coordination with the Director of the Defense Standardization Program Office, use the index and repositories established pursuant to paragraph (1) to provide access to interfaces and relevant documentation to authorized Federal Government and non-Governmental entities. Coordination.

(B) NON-GOVERNMENT RECIPIENT USE LIMITS.—A non-Governmental entity that receives access under subparagraph (A) may not further release, disclose, or use such data except as authorized.

(d) SYSTEM OF SYSTEMS INTEGRATION TECHNOLOGY AND EXPERIMENTATION.—

(1) DEMONSTRATION AND ASSESSMENT.—

(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director for Command, Control, Communications, and Computers/Cyber and the Chief Information Officer of the Department of Defense, acting through the Joint All-Domain Command and Control cross-functional team, shall conduct demonstrations and complete an assessment of the technologies developed under the System of Systems Integration Technology and Experimentation program of the Defense Advanced Research Projects Agency, including a covered technology, and the applicability of any such technologies to the Joint All-Domain Command and Control architecture. Deadline.

(B) COVERAGE.—The demonstrations and assessment required under subparagraph (A) shall include—

(i) at least three demonstrations of the use of a covered technology to create, under constrained schedules and budgets, novel kill chains involving previously incompatible weapon systems, sensors, and command, control, and communication systems from multiple military services in cooperation with United States Indo-Pacific Command or United States European Command;

Evaluation.

(ii) an evaluation as to whether the communications enabled via a covered technology are sufficient for military missions and whether such technology results in any substantial performance loss in communication between systems, major subsystems, and major components;

Evaluation.

(iii) an evaluation as to whether a covered technology obviates the need to develop, impose, and maintain strict adherence to common communication and interface standards for weapon systems;

(iv) the appropriate roles and responsibilities of the Chief Information Officer of the Department of Defense, the Under Secretary of Defense for Acquisition and Sustainment, the heads of the combatant commands, the Secretaries concerned, the Defense Advanced Research Projects Agency, and the defense industrial base in using and maintaining a covered technology to generate diverse and recomposable kill chains as part of the Joint All-Domain Command and Control architecture;

(v) for at least one of the demonstrations conducted under clause (i), demonstration of the use of technology developed under the High-Assurance Cyber Military Systems program of the Defense Advanced Research Projects Agency to secure legacy weapon systems and command and control capabilities while facilitating interoperability;

Evaluation.

(vi) an evaluation of how the technology referred to in clause (v) and covered technology should be used to improve cybersecurity and interoperability across critical weapon systems and command and control capabilities across the joint forces; and

Coordination.

(vii) coordination with the program manager for the Time Sensitive Targeting Defeat program under the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Intelligence and Security.

(2) CHIEF INFORMATION OFFICER ASSESSMENT.—

Coordination.

(A) IN GENERAL.—The Chief Information Officer for the Department of Defense, in coordination with the Principal Cyber Advisor to the Secretary of Defense and the Director of the Cybersecurity Directorate of the National Security Agency, shall assess the technologies developed under the System of Systems Integration Technology and Experimentation program of the Defense Advanced Research Projects Agency, including the covered technology,

and applicability of such technology to the business systems and cybersecurity tools of the Department.

(B) COVERAGE.—The assessment required under subparagraph (A) shall include— Demonstrations.

(i) an evaluation as to how the technologies referred to in such subparagraph could be used in conjunction with or instead of existing cybersecurity standards, frameworks, and technologies designed to enable communication between, and coordination of, cybersecurity tools; Evaluations.

(ii) as appropriate, demonstrations by the Chief Information Office of the use of such technologies in enabling communication between, and coordination of, previously incompatible cybersecurity tools; and Coordination.

(iii) as appropriate, demonstrations of the use of such technologies in enabling communication between previously incompatible business systems.

(3) SUSTAINMENT OF CERTAIN ENGINEERING RESOURCES AND CAPABILITIES.—During the period the demonstrations and assessments required under this subsection are conducted, and thereafter to the extent required to execute the activities directed by the Joint All-Domain Command and Control cross-functional team, the Joint All-Domain Command and Control cross-functional team shall sustain the System of Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems engineering resources and capabilities developed by the Defense Advanced Research Projects Agency.

(4) TRANSFER OF RESPONSIBILITY.—Not earlier than 1 year before, and not later than 2 years after the date of the enactment of this Act, the Secretary of Defense may transfer responsibility for maintaining the engineering resources and capabilities described in paragraph (3) to a different organization within the Department. Time period.

(e) OPEN STANDARDS.—Nothing in this section shall be construed as requiring, preventing, or interfering with the use or application of any given communication standard or interface. The communication described in subsection (a)(2)(A) may be accomplished by using existing open standards, by the creation and use of new open standards, or through other approaches, provided that such standards meet the requirements of subsection (a)(2)(B).

(f) DEFINITIONS.—In this section:

(1) The term "covered technology" means the domain-specific programming language for interface field transformations and its associated compilation toolchain (commonly known as the "System of Systems Technology Integration ToolChain for Heterogeneous Electronic Systems") developed under the Defense Advanced Research Projects Agency System of Systems Integration Technology and Experimentation program, or any other technology that is functionally equivalent.

(2) The term "desired modularity" means the desired degree to which weapon systems, components within a weapon system, and components across weapon systems can function as modules that can communicate across component boundaries and through interfaces and can be separated and recombined to achieve various effects, missions, or capabilities, as determined by the program officer for such weapon system.

(3) The term "machine-readable format" means a format that can be easily processed by a computer without human intervention.

(4) The terms "major system", "major system component", "modular open system approach", "modular system", "modular system interface", and "weapon system" have the meanings given such terms, respectively, in section 2446a of title 10, United States Code.

SEC. 805. CONGRESSIONAL NOTIFICATION OF TERMINATION OF A MIDDLE TIER ACQUISITION PROGRAM.

Section 804 of the National Defense Authorization Act for Fiscal Year 2016 (10 U.S.C. 2302 note) is amended by adding at the end the following new subsection:

"(e) REPORT.—Not later than 30 days after the date of termination of an acquisition program commenced using the authority under this section, the Secretary of Defense shall submit to Congress a notification of such termination. Such notice shall include—

"(1) the initial amount of a contract awarded under such acquisition program;

"(2) the aggregate amount of funds awarded under such contract; and

"(3) written documentation of the reason for termination of such acquisition program.".

SEC. 806. DEFINITION OF MATERIAL WEAKNESS FOR CONTRACTOR BUSINESS SYSTEMS.

Section 893 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 10 U.S.C. 2302 note) is amended—

(1) by striking "significant deficiencies" both places it appears and inserting "material weaknesses";

(2) by striking "significant deficiency" each place it appears and inserting "material weakness"; and

(3) by amending subsection (g)(4) to read as follows:

"(4) The term 'material weakness' means a deficiency or combination of deficiencies in the internal control over information in contractor business systems, such that there is a reasonable possibility that a material misstatement of such information will not be prevented, or detected and corrected, on a timely basis. For purposes of this paragraph, a reasonable possibility exists when the likelihood of an event occurring—

"(A) is probable; or

"(B) is more than remote but less than likely.".

10 USC 9081 note.

SEC. 807. SPACE SYSTEM ACQUISITION AND THE ADAPTIVE ACQUISITION FRAMEWORK.

(a) SERVICE ACQUISITION EXECUTIVE FOR SPACE SYSTEMS AND PROGRAMS.—Before implementing the application of the adaptive acquisition framework to a Space Systems Acquisition pathway described in subsection (c), there shall be within the Department of the Air Force an individual serving as the Service Acquisition Executive of the Department of the Air Force for Space Systems and Programs as required under section 957 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1566; 10 U.S.C. 9016 note).

(b) MILESTONE DECISION AUTHORITY FOR UNITED STATES SPACE FORCE.—

(1) PROGRAM EXECUTIVE OFFICER.—The Service Acquisition Executive for Space Systems and Programs of the United States Space Force may further delegate authority to an appropriate program executive officer to serve as the milestone decision authority for major defense acquisition programs of the United States Space Force.

(2) PROGRAM MANAGER.—The program executive officer assigned under paragraph (1) may further delegate authority over major systems to an appropriate program manager.

(c) ADAPTIVE ACQUISITION FRAMEWORK APPLICATION TO SPACE ACQUISITION.—

(1) IN GENERAL.—The Secretary of Defense shall take such actions necessary to ensure the adaptive acquisition framework (as described in Department of Defense Instruction 5000.02, "Operation of the Adaptive Acquisition Framework") includes one or more pathways specifically tailored for Space Systems Acquisition in order to achieve faster acquisition, improve synchronization and more rapid fielding of critical end-to-end capabilities (including by using new commercial capabilities and services), while maintaining accountability for effective programs that are delivered on time and on budget.

(2) GOAL.—The goal of the application of the adaptive acquisition framework to a Space Systems Acquisition pathway shall be to quickly and effectively acquire end-to-end space warfighting capabilities needed to address the requirements of the national defense strategy (as defined under section 113(g) of title 10, United States Code).

(d) REPORT.—

(1) IN GENERAL.—Not later than May 15, 2021, the Secretary of Defense shall submit to the congressional defense committees a report on the application of the adaptive acquisition framework to any Space Systems Acquisition pathway established under subsection (a) that includes the following:

(A) Proposed United States Space Force budget line items for fiscal year 2022, including— Proposals.

(i) a comparison with budget line items for any major defense acquisition programs, middle tier acquisition programs, covered software programs, and major systems of the United States Space Force for three previous fiscal years;

(ii) existing and recommended measures to ensure sufficient transparency and accountability related to the performance of the Space Systems Acquisition pathway; and Recommendations.

(iii) proposed mechanisms to enable insight into the funding prioritization process and significant funding changes, including the independent cost estimate basis and full funding considerations for any major defense acquisition programs, middle tier acquisition programs, covered software programs, and major systems procured by the United States Space Force.

(B) Proposed revised, flexible, and streamlined options for joint requirements validation in order to be more responsive and innovative, while ensuring the ability of Proposals.

the Joint Chiefs of Staff to ensure top-level system requirements are properly prioritized to address joint-warfighting needs.

List. (C) A list of acquisition programs of the United States Space Force for which multiyear contracting authority under sections 2306b or 2306c of title 10, United States Code, is recommended.

List. (D) A list of space systems acquisition programs for which alternative acquisition pathways may be used.

Procedures. (E) Policies or procedures for potential new pathways in the application of the adaptive acquisition framework to a Space Systems Acquisition with specific acquisition key decision points and reporting requirements for development, fielding, and sustainment activities that meet the requirements of the adaptive acquisition framework.

Analysis. (F) An analysis of the need for updated determination authority for procurement of useable end items that are not weapon systems.

(G) Policies and a governance structure, for both the Office of the Secretary of Defense and each military department, for a separate United States Space Force budget topline, corporate process, and portfolio management process.

Analysis. (H) An analysis of the risks and benefits of the delegation of the authority of the head of contracting activity authority to the Chief of Space Operations in a manner that would not expand the operations of the United States Space Force.

Deadline. Analysis. Recommendations. (2) COMPTROLLER GENERAL REVIEW.—Not later than 60 days after the submission of the report required under paragraph (1), the Comptroller General of the United States shall review such report and submit to the congressional defense committees an analysis and recommendations based on such report.

(e) DEFINITIONS.—In this section:

(1) COVERED SOFTWARE PROGRAM.—The term "covered software program" means an acquisition program or project that is carried out using the software acquisition pathway established under section 800 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1478; 10 U.S.C. 2223a note).

(2) MAJOR DEFENSE ACQUISITION PROGRAM.—The term "major defense acquisition program" has the meaning given in section 2430 of title 10, United States Code.

(3) MAJOR SYSTEM.—The term "major system" has the meaning given in section 2302 of title 10, United States Code.

(4) MIDDLE TIER ACQUISITION PROGRAM.—The term "middle tier acquisition program" means an acquisition program or project that is carried out using the rapid fielding or rapid prototyping acquisition pathway under section 804 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 10 U.S.C. 2302 note).

(5) MILESTONE DECISION AUTHORITY.—The term "milestone decision authority" has the meaning given in section 2431a of title 10, United States Code.

(6) PROGRAM EXECUTIVE OFFICER; PROGRAM MANAGER.—The terms "program executive officer" and "program manager" have

the meanings given those terms, respectively, in section 1737 of title 10, United States Code.

SEC. 808. ACQUISITION AUTHORITY OF THE DIRECTOR OF THE JOINT ARTIFICIAL INTELLIGENCE CENTER.

10 USC 4001 note.

(a) AUTHORITY.—The Secretary of Defense shall delegate to the Director of the Joint Artificial Intelligence Center the acquisition authority to exercise the functions of a head of an agency (as defined in section 2302 of title 10, United States Code) with respect to appropriate acquisition activities of the Center.

(b) JAIC ACQUISITION EXECUTIVE.—

(1) IN GENERAL.—The staff of the Director shall include an acquisition executive who shall be responsible for the supervision of appropriate acquisition activities under subsection (a). Subject to the authority, direction, and control of the Director of the Center, the acquisition executive shall have the authority—

(A) to negotiate memoranda of agreement with any element of the Department of Defense to carry out the acquisition of technologies, services, and capabilities developed or identified by the Center; Memorandum.

(B) to supervise the acquisition of technologies, services, and capabilities to support the mission of the Center;

(C) to represent the Center in discussions with the Secretaries concerned regarding acquisition programs relating to such appropriate acquisition activities for which the Center is involved; and

(D) to work with the Secretaries concerned to ensure that the Center is appropriately represented in any joint working group or integrated product team regarding acquisition programs relating to such appropriate activities for which the Center is involved.

(2) DELIVERY OF ACQUISITION SOLUTIONS.—The acquisition executive of the Center shall be—

(A) responsible to the Director for rapidly delivering capabilities to meet validated requirements;

(B) subordinate to the Under Secretary of Defense for Acquisition and Sustainment in matters of acquisition; and

(C) included on the distribution list for acquisition directives and instructions of the Department of Defense.

(c) ACQUISITION PERSONNEL.—

(1) IN GENERAL.—The Secretary of Defense shall provide the Center with at least 10 full-time employees to support the Director in carrying out the requirements of this section, including personnel with experience in—

(A) acquisition practices and processes;

(B) the Joint Capabilities Integration and Development System process;

(C) program management;

(D) software development and systems engineering; and

(E) cost analysis.

(2) EXISTING PERSONNEL.—The personnel provided under this subsection shall be provided from among the existing personnel of the Department of Defense.

(d) FUNDING.—In exercising the acquisition authority granted in subsection (a), the Director may not obligate or expend more than $75,000,000 out of the funds made available in each of fiscal years 2021, 2022, 2023, 2024, and 2025 to enter into new contracts to support appropriate acquisition activities carried out under this section.

(e) IMPLEMENTATION PLAN AND DEMONSTRATION REQUIRED.—

(1) IN GENERAL.—The Secretary of Defense—

Time period.

(A) may use the acquisition authority granted under subsection (a) on or after 30 days after the date on which the Secretary provides to the congressional defense committees a plan for implementation of such authority; and

Deadline.

(B) by March 15, 2022, shall provide a demonstration of operational capability delivered under such authority.

(2) IMPLEMENTATION PLAN.—The plan shall include the following:

(A) Description of the types of activities to be undertaken using the acquisition authority provided under subsection (a).

(B) Plan for the negotiation and approval of any such memorandum of agreement with an element of the Department of Defense to support Center missions and transition of artificial intelligence capabilities into appropriate acquisition programs or into operational use.

(C) Plan for oversight of the position of acquisition executive established in subsection (b).

Assessment.

(D) Assessment of the acquisition workforce, tools, and infrastructure needs of the Center to support the authority under subsection (a) until September 30, 2025.

(E) Other matters as appropriate.

(3) DEMONSTRATION.—The capability demonstration shall include a description of how the acquisition authority enabled the capability, how requirements were established and agreed upon, how testing was conducted, and how the capability was transitioned to the user, as well as any other matters deemed appropriate by the Center.

(4) RELATIONSHIP TO OTHER AUTHORITIES.—The requirement to submit a plan under this subsection is in addition to the requirements under section 260 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1293).

(f) SUNSET.—Effective October 1, 2025, the Director may not exercise the authority under subsection (a) and may not enter into any new contracts under this section. The performance on any contract entered into before such date may continue according to the terms of such contract.

(g) DEFINITIONS.—In this section:

(1) CENTER.—The term "Center" has the meaning given the term "Joint Artificial Intelligence Center" in section 260(c) of National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1294).

(3) DIRECTOR.—The term "Director" means the Director of the Center.

(4) ELEMENT.—The term "element" means an element described under section 111(b) of title 10, United States Code.

(5) SECRETARY CONCERNED.—The term "Secretary concerned" has the meaning given in section 101(9) of title 10, United States Code.

SEC. 809. ASSESSMENTS OF THE PROCESS FOR DEVELOPING CAPABILITY REQUIREMENTS FOR DEPARTMENT OF DEFENSE ACQUISITION PROGRAMS.

(a) IN GENERAL.—The Secretary of Defense and the individual appointed under section 2361a(c) of title 10, United States Code, (in this section referred to as the "Director") shall each—

(1) conduct an assessment of the processes for developing and approving capability requirements for the acquisition programs of the Department of Defense and each military department; and

(2) develop recommendations for reforming such process to improve the agility and timeliness of such process. Recommendations.

(b) ASSESSMENT ELEMENTS.—Each assessment conducted under subsection (a) shall include the following:

(1) An assessment of the—

(A) adherence of the capability requirements development and approval processes to statute, regulations, policies, and directives;

(B) alignment and standardization of the capability requirements development, acquisition, and budget processes;

(C) technical feasibility of each approved capability requirement;

(D) training and development of the workforce in capability requirements development and evaluation;

(E) ability of the process for developing capability requirements to address the urgent needs of the Department of Defense;

(F) capacity to review changes in capability requirements for programs of record;

(G) validation of decisions made to approve capability requirements and the alignment of each such decision to the national defense strategy required under section 113(g) of title 10, United States Code;

(H) extent to which portfolio management techniques are used in the process for developing capability requirements to coordinate decisions and avoid duplication of capabilities across acquisition programs; and

(I) implementation by each military department of Comptroller General of the United States recommendations pertaining to the process for developing and approving capability requirements.

(2) A comprehensive analysis of the circumstances and factors contributing to the length of time between the start of a Capabilities-Based Assessment and the date the Joint Requirements Oversight Council approves the related Capability Development Document. Analysis.

(3) Identification and comparison of best practices in the private sector and the public sector for the development and approval of capability requirements.

(4) Any additional matters that the Secretary or Director determine appropriate.

(c) REPORTS.—

(1) ASSESSMENT BY SECRETARY.—Not later than October 1, 2021, the Secretary of Defense shall submit to the congressional defense committees a report on the assessment conducted by the Secretary under subsection (a), including—

(A) a description of such assessment;

Analysis.

(B) the results of such assessment, including the analysis described in subsection (b)(2);

Plan.

(C) a plan to reduce, when appropriate, the length of time between the start of a Capabilities-Based Assessment and the date the Joint Requirements Oversight Council approves the related Capability Development Document; and

Recommendations.

(D) any additional recommendations for legislation, regulations, or policies that the Secretary determines appropriate.

(2) ASSESSMENT BY DIRECTOR.—

(A) REPORT TO SECRETARY.—Not later than November 30, 2021, the Director shall submit to the Secretary of Defense a report on the assessment conducted by the Director pursuant to subsection (a).

Recommendations.

(B) REPORT TO CONGRESS.—Not later than January 1, 2022, the Secretary of Defense shall submit to the congressional defense committees the report described in subparagraph (A) together with such comments as the Secretary determines appropriate, including—

(i) a description and the results of the assessment conducted pursuant to subsection (a)(2);

(ii) recommendations on how the Department of Defense can improve the efficiency of developing and approving capability requirements; and

(iii) any additional recommendations for legislation, regulations, or policies that the Secretary determines appropriate.

Subtitle B—Amendments to General Contracting Authorities, Procedures, and Limitations

SEC. 811. SUSTAINMENT REFORM FOR THE DEPARTMENT OF DEFENSE.

(a) SUSTAINMENT ACTIVITIES IN THE NATIONAL DEFENSE STRATEGY.—

(1) IN GENERAL.—Section 113(g)(1)(B) of title 10, United States Code, as amended by section 551 of this Act, is further amended by adding at the end the following new clauses:

"(viii) A strategic framework prescribed by the Secretary that guides how the Department will prioritize and integrate activities relating to sustainment of major defense acquisition programs, core logistics capabilities (as described under section 2464 of this title), commercial logistics capabilities, and the national technology and industrial base (as defined in section 2500 of this title).

Time period.

"(ix) A strategic framework prescribed by the Secretary that guides how the Department will specifically address contested logistics, including major investments for related infrastructure, logistics-related authorities, force posture, related

individual (which may include an interim security clearance), while such individual awaits a final determination with respect to the security clearance required for such position.

(b) UNCLASSIFIED WORK SPACES.—As part of the policy under subsection (a), the Secretary of Defense shall—

(1) ensure, to the extent practicable, that all facilities of the Department of Defense at which covered individuals perform job functions have unclassified workspaces; and

(2) issue guidelines under which appropriately screened individuals, who are not covered individuals, may use the unclassified workspaces on a space-available basis. Guidelines.

(c) REPORT.—Not later than one year after the date of enactment of this Act, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report setting forth the policy required by subsection (a). The report shall include the following:

(1) Identification of any challenges or impediments to allowing covered individuals fill positions on a probationary basis as described in subsection (a).

(2) A plan for implementing the policy. Implementation plan.

(3) A description of how existing facilities may be modified to accommodate unclassified workspaces.

(4) Identification of impediments to making unclassified workspace available.

(d) COVERED INDIVIDUAL DEFINED.—In this section, the term "covered individual" includes a member of the Armed Forces, a civilian employee of the Department of Defense, or an applicant for a civilian position within the Department of Defense, who has applied for, but who has not yet received, a security clearance that is required for the individual to perform one or more job functions.

SEC. 1102. ENHANCEMENT OF PUBLIC-PRIVATE TALENT EXCHANGE PROGRAMS IN THE DEPARTMENT OF DEFENSE.

(a) PUBLIC-PRIVATE TALENT EXCHANGE.—Section 1599g of title 10, United States Code, is amended—

(1) in subsection (b)(1), by amending subparagraph (C) to read as follows:

"(C) shall contain language ensuring that such employee of the Department does not improperly use information that such employee knows relates to a Department acquisition or procurement for the benefit or advantage of the private-sector organization."; and

(2) by amending paragraph (4) of subsection (f) to read as follows:

"(4) may not perform work that is considered inherently governmental in nature; and".

(b) APPLICATION OF EXCHANGE AUTHORITY TO MODERNIZATION PRIORITIES.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall take steps to ensure that the authority of the Secretary to carry out a public-private talent exchange program under section 1599g of title 10, United States Code (as amended by subsection (a)), is used to— Deadline. 10 USC 1599g note.

(1) carry out exchanges of personnel with private sector entities that are working on the modernization priorities of the Department of Defense; and

(2) carry out exchanges in—

(A) the office of the Under Secretary of Defense for Research and Engineering;

(B) the office of the Chief Information Officer of the Department of Defense;

(C) each Armed Force under the jurisdiction of the Secretary of a military department; and

(D) any other organizations or elements of the Department of Defense the Secretary determines appropriate.

(c) CONFLICTS OF INTEREST.—The Secretary shall implement a system to identify, mitigate, and manage any conflicts of interests that may arise as a result of an individual's participation in a public-private talent exchange under section 1599g of title 10, United States Code.

Consultation.

(d) TREATMENT OF PROGRAM PARTICIPANTS.—The Secretary of Defense, in consultation with each Secretary of a military department, shall develop practices to ensure that participation by a member of an Armed Force under the jurisdiction of the Secretary of a military department in an public-private talent exchange under section 1599g of title 10, United States Code, is taken into consideration in subsequent assignments.

(e) BRIEFING ON USE OF EXISTING EXCHANGE PROGRAM AUTHORITY.—

Deadline.
Time period.

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter for 5 years, the Secretary of Defense shall provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the efforts undertaken—

(A) to implement the public-private exchange programs of the Department of Defense; and

(B) to ensure that such programs seek opportunities for exchanges with private sector entities working on modernization priorities of the Department of Defense, including artificial intelligence applications, in accordance with the requirements of this section.

(2) ELEMENTS.—Each briefing under paragraph (1) shall include an explanation of—

(A) what barriers may prevent supervisors from nominating their staff and encouraging participation in public-private exchange programs;

(B) how the Department can incentivize senior leaders and supervisors to encourage participation in such programs;

(C) how the Department is implementing the requirment of subsection (c) relating to conflicts of interest; and

(D) what, if any, statutory changes or authorities are needed to effectively carry out such programs.

Paid Parental Leave Technical Corrections Act of 2020.
2 USC 1301 note.

SEC. 1103. PAID PARENTAL LEAVE TECHNICAL CORRECTIONS.

(a) SHORT TITLE.—This section may be cited as the "Paid Parental Leave Technical Corrections Act of 2020".

(b) PAID PARENTAL LEAVE FOR EMPLOYEES OF DISTRICT OF COLUMBIA COURTS AND DISTRICT OF COLUMBIA PUBLIC DEFENDER SERVICE.—

(1) DISTRICT OF COLUMBIA COURTS.—Section 11–1726, District of Columbia Official Code, is amended by adding at the end the following new subsection:

"(d) In carrying out the Family and Medical Leave Act of 1993 (29 U.S.C. 2601 et seq.) with respect to nonjudicial employees of the District of Columbia courts, the Joint Committee on Judicial Administration shall, notwithstanding any provision of such Act, establish a paid parental leave program for the leave described in subparagraphs (A) and (B) of section 102(a)(1) of such Act (29 U.S.C. 2612(a)(1)) (relating to leave provided in connection with the birth of a child or a placement of a child for adoption or foster care). In developing the terms and conditions for this program, the Joint Committee may be guided by the terms and conditions applicable to the provision of paid parental leave for employees of the Federal Government under chapter 63 of title 5, United States Code, and any corresponding regulations.".

(2) DISTRICT OF COLUMBIA PUBLIC DEFENDER SERVICE.—Section 305 of the District of Columbia Court Reform and Criminal Procedure Act of 1970 (section 2–1605, D.C. Official Code) is amended by adding at the end the following new subsection:

"(d) In carrying out the Family and Medical Leave Act of 1993 (29 U.S.C. 2601 et seq.) with respect to employees of the Service, the Director shall, notwithstanding any provision of such Act, establish a paid parental leave program for the leave described in subparagraphs (A) and (B) of section 102(a)(1) of such Act (29 U.S.C. 2612(a)(1)) (relating to leave provided in connection with the birth of a child or the placement of a child for adoption or foster care). In developing the terms and conditions for this program, the Director may be guided by the terms and conditions applicable to the provision of paid parental leave for employees of the Federal Government under chapter 63 of title 5, United States Code, and any corresponding regulations.".

(c) FAA AND TSA.—

(1) IN GENERAL.—Section 40122(g) of title 49, United States Code, is amended—

(A) by redesignating paragraph (5) as paragraph (6); and

(B) by inserting after paragraph (4) the following:

"(5) PAID PARENTAL LEAVE.—The Administrator shall implement a paid parental leave benefit for employees of the Administration that is, at a minimum, consistent with the paid parental leave benefits provided under section 6382 of title 5.".

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall apply with respect to any birth or placement occurring on or after October 1, 2020. Applicability. 49 USC 40122 note.

(3) RULE OF CONSTRUCTION.—Nothing in this subsection, or any amendment made by this subsection, may be construed to affect leave provided to an employee of the Transportation Security Administration before October 1, 2020. 49 USC 40122 note.

(d) TITLE 38 EMPLOYEES.—

(1) IN GENERAL.—Section 7425 of title 38, United States Code, is amended—

(A) in subsection (b), by striking "Notwithstanding" and inserting "Except as provided in subsection (c), and notwithstanding"; and

(B) by adding at the end the following:

"(c) Notwithstanding any other provision of this subchapter, the Administration shall provide to individuals appointed to any

position described in section 7421(b) who are employed for compensation by the Administration, family and medical leave in the same manner and subject to the same limitations to the maximum extent practicable, as family and medical leave is provided under subchapter V of chapter 63 of title 5 to employees, as defined in section 6381(1) of such title.".

38 USC 7425 note.

(2) APPLICABILITY.—The amendments made by paragraph (1) shall apply with respect to any event for which leave may be taken under subchapter V of chapter 63 of title 5, United States Code, occurring on or after October 1, 2020.

(e) EMPLOYEES OF EXECUTIVE OFFICE OF THE PRESIDENT.—

(1) IN GENERAL.—Section 412 of title 3, United States Code, is amended—

(A) in subsection (a), by adding at the end the following:

"(3) EXCEPTION.—Notwithstanding section 401(b)(2), the requirements of paragraph (2)(B) shall not apply with respect to leave under subparagraph (A) or (B) of section 102(a)(1) of the Family and Medical Leave Act of 1993 (29 U.S.C. 2612(a)(1)).";

(B) by redesignating subsections (c) and (d) as subsections (d) and (e), respectively;

(C) by inserting after subsection (b) the following:

"(c) SPECIAL RULES FOR SUBSTITUTION OF PAID LEAVE.—

"(1) SUBSTITUTION OF PAID LEAVE.—A covered employee may elect to substitute for any leave without pay under subparagraph (A) or (B) of section 102(a)(1) of the Family and Medical Leave Act of 1993 (29 U.S.C. 2612(a)(1)) any paid leave which is available to such employee for that purpose.

"(2) AVAILABLE LEAVE.—The paid leave that is available to a covered employee for purposes of paragraph (1) is leave of the type and in the amount available to an employee under section 6382(d)(2)(B) of title 5, United States Code, for substitution for leave without pay under subparagraph (A) or (B) of section 6382(a)(1) of such title.

"(3) CONSISTENCY WITH TITLE 5.—Paid leave shall be substituted under this subsection in a manner that is consistent with the requirements in section 6382(d)(2) of title 5, United States Code, except that a reference in that section to an employing agency shall be considered to be a reference to an employing office, and subparagraph (E) of that section shall not apply.";

(D) in paragraph (2) of subsection (d), as redesignated by subparagraph (B)—

(i) in subparagraph (A), by striking "and" at the end of the subparagraph;

(ii) in subparagraph (B) by striking the period at the end and inserting "; and"; and

(iii) by adding at the end the following:

"(C) except that the President or designee shall issue regulations to implement subsection (c) in accordance with the requirements of that subsection."; and

(E) in paragraph (1) of subsection (e), as redesignated by subparagraph (B), by inserting after "subsection (c)" the following: "(as in effect on the date of enactment of the Presidential and Executive Office Accountability Act)".

(2) APPLICABILITY.—The amendments made by this subsection shall apply with respect to any birth or placement occurring on or after October 1, 2020. 3 USC 412 note.

(f) AMENDMENTS TO TITLE 5 FAMILY AND MEDICAL LEAVE ACT PROVISIONS.—Chapter 63 of title 5, United States Code, is amended—

(1) in section 6301(2), by amending clause (v) to read as follows:

"(v) an employee of the Veterans Health Administration who is covered by a leave system established under section 7421 of title 38;";

(2) in section 6381(1)—

(A) in subparagraph (A), by striking "(v) or"; and

(B) by amending subparagraph (B) to read as follows:

"(B) has completed at least 12 months of service as an employee (as defined in section 2105) of the Government of the United States, including service with the United States Postal Service, the Postal Regulatory Commission, and a nonappropriated fund instrumentality as described in section 2105(c);"; and

(3) in section 6382(d)—

(A) in paragraph (1), by striking "under subchapter I" in each place it appears; and

(B) in paragraph (2)(B)(ii), by striking "under subchapter I".

(g) AMENDMENT TO CONGRESSIONAL ACCOUNTABILITY ACT OF 1995.—

(1) IN GENERAL.—Section 202(d)(2)(B) of the Congressional Accountability Act of 1995 (2 U.S.C. 1312(d)(2)(B)), as amended by section 7603 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92), is amended by inserting "accrued" before "sick leave".

(2) EFFECTIVE DATE.—The amendment made by this subsection shall apply with respect to any event for which leave may be taken under subparagraph (A) or (B) of section 102(a)(1) of the Family and Medical Leave Act of 1995 (29 U.S.C. 2612(a)(1)) and occurring on or after October 1, 2020. 2 USC 1312 note.

SEC. 1104. AUTHORITY TO PROVIDE TRAVEL AND TRANSPORTATION ALLOWANCES IN CONNECTION WITH TRANSFER CEREMONIES OF CERTAIN CIVILIAN EMPLOYEES WHO DIE OVERSEAS.

(a) TRAVEL AND TRANSPORTATION ALLOWANCES.—

(1) IN GENERAL.—Subchapter II of chapter 75 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 1492. Authority to provide travel and transportation allowances in connection with transfer ceremonies of certain civilian employees who die overseas 10 USC 1492.

"(a) AUTHORITY.—A covered official may treat a covered relative of a covered employee under the jurisdiction of that covered official in the same manner the Secretary of a military department treats, under section 481f(d) of title 37, next of kin and family members of a member of the armed forces who dies while located or serving overseas.

"(b) DEFINITIONS.—In this section:

"(F) designate a Department of Defense entity to develop, apply, and continually refine an assessment capability for defining and measuring the impact of Department information operations, which entity shall be organizationally independent of Department components performing or otherwise engaged in operational support to Department information operations.".

SEC. 1750. REPORT ON USE OF ENCRYPTION BY DEPARTMENT OF DEFENSE NATIONAL SECURITY SYSTEMS.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to Congress a report detailing the mission need and efficacy of full disk encryption across Non-classified Internet Protocol Router Network (NIPRNet) and Secretary Internet Protocol Router Network (SIPRNet) endpoint computer systems. Such report shall cover matters relating to cost, mission impact, and implementation timeline.

SEC. 1751. GUIDANCE AND DIRECTION ON USE OF DIRECT HIRING PROCESSES FOR ARTIFICIAL INTELLIGENCE PROFESSIONALS AND OTHER DATA SCIENCE AND SOFTWARE DEVELOPMENT PERSONNEL.

10 USC 1599h note.

(a) GUIDANCE REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall review applicable Department of Defense guidance and where beneficial issue new guidance to the secretaries of the military departments and the heads of the defense components on improved use of the direct hiring processes for artificial intelligence professionals and other data science and software development personnel.

Deadline. Review.

(b) OBJECTIVE.—The objective of the guidance issued under subsection (a) shall be to ensure that organizational leaders assume greater responsibility for the results of civilian hiring of artificial intelligence professionals and other data science and software development personnel.

(c) CONTENTS OF GUIDANCE.—At a minimum, the guidance required by subsection (a) shall—

(1) instruct human resources professionals and hiring authorities to utilize available direct hiring authorities (including excepted service authorities) for the hiring of artificial intelligence professionals and other data science and software development personnel, to the maximum extent practicable;

(2) instruct hiring authorities, when using direct hiring authorities, to prioritize utilization of panels of subject matter experts over human resources professionals to assess applicant qualifications and determine which applicants are best qualified for a position;

(3) authorize and encourage the use of ePortfolio reviews to provide insight into the previous work of applicants as a tangible demonstration of capabilities and contribute to the assessment of applicant qualifications by subject matter experts; and

(4) encourage the use of referral bonuses for recruitment and hiring of highly qualified artificial intelligence professionals and other data science and software development personnel in accordance with volume 451 of Department of Defense Instruction 1400.25.

(d) REPORT.—

(1) IN GENERAL.—Not later than one year after the date on which the guidance is issued under subsection (a), the Secretary shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a report on the guidance issued pursuant to subsection (a).

(2) CONTENTS.—At a minimum, the report submitted under paragraph (1) shall address the following:

(A) The objectives of the guidance and the manner in which the guidance seeks to achieve those objectives.

(B) The effect of the guidance on the hiring process for artificial intelligence professionals and other data science and software development personnel, including the effect on—

(i) hiring time;

(ii) the use of direct hiring authority;

(iii) the use of subject matter experts; and

(iv) the quality of new hires, as assessed by hiring managers and organizational leaders.

6 USC 1500.

SEC. 1752. NATIONAL CYBER DIRECTOR.

(a) ESTABLISHMENT.—There is established, within the Executive Office of the President, the Office of the National Cyber Director (in this section referred to as the "Office").

(b) NATIONAL CYBER DIRECTOR.—

President.

(1) IN GENERAL.—The Office shall be headed by the National Cyber Director (in this section referred to as the "Director") who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) POSITION.—The Director shall hold office at the pleasure of the President.

(3) PAY AND ALLOWANCES.—The Director shall be entitled to receive the same pay and allowances as are provided for level II of the Executive Schedule under section 5313 of title 5, United States Code.

(c) DUTIES OF THE NATIONAL CYBER DIRECTOR.—

(1) IN GENERAL.—Subject to the authority, direction, and control of the President, the Director shall—

(A) serve as the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of—

(i) information security and data protection;

(ii) programs and policies intended to improve the cybersecurity posture of the United States;

(iii) efforts to understand and deter malicious cyber activity;

(iv) efforts to increase the security of information and communications technology and services and to promote national supply chain risk management and vendor security;

(v) diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace;

(vi) awareness and adoption of emerging technology that may enhance, augment, or degrade the cybersecurity posture of the United States; and

SEC. 4701. DEPARTMENT OF ENERGY NATIONAL SECURITY PROGRAMS
(In Thousands of Dollars)

Program	FY 2021 Request	Conference Authorized
Construction:		
15–D–412 Utility Saft	50,000	50,000
21–D–401 Hoisting Capability Project	10,000	10,000
Total, Construction	**60,000**	**60,000**
Total, Waste Isolation Pilot Plant	**383,260**	**383,260**
Program direction	275,285	275,285
Program support	12,979	12,979
Technology development	25,000	25,000
Safeguards and Security		
Safeguards and Security	320,771	320,771
Total, Safeguards and Security	**320,771**	**320,771**
Prior year balances credited	–109,000	–109,000
Total, Defense Environmental Cleanup	**4,983,608**	**5,815,767**
Other Defense Activities		
Environment, health, safety and security		
Environment, health, safety and security	134,320	134,320
Program direction	75,368	75,368
Total, Environment, Health, safety and security	**209,688**	**209,688**
Independent enterprise assessments		
Independent enterprise assessments	26,949	26,949
Program direction	54,635	54,635
Total, Independent enterprise assessments	**81,584**	**81,584**
Specialized security activities	258,411	258,411
Office of Legacy Management		
Legacy management	293,873	140,194
Rejection of proposed transfer		[–153,679]
Program direction	23,120	23,120
Total, Office of Legacy Management	**316,993**	**163,314**
Defense related administrative support	183,789	183,789
Office of hearings and appeals	4,262	4,262
Subtotal, Other defense activities	**1,054,727**	**901,048**
Total, Other Defense Activities	**1,054,727**	**901,048**

DIVISION E—NATIONAL ARTIFICIAL INTELLIGENCE INITIATIVE ACT OF 2020

National Artificial Intelligence Initiative Act of 2020.
15 USC 9401 note.

SEC. 5001. SHORT TITLE.

This division may be cited as the "National Artificial Intelligence Initiative Act of 2020".

15 USC 9401.

SEC. 5002. DEFINITIONS.

In this division:

(1) ADVISORY COMMITTEE.—The term "Advisory Committee" means the National Artificial Intelligence Advisory Committee established under section 5104(a).

(2) AGENCY HEAD.—The term "agency head" means the head of any Executive agency (as defined in section 105 of title 5, United States Code).

(3) ARTIFICIAL INTELLIGENCE.—The term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—

(A) perceive real and virtual environments;

(B) abstract such perceptions into models through analysis in an automated manner; and

(C) use model inference to formulate options for information or action.

(4) COMMUNITY COLLEGE.—The term "community college" means a public institution of higher education at which the highest degree that is predominantly awarded to students is an associate's degree, including 2-year Tribal Colleges or Universities under section 316 of the Higher Education Act of 1965 (20 U.S.C. 1059c) and public 2-year State institutions of higher education.

(5) INITIATIVE.—The term "Initiative" means the National Artificial Intelligence Initiative established under section 5101(a).

(6) INITIATIVE OFFICE.—The term "Initiative Office" means the National Artificial Intelligence Initiative Office established under section 5102(a).

(7) INSTITUTE.—The term "Institute" means an Artificial Intelligence Research Institute described in section 5201(b)(2).

(8) INSTITUTION OF HIGHER EDUCATION.—The term "institution of higher education" has the meaning given the term in section 101 and section 102(c) of the Higher Education Act of 1965 (20 U.S.C. 1001).

(9) INTERAGENCY COMMITTEE.—The term "Interagency Committee" means the interagency committee established under section 5103(a).

(10) K-12 EDUCATION.—The term "K-12 education" means elementary school and secondary school education provided by local educational agencies, as such agencies are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(11) MACHINE LEARNING.—The term "machine learning" means an application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed.

TITLE LI—NATIONAL ARTIFICIAL INTELLIGENCE INITIATIVE

15 USC 9411.

SEC. 5101. NATIONAL ARTIFICIAL INTELLIGENCE INITIATIVE.

President.

(a) ESTABLISHMENT; PURPOSES.—The President shall establish and implement an initiative to be known as the "National Artificial Intelligence Initiative". The purposes of the Initiative shall be to—

(1) ensure continued United States leadership in artificial intelligence research and development;

(2) lead the world in the development and use of trustworthy artificial intelligence systems in the public and private sectors;

(3) prepare the present and future United States workforce for the integration of artificial intelligence systems across all sectors of the economy and society; and

(4) coordinate ongoing artificial intelligence research, development, and demonstration activities among the civilian agencies, the Department of Defense and the Intelligence Community to ensure that each informs the work of the others.

(b) INITIATIVE ACTIVITIES.—In carrying out the Initiative, the President. President, acting through the Initiative Office, the Interagency Committee, and agency heads as the President considers appropriate, shall carry out activities that include the following:

(1) Sustained and consistent support for artificial intelligence research and development through grants, cooperative agreements, testbeds, and access to data and computing resources.

(2) Support for K-12 education and postsecondary educational programs, including workforce training and career and technical education programs, and informal education programs to prepare the American workforce and the general public to be able to create, use, and interact with artificial intelligence systems.

(3) Support for interdisciplinary research, education, and workforce training programs for students and researchers that promote learning in the methods and systems used in artificial intelligence and foster interdisciplinary perspectives and collaborations among subject matter experts in relevant fields, including computer science, mathematics, statistics, engineering, social sciences, health, psychology, behavioral science, ethics, security, legal scholarship, and other disciplines that will be necessary to advance artificial intelligence research and development responsibly.

(4) Interagency planning and coordination of Federal artificial intelligence research, development, demonstration, standards engagement, and other activities under the Initiative, as appropriate.

(5) Outreach to diverse stakeholders, including citizen groups, industry, and civil rights and disability rights organizations, to ensure public input is taken into account in the activities of the Initiative.

(6) Leveraging existing Federal investments to advance objectives of the Initiative.

(7) Support for a network of interdisciplinary artificial intelligence research institutes, as described in section 5201(b)(7)(B).

(8) Support opportunities for international cooperation with strategic allies, as appropriate, on the research and development, assessment, and resources for trustworthy artificial intelligence systems.

(c) LIMITATION.—The Initiative shall not impact sources and Determination. methods, as determined by the Director of National Intelligence.

(d) RULES OF CONSTRUCTION.—Nothing in this division shall be construed as—

(1) modifying any authority or responsibility, including any operational authority or responsibility of any head of a Federal department or agency, with respect to intelligence or the intelligence community, as those terms are defined in 50 U.S.C. 3003;

(2) authorizing the Initiative, or anyone associated with its derivative efforts to approve, interfere with, direct or to conduct an intelligence activity, resource, or operation; or

(3) authorizing the Initiative, or anyone associated with its derivative efforts to modify the classification of intelligence information.

(e) SUNSET.—The Initiative established in this division shall terminate on the date that is 10 years after the date of enactment of this Act.

15 USC 9412.

SEC. 5102. NATIONAL ARTIFICIAL INTELLIGENCE INITIATIVE OFFICE.

Appointment.

(a) IN GENERAL.—The Director of the Office of Science and Technology Policy shall establish or designate, and appoint a director of, an office to be known as the "National Artificial Intelligence Initiative Office" to carry out the responsibilities described in subsection (b) with respect to the Initiative. The Initiative Office shall have sufficient staff to carry out such responsibilities, including staff detailed from the Federal departments and agencies described in section 5103(c), as appropriate.

(b) RESPONSIBILITIES.—The Director of the Initiative Office shall—

(1) provide technical and administrative support to the Interagency Committee and the Advisory Committee;

(2) serve as the point of contact on Federal artificial intelligence activities for Federal departments and agencies, industry, academia, nonprofit organizations, professional societies, State governments, and such other persons as the Initiative Office considers appropriate to exchange technical and programmatic information;

(3) conduct regular public outreach to diverse stakeholders, including civil rights and disability rights organizations; and

(4) promote access to the technologies, innovations, best practices, and expertise derived from Initiative activities to agency missions and systems across the Federal Government.

Coordination. Updates. Summary.

(c) FUNDING ESTIMATE.—The Director of the Office of Science and Technology Policy, in coordination with each participating Federal department and agency, as appropriate, shall develop and annually update an estimate of the funds necessary to carry out the activities of the Initiative Coordination Office and submit such estimate with an agreed summary of contributions from each agency to Congress as part of the President's annual budget request to Congress.

15 USC 9413.

SEC. 5103. COORDINATION BY INTERAGENCY COMMITTEE.

(a) INTERAGENCY COMMITTEE.—The Director of the Office of Science and Technology Policy, acting through the National Science and Technology Council, shall establish or designate an Interagency Committee to coordinate Federal programs and activities in support of the Initiative.

(b) CO-CHAIRS.—The Interagency Committee shall be co-chaired by the Director of the Office of Science and Technology Policy

and, on an annual rotating basis, a representative from the Department of Commerce, the National Science Foundation, or the Department of Energy, as selected by the Director of the Office of Science and Technology Policy.

(c) AGENCY PARTICIPATION.—The Committee shall include representatives from Federal agencies as considered appropriate by determination and agreement of the Director of the Office of Science and Technology Policy and the head of the affected agency. Determination.

(d) RESPONSIBILITIES.—The Interagency Committee shall—

(1) provide for interagency coordination of Federal artificial intelligence research, development, and demonstration activities and education and workforce training activities and programs of Federal departments and agencies undertaken pursuant to the Initiative;

(2) not later than 2 years after the date of the enactment of this Act, develop a strategic plan for artificial intelligence (to be updated not less than every 3 years) that establishes goals, priorities, and metrics for guiding and evaluating how the agencies carrying out the Initiative will— Deadline. Strategic plan. Updates. Time period.

(A) determine and prioritize areas of artificial intelligence research, development, and demonstration requiring Federal Government leadership and investment;

(B) support long-term funding for interdisciplinary artificial intelligence research, development, demonstration, and education;

(C) support research and other activities on ethical, legal, environmental, safety, security, bias, and other appropriate societal issues related to artificial intelligence;

(D) provide or facilitate the availability of curated, standardized, secure, representative, aggregate, and privacy-protected data sets for artificial intelligence research and development;

(E) provide or facilitate the necessary computing, networking, and data facilities for artificial intelligence research and development;

(F) support and coordinate Federal education and workforce training activities related to artificial intelligence; and

(G) support and coordinate the network of artificial intelligence research institutes described in section 5201(b)(7)(B);

(3) as part of the President's annual budget request to Congress, propose an annually coordinated interagency budget for the Initiative to the Office of Management and Budget that is intended to ensure that the balance of funding across the Initiative is sufficient to meet the goals and priorities established for the Initiative; and

(4) in carrying out this section, take into consideration the recommendations of the Advisory Committee, existing reports on related topics, and the views of academic, State, industry, and other appropriate groups.

(e) ANNUAL REPORT.—For each fiscal year beginning with fiscal year 2022, not later than 90 days after submission of the President's annual budget request for such fiscal year, the Interagency Committee shall prepare and submit to the Committee on Science, Space, and Technology, the Committee on Energy and Commerce,

the Committee on Transportation and Infrastructure, the Committee on Armed Services, the House Permanent Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Appropriations of the House of Representatives and the Committee on Commerce, Science, and Transportation, the Committee on Health, Education, Labor, and Pensions, the Committee on Energy and Natural Resources, the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, the Senate Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Appropriations of the Senate a report that includes a summarized budget in support of the Initiative for such fiscal year and the preceding fiscal year, including a disaggregation of spending and a description of any Institutes established under section 5201 for the Department of Commerce, the Department of Defense, the Department of Energy, the Department of Agriculture, the Department of Health and Human Services, and the National Science Foundation.

15 USC 9414.

SEC. 5104. NATIONAL ARTIFICIAL INTELLIGENCE ADVISORY COMMITTEE.

Consultation.
Establishment.

(a) IN GENERAL.—The Secretary of Commerce shall, in consultation with the Director of the Office of Science and Technology Policy, the Secretary of Defense, the Secretary of Energy, the Secretary of State, the Attorney General, and the Director of National Intelligence establish an advisory committee to be known as the "National Artificial Intelligence Advisory Committee".

Appointments.

(b) QUALIFICATIONS.—The Advisory Committee shall consist of members, appointed by the Secretary of Commerce, who are representing broad and interdisciplinary expertise and perspectives, including from academic institutions, companies across diverse sectors, nonprofit and civil society entities, including civil rights and disability rights organizations, and Federal laboratories, who are representing geographic diversity, and who are qualified to provide advice and information on science and technology research, development, ethics, standards, education, technology transfer, commercial application, security, and economic competitiveness related to artificial intelligence.

(c) MEMBERSHIP CONSIDERATION.—In selecting the members of the Advisory Committee, the Secretary of Commerce shall seek and give consideration to recommendations from Congress, industry, nonprofit organizations, the scientific community (including the National Academies of Sciences, Engineering, and Medicine, scientific professional societies, and academic institutions), the defense and law enforcement communities, and other appropriate organizations.

(d) DUTIES.—The Advisory Committee shall advise the President and the Initiative Office on matters related to the Initiative, including recommendations related to—

(1) the current state of United States competitiveness and leadership in artificial intelligence, including the scope and scale of United States investments in artificial intelligence research and development in the international context;

(2) the progress made in implementing the Initiative, including a review of the degree to which the Initiative has achieved the goals according to the metrics established by the Interagency Committee under section 5103(d)(2);

(3) the state of the science around artificial intelligence, including progress toward artificial general intelligence;

(4) issues related to artificial intelligence and the United States workforce, including matters relating to the potential for using artificial intelligence for workforce training, the possible consequences of technological displacement, and supporting workforce training opportunities for occupations that lead to economic self-sufficiency for individuals with barriers to employment and historically underrepresented populations, including minorities, Indians (as defined in 25 U.S.C. 5304), low-income populations, and persons with disabilities.

(5) how to leverage the resources of the initiative to streamline and enhance operations in various areas of government operations, including health care, cybersecurity, infrastructure, and disaster recovery;

(6) the need to update the Initiative;

(7) the balance of activities and funding across the Initiative;

(8) whether the strategic plan developed or updated by the Interagency Committee established under section 5103(d)(2) is helping to maintain United States leadership in artificial intelligence;

(9) the management, coordination, and activities of the Initiative;

(10) whether ethical, legal, safety, security, and other appropriate societal issues are adequately addressed by the Initiative;

(11) opportunities for international cooperation with strategic allies on artificial intelligence research activities, standards development, and the compatibility of international regulations;

(12) accountability and legal rights, including matters relating to oversight of artificial intelligence systems using regulatory and nonregulatory approaches, the responsibility for any violations of existing laws by an artificial intelligence system, and ways to balance advancing innovation while protecting individual rights; and

(13) how artificial intelligence can enhance opportunities for diverse geographic regions of the United States, including urban, Tribal, and rural communities.

(e) SUBCOMMITTEE ON ARTIFICIAL INTELLIGENCE AND LAW ENFORCEMENT.—

(1) ESTABLISHMENT.—The chairperson of the Advisory Committee shall establish a subcommittee on matters relating to the development of artificial intelligence relating to law enforcement matters.

(2) ADVICE.—The subcommittee shall provide advice to the President on matters relating to the development of artificial intelligence relating to law enforcement, including advice on the following:

(A) Bias, including whether the use of facial recognition by government authorities, including law enforcement agencies, is taking into account ethical considerations and addressing whether such use should be subject to additional oversight, controls, and limitations.

(B) Security of data, including law enforcement's access to data and the security parameters for that data.

(C) Adoptability, including methods to allow the United States Government and industry to take advantage of artificial intelligence systems for security or law enforcement purposes while at the same time ensuring the potential abuse of such technologies is sufficiently mitigated.

(D) Legal standards, including those designed to ensure the use of artificial intelligence systems are consistent with the privacy rights, civil rights and civil liberties, and disability rights issues raised by the use of these technologies.

Recommendations.

(f) REPORTS.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than once every 3 years thereafter, the Advisory Committee shall submit to the President, the Committee on Science, Space, and Technology, the Committee on Energy and Commerce, the House Permanent Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Armed Services of the House of Representatives, and the Committee on Commerce, Science, and Transportation, the Senate Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Committee on Armed Services of the Senate, a report on the Advisory Committee's findings and recommendations under subsection (d) and subsection (e).

(g) TRAVEL EXPENSES OF NON-FEDERAL MEMBERS.—Non-Federal members of the Advisory Committee, while attending meetings of the Advisory Committee or while otherwise serving at the request of the head of the Advisory Committee away from their homes or regular places of business, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by section 5703 of title 5, United States Code, for individuals in the Government serving without pay. Nothing in this subsection shall be construed to prohibit members of the Advisory Committee who are officers or employees of the United States from being allowed travel expenses, including per diem in lieu of subsistence, in accordance with existing law.

(h) FACA EXEMPTION.—The Secretary of Commerce shall charter the Advisory Committee in accordance with the Federal Advisory Committee Act (5 U.S.C. App.), except that the Advisory Committee shall be exempt from section 14 of such Act.

SEC. 5105. NATIONAL ACADEMIES ARTIFICIAL INTELLIGENCE IMPACT STUDY ON WORKFORCE.

Deadline. Contracts.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the National Science Foundation shall enter into a contract with the National Research Council of the National Academies of Sciences, Engineering, and Medicine to conduct a study of the current and future impact of artificial intelligence on the workforce of the United States across sectors.

(b) CONTENTS.—The study shall address—

(1) workforce impacts across sectors caused by the increased adoption of artificial intelligence, automation, and other related trends;

(2) workforce needs and employment opportunities generated by the increased adoption of artificial intelligence across sectors;

(3) research gaps and data needed to better understand and track paragraphs (1) and (2); and

(4) recommendations to address the challenges and opportunities described in paragraphs (1), (2), and (3). Recommendations.

(c) STAKEHOLDERS.—In conducting the study, the National Academies of Sciences, Engineering, and Medicine shall seek input from a wide range of stakeholders in the public and private sectors.

(d) REPORT TO CONGRESS.—The contract entered into under subsection (a) shall require the National Academies of Sciences, Engineering, and Medicine, not later than 2 years after the date of the enactment of this Act, to— Requirements.

(1) submit to the Committee on Science, Space, and Technology and the Committee on Education and Labor of the House of Representatives and the Committee on Commerce, Science, and Transportation and the Committee on Health, Education, Pension, and Labor of the Senate a report containing the findings and recommendations of the study conducted under subsection (a); and Recommendations.

(2) make a copy of such report available on a publicly accessible website. Records. Public information. Web posting.

SEC. 5106. NATIONAL AI RESEARCH RESOURCE TASK FORCE. 15 USC 9415.

(a) ESTABLISHMENT OF TASK FORCE.—

(1) ESTABLISHMENT.—

(A) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Office of Science and Technology Policy, shall establish a task force— Coordination.

(i) to investigate the feasibility and advisability of establishing and sustaining a National Artificial Intelligence Research Resource; and

(ii) to propose a roadmap detailing how such resource should be established and sustained.

(B) DESIGNATION.—The task force established by subparagraph (A) shall be known as the "National Artificial Intelligence Research Resource Task Force" (in this section referred to as the "Task Force").

(2) MEMBERSHIP.—

(A) COMPOSITION.—The Task Force shall be composed of 12 members selected by the co-chairpersons of the Task Force from among technical experts in artificial intelligence or related subjects, of whom—

(i) 4 shall be representatives from the Interagency Committee established in section 5103, including the co-chairpersons of the Task Force;

(ii) 4 shall be representatives from institutions of higher education; and

(iii) 4 shall be representatives from private organizations.

(B) APPOINTMENT.—Not later than 120 days after enactment of this Act, the co-chairpersons of the Task Force shall appoint members to the Task Force pursuant to subparagraph (A). Deadline.

(C) TERM OF APPOINTMENT.—Members of the Task Force shall be appointed for the life of the Task Force.

(D) VACANCY.—Any vacancy occurring in the membership of the Task Force shall be filled in the same manner in which the original appointment was made.

(E) CO-CHAIRPERSONS.—The Director of the Office of Science and Technology Policy and the Director of the

National Sciences Foundation, or their designees, shall be the co-chairpersons of the Task Force. If the role of the Director of the National Science Foundation is vacant, the Chair of the National Science Board shall act as a co-chairperson of the Task Force.

(F) EXPENSES FOR NON-FEDERAL MEMBERS.—

(i) Except as provided in clause (ii), non-Federal Members of the Task Force shall not receive compensation for their participation on the Task Force.

(ii) Non-Federal Members of the Task Force shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for employees under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Task Force.

(b) ROADMAP AND IMPLEMENTATION PLAN.—

(1) IN GENERAL.—The Task Force shall develop a coordinated roadmap and implementation plan for creating and sustaining a National Artificial Intelligence Research Resource.

(2) CONTENTS.—The roadmap and plan required by paragraph (1) shall include the following:

(A) Goals for establishment and sustainment of a National Artificial Intelligence Research Resource and metrics for success.

(B) A plan for ownership and administration of the National Artificial Intelligence Research Resource, including—

(i) an appropriate agency or organization responsible for the implementation, deployment, and administration of the Resource; and

(ii) a governance structure for the Resource, including oversight and decision-making authorities.

(C) A model for governance and oversight to establish strategic direction, make programmatic decisions, and manage the allocation of resources;

(D) Capabilities required to create and maintain a shared computing infrastructure to facilitate access to computing resources for researchers across the country, including scalability, secured access control, resident data engineering and curation expertise, provision of curated data sets, compute resources, educational tools and services, and a user interface portal.

Assessment. Recommendations.

(E) An assessment of, and recommended solutions to, barriers to the dissemination and use of high-quality government data sets as part of the National Artificial Intelligence Research Resource.

Assessment. Requirements.

(F) An assessment of security requirements associated with the National Artificial Intelligence Research Resource and its research and a recommendation for a framework for the management of access controls.

Assessment.

(G) An assessment of privacy and civil rights and civil liberties requirements associated with the National Artificial Intelligence Research Resource and its research.

(H) A plan for sustaining the Resource, including through Federal funding and partnerships with the private sector.

(I) Parameters for the establishment and sustainment of the National Artificial Intelligence Research Resource, including agency roles and responsibilities and milestones to implement the Resource.

(c) CONSULTATIONS.—In conducting its duties required under subsection (b), the Task Force shall consult with the following:

(1) The National Science Foundation.

(2) The Office of Science and Technology Policy.

(3) The National Academies of Sciences, Engineering, and Medicine.

(4) The National Institute of Standards and Technology.

(5) The Director of National Intelligence.

(6) The Department of Energy.

(7) The Department of Defense.

(8) The General Services Administration.

(9) The Department of Justice.

(10) The Department of Homeland Security.

(11) The Department of Health and Human Services.

(12) Private industry.

(13) Institutions of higher education.

(14) Civil and disabilities rights organizations.

(15) Such other persons as the Task Force considers appropriate.

(d) STAFF.—Staff of the Task Force shall comprise detailees with expertise in artificial intelligence, or related fields from the Office of Science and Technology Policy, the National Science Foundation, or any other agency the co-chairs deem appropriate, with the consent of the head of the agency.

(e) TASK FORCE REPORTS.—

Recommendations.

(1) INITIAL REPORT.—Not later than 12 months after the date on which all of the appointments have been made under subsection (a)(2)(B), the Task Force shall submit to Congress and the President an interim report containing the findings, conclusions, and recommendations of the Task Force. The report shall include specific recommendations regarding steps the Task Force believes necessary for the establishment and sustainment of a National Artificial Intelligence Research Resource.

(2) FINAL REPORT.—Not later than 6 months after the submittal of the interim report under paragraph (1), the Task Force shall submit to Congress and the President a final report containing the findings, conclusions, and recommendations of the Task Force, including the specific recommendations required by subsection (b).

(f) TERMINATION.—

(1) IN GENERAL.—The Task Force shall terminate 90 days after the date on which it submits the final report under subsection (e)(2).

(2) RECORDS.—Upon termination of the Task Force, all of its records shall become the records of the National Archives and Records Administration.

(g) DEFINITIONS.—In this section:

(1) NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH RESOURCE AND RESOURCE.—The terms "National Artificial Intelligence Research Resource" and "Resource" mean a system that provides researchers and students across scientific fields and disciplines with access to compute resources, co-located with

publicly-available, artificial intelligence-ready government and non-government data sets and a research environment with appropriate educational tools and user support.

(2) OWNERSHIP.—The term "ownership" means responsibility and accountability for the implementation, deployment, and ongoing development of the National Artificial Intelligence Research Resource, and for providing staff support to that effort.

TITLE LII—NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH INSTITUTES

15 USC 9431.

SEC. 5201. NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH INSTITUTES.

(a) IN GENERAL.—Subject to the availability of funds appropriated for this purpose, the Director of the National Science Foundation shall establish a program to award financial assistance for the planning, establishment, and support of a network of Institutes (as described in subsection (b)(2)) in accordance with this section.

(b) FINANCIAL ASSISTANCE TO ESTABLISH AND SUPPORT NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH INSTITUTES.—

Determination.

(1) IN GENERAL.—Subject to the availability of funds appropriated for this purpose, the Secretary of Energy, the Secretary of Commerce, the Director of the National Science Foundation, and every other agency head may award financial assistance to an eligible entity, or consortia thereof, as determined by an agency head, to establish and support an Institute.

(2) ARTIFICIAL INTELLIGENCE INSTITUTES.—An Institute described in this subsection is an artificial intelligence research institute that—

(A) is focused on—

(i) a particular economic or social sector, including health, education, manufacturing, agriculture, security, energy, and environment, and includes a component that addresses the ethical, societal, safety, and security implications relevant to the application of artificial intelligence in that sector; or

(ii) a cross-cutting challenge for artificial intelligence systems, including trustworthiness, or foundational science;

(B) requires partnership among public and private organizations, including, as appropriate, Federal agencies, institutions of higher education, including community colleges, nonprofit research organizations, Federal laboratories, State, local, and Tribal governments, industry, including startup companies, and civil society organizations, including civil rights and disability rights organizations (or consortia thereof);

(C) has the potential to create an innovation ecosystem, or enhance existing ecosystems, to translate Institute research into applications and products, as appropriate to the topic of each Institute;

(D) supports interdisciplinary research and development across multiple institutions of higher education and organizations;

(E) supports interdisciplinary education activities, including curriculum development, research experiences, and faculty professional development across undergraduate, graduate, and professional academic programs; and

(F) supports workforce development in artificial intelligence related disciplines in the United States, including increasing participation of historically underrepresented communities.

(3) USE OF FUNDS.—Financial assistance awarded under paragraph (1) may be used by an Institute for—

(A) managing and making available to researchers accessible, curated, standardized, secure, and privacy protected data sets from the public and private sectors for the purposes of training and testing artificial intelligence systems and for research using artificial intelligence systems, pursuant to subsections (c), (e), and (f) of section 22A the National Institute of Standards and Technology Act (as added by section 5301 of this division); Data.

(B) developing and managing testbeds for artificial intelligence systems, including sector-specific test beds, designed to enable users to evaluate artificial intelligence systems prior to deployment;

(C) conducting research and education activities involving artificial intelligence systems to solve challenges with social, economic, health, scientific, and national security implications;

(D) providing or brokering access to computing resources, networking, and data facilities for artificial intelligence research and development relevant to the Institute's research goals;

(E) providing technical assistance to users, including software engineering support, for artificial intelligence research and development relevant to the Institute's research goals;

(F) engaging in outreach and engagement to broaden participation in artificial intelligence research and the artificial intelligence workforce; and

(G) such other activities that an agency head, whose agency's missions contribute to or are affected by artificial intelligence, considers consistent with the purposes described in section 5101(a).

(4) DURATION.—

(A) INITIAL PERIODS.—An award of financial assistance under paragraph (1) shall be awarded for an initial period of 5 years.

(B) EXTENSION.—An established Institute may apply for, and the agency head may grant, extended funding for periods of 5 years on a merit-reviewed basis using the merit review criteria of the sponsoring agency.

(5) APPLICATION FOR FINANCIAL ASSISTANCE.—A person seeking financial assistance under paragraph (1) shall submit to an agency head an application at such time, in such manner,

and containing such information as the agency head may require.

(6) COMPETITIVE, MERIT REVIEW.—In awarding financial assistance under paragraph (1), the agency head shall—

(A) use a competitive, merit review process that includes peer review by a diverse group of individuals with relevant expertise from both the private and public sectors; and

(B) ensure the focus areas of the Institute do not substantially and unnecessarily duplicate the efforts of any other Institute.

(7) COLLABORATION.—

(A) IN GENERAL.—In awarding financial assistance under paragraph (1), an agency head may collaborate with Federal departments and agencies whose missions contribute to or are affected by artificial intelligence systems.

(B) COORDINATING NETWORK.—The Director of the National Science Foundation shall establish a network of Institutes receiving financial assistance under this subsection, to be known as the "Artificial Intelligence Leadership Network", to coordinate cross-cutting research and other activities carried out by the Institutes.

(8) LIMITATION.—No funds authorized in this title shall be awarded to Institutes outside of the United States. All awardees and subawardees for such Institute shall be based in the United States, in addition to any other eligibility criteria as established by each agency head.

TITLE LIII—DEPARTMENT OF COMMERCE ARTIFICIAL INTELLIGENCE ACTIVITIES

SEC. 5301. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACTIVITIES.

The National Institute of Standards and Technology Act (15 U.S.C. 271 et seq.) is amended by inserting after section 22 the following:

15 USC 278h–1.

"SEC. 22A. STANDARDS FOR ARTIFICIAL INTELLIGENCE.

"(a) MISSION.—The Institute shall—

"(1) advance collaborative frameworks, standards, guidelines, and associated methods and techniques for artificial intelligence;

"(2) support the development of a risk-mitigation framework for deploying artificial intelligence systems;

"(3) support the development of technical standards and guidelines that promote trustworthy artificial intelligence systems; and

"(4) support the development of technical standards and guidelines by which to test for bias in artificial intelligence training data and applications.

"(b) SUPPORTING ACTIVITIES.—The Director of the National Institute of Standards and Technology may—

"(1) support measurement research and development of best practices and voluntary standards for trustworthy artificial intelligence systems, which may include—

"(A) privacy and security, including for datasets used to train or test artificial intelligence systems and software and hardware used in artificial intelligence systems;

"(B) advanced computer chips and hardware designed for artificial intelligence systems;

"(C) data management and techniques to increase the usability of data, including strategies to systematically clean, label, and standardize data into forms useful for training artificial intelligence systems and the use of common, open licenses;

"(D) safety and robustness of artificial intelligence systems, including assurance, verification, validation, security, control, and the ability for artificial intelligence systems to withstand unexpected inputs and adversarial attacks;

"(E) auditing mechanisms and benchmarks for accuracy, transparency, verifiability, and safety assurance for artificial intelligence systems;

"(F) applications of machine learning and artificial intelligence systems to improve other scientific fields and engineering;

"(G) model documentation, including performance metrics and constraints, measures of fairness, training and testing processes, and results;

"(H) system documentation, including connections and dependences within and between systems, and complications that may arise from such connections; and

"(I) all other areas deemed by the Director to be critical to the development and deployment of trustworthy artificial intelligence;

"(2) produce curated, standardized, representative, high-value, secure, aggregate, and privacy protected data sets for artificial intelligence research, development, and use; Data.

"(3) support one or more institutes as described in section 5201(b) of the National Artificial Intelligence Initiative Act of 2020 for the purpose of advancing measurement science, voluntary consensus standards, and guidelines for trustworthy artificial intelligence systems;

"(4) support and strategically engage in the development of voluntary consensus standards, including international standards, through open, transparent, and consensus-based processes; and

"(5) enter into and perform such contracts, including cooperative research and development arrangements and grants and cooperative agreements or other transactions, as may be necessary in the conduct of the work of the National Institute of Standards and Technology and on such terms as the Director considers appropriate, in furtherance of the purposes of this division. Contracts. Grants.

"(c) RISK MANAGEMENT FRAMEWORK.—Not later than 2 years after the date of the enactment of this Act, the Director shall work to develop, and periodically update, in collaboration with other public and private sector organizations, including the National Deadline. Updates.

Science Foundation and the Department of Energy, a voluntary risk management framework for trustworthy artificial intelligence systems. The framework shall—

Guidelines.
Procedures.

"(1) identify and provide standards, guidelines, best practices, methodologies, procedures and processes for—

"(A) developing trustworthy artificial intelligence systems;

"(B) assessing the trustworthiness of artificial intelligence systems; and

"(C) mitigating risks from artificial intelligence systems;

"(2) establish common definitions and characterizations for aspects of trustworthiness, including explainability, transparency, safety, privacy, security, robustness, fairness, bias, ethics, validation, verification, interpretability, and other properties related to artificial intelligence systems that are common across all sectors;

"(3) provide case studies of framework implementation;

"(4) align with international standards, as appropriate;

"(5) incorporate voluntary consensus standards and industry best practices; and

"(6) not prescribe or otherwise require the use of specific information or communications technology products or services.

"(d) PARTICIPATION IN STANDARD SETTING ORGANIZATIONS.—

"(1) REQUIREMENT.—The Institute shall participate in the development of standards and specifications for artificial intelligence.

"(2) PURPOSE.—The purpose of this participation shall be to ensure—

"(A) that standards promote artificial intelligence systems that are trustworthy; and

"(B) that standards relating to artificial intelligence reflect the state of technology and are fit-for-purpose and developed in transparent and consensus-based processes that are open to all stakeholders.

Deadline.

"(e) DATA SHARING BEST PRACTICES.—Not later than 1 year after the date of enactment of this Act, the Director shall, in collaboration with other public and private sector organizations, develop guidance to facilitate the creation of voluntary data sharing arrangements between industry, federally funded research centers, and Federal agencies for the purpose of advancing artificial intelligence research and technologies, including options for partnership models between government entities, industry, universities, and nonprofits that incentivize each party to share the data they collected.

Deadline.

"(f) BEST PRACTICES FOR DOCUMENTATION OF DATA SETS.—Not later than 1 year after the date of enactment of this Act, the Director shall, in collaboration with other public and private sector organizations, develop best practices for datasets used to train artificial intelligence systems, including—

"(1) standards for metadata that describe the properties of datasets, including—

"(A) the origins of the data;

"(B) the intent behind the creation of the data;

"(C) authorized uses of the data;

"(D) descriptive characteristics of the data, including what populations are included and excluded from the datasets; and

"(E) any other properties as determined by the Director; and

"(2) standards for privacy and security of datasets with human characteristics.

"(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Institute of Standards and Technology to carry out this section—

"(1) $64,000,000 for fiscal year 2021;
"(2) $70,400,000 for fiscal year 2022;
"(3) $77,440,000 for fiscal year 2023;
"(4) $85,180,000 for fiscal year 2024; and
"(5) $93,700,000 for fiscal year 2025.".

SEC. 5302. STAKEHOLDER OUTREACH. 15 USC 9441.

In carrying out the activities under section 22A of the National Institute of Standards and Technology Act (15 U.S.C. 271 et seq.) as amended by title III of this Act, the Director shall—

(1) solicit input from university researchers, private sector experts, relevant Federal agencies, Federal laboratories, State, Tribal, and local governments, civil society groups, and other relevant stakeholders;

(2) solicit input from experts in relevant fields of social science, technology ethics, and law; and

(3) provide opportunity for public comment on guidelines and best practices developed as part of the Initiative, as appropriate.

SEC. 5303. NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION ARTIFICIAL INTELLIGENCE CENTER. 15 USC 9442.

(a) IN GENERAL.—The Administrator of the National Oceanic and Atmospheric Administration (hereafter referred to as "the Administrator") shall establish, a Center for Artificial Intelligence (hereafter referred to as "the Center"). Establishment.

(b) CENTER GOALS.—The goals of the Center shall be to—

(1) coordinate and facilitate the scientific and technological efforts related to artificial intelligence across the National Oceanic and Atmospheric Administration; and Coordination.

(2) expand external partnerships, and build workforce proficiency to effectively transition artificial intelligence research and applications to operations.

(c) COMPREHENSIVE PROGRAM.—Through the Center, the Administrator shall implement a comprehensive program to improve the use of artificial intelligence systems across the agency in support of the mission of the National Oceanic and Atmospheric Administration.

(d) CENTER PRIORITIES.—The priorities of the Center shall be to—

(1) coordinate and facilitate artificial intelligence research and innovation, tools, systems, and capabilities across the National Oceanic and Atmospheric Administration; Coordination.

(2) establish data standards and develop and maintain a central repository for agency-wide artificial intelligence applications; Data standards.

(3) accelerate the transition of artificial intelligence research to applications in support of the mission of the National Oceanic and Atmospheric Administration;

(4) develop and conduct training for the workforce of the National Oceanic and Atmospheric Administration related to artificial intelligence research and application of artificial intelligence for such agency;

(5) facilitate partnerships between the National Oceanic and Atmospheric Administration and other public sector organizations, private sector organizations, and institutions of higher education for research, personnel exchange, and workforce development with respect to artificial intelligence systems; and

Data.

(6) make data of the National Oceanic and Atmospheric Administration accessible, available, and ready for artificial intelligence applications.

(e) STAKEHOLDER ENGAGEMENT.—In carrying out the activities authorized in this section, the Administrator shall—

(1) collaborate with a diverse set of stakeholders including private sector entities and institutions of higher education;

(2) leverage the collective body of research on artificial intelligence and machine learning; and

(3) engage with relevant Federal agencies, research communities, and potential users of data and methods made available through the Center.

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Administrator to carry out this section $10,000,000 for fiscal year 2021.

(g) PROTECTION OF NATIONAL SECURITY INTERESTS.—

Consultation.
Determination.

(1) IN GENERAL.—Notwithstanding any other provision of this section, the Administrator, in consultation with the Secretary of Defense as appropriate, may withhold models or data used by the Center if the Administrator determines doing so to be necessary to protect the national security interests of the United States.

(2) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to supersede any other provision of law governing the protection of the national security interests of the United States.

TITLE LIV—NATIONAL SCIENCE FOUNDATION ARTIFICIAL INTELLIGENCE ACTIVITIES

15 USC 9451.

SEC. 5401. ARTIFICIAL INTELLIGENCE RESEARCH AND EDUCATION.

(a) IN GENERAL.—the Director of the National Science Foundation shall fund research and education activities in artificial intelligence systems and related fields, including competitive awards or grants to institutions of higher education or eligible nonprofit organizations (or consortia thereof).

(b) USES OF FUNDS.—In carrying out the activities under subsection (a), the Director of the National Science Foundation shall—

(1) support research, including interdisciplinary research, on artificial intelligence systems and related areas, including

fields and research areas that will contribute to the development and deployment of trustworthy artificial intelligence systems, and fields and research areas that address the application of artificial intelligence systems to scientific discovery and societal challenges;

(2) use the existing programs of the National Science Foundation, in collaboration with other Federal departments and agencies, as appropriate to—

(A) improve the teaching and learning of topics related to artificial intelligence systems in K-12 education and postsecondary educational programs, including workforce training and career and technical education programs, undergraduate and graduate education programs, and in informal settings; and

(B) increase participation in artificial intelligence related fields, including by individuals identified in sections 33 and 34 of the Science and Engineering Equal Opportunity Act (42 U.S.C. 1885a, 1885b);

(3) support partnerships among institutions of higher education, Federal laboratories, nonprofit organizations, State, local, and Tribal governments, industry, and potential users of artificial intelligence systems that facilitate collaborative research, personnel exchanges, and workforce development and identify emerging research needs with respect to artificial intelligence systems;

(4) ensure adequate access to research and education infrastructure with respect to artificial intelligence systems, which may include the development of new computing resources and partnership with the private sector for the provision of cloud-based computing services;

(5) conduct prize competitions, as appropriate, pursuant to section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719);

(6) coordinate research efforts funded through existing programs across the directorates of the National Science Foundation; Coordination.

(7) provide guidance on data sharing by grantees to public and private sector organizations consistent with the standards and guidelines developed under section 22A(e) of the National Institute of Standards and Technology Act (as added by section 5301 of this division); and

(8) evaluate opportunities for international collaboration with strategic allies on artificial intelligence research and development. Evaluation.

(c) ENGINEERING SUPPORT.—In general, the Director shall permit applicants to include in their proposed budgets funding for software engineering support to assist with the proposed research.

(d) ETHICS.—

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

(A) a number of emerging areas of research, including artificial intelligence, have potential ethical, social, safety, and security risks that might be apparent as early as the basic research stage;

(B) the incorporation of ethical, social, safety, and security considerations into the research design and review

process for Federal awards may help mitigate potential harms before they happen;

(C) the National Science Foundation's agreement with the National Academies of Sciences, Engineering, and Medicine to conduct a study and make recommendations with respect to governance of research in computing and computing technologies is a positive step toward accomplishing this goal; and

(D) the National Science Foundation should continue to work with stakeholders to understand and adopt policies that promote best practices for governance of research in emerging technologies at every stage of research.

(2) REPORT ON ETHICS STATEMENTS.—No later than 6 months after publication of the study described in paragraph (1)(C), the Director shall report to Congress on options for requiring an ethics or risk statement as part of all or a subset of applications for research funding to the National Science Foundation.

(e) EDUCATION.—

Grants.

(1) IN GENERAL.—The Director of the National Science Foundation shall award grants for artificial intelligence education research, development and related activities to support K-12 and postsecondary education programs and activities, including workforce training and career and technical education programs and activities, undergraduate, graduate, and postdoctoral education, and informal education programs and activities that—

(A) support the development of a diverse workforce pipeline for science and technology with respect to artificial intelligence systems;

(B) increase awareness of potential ethical, social, safety, and security risks of artificial intelligence systems;

(C) promote curriculum development for teaching topics related to artificial intelligence, including in the field of technology ethics;

(D) support efforts to achieve equitable access to K-12 artificial intelligence education in diverse geographic areas and for populations historically underrepresented in science, engineering, and artificial intelligence fields; and

(E) promote the widespread understanding of artificial intelligence principles and methods to create an educated workforce and general public able to use products enabled by artificial intelligence systems and adapt to future societal and economic changes caused by artificial intelligence systems.

(2) ARTIFICIAL INTELLIGENCE FACULTY FELLOWSHIPS.—

Grants.

(A) FACULTY RECRUITMENT FELLOWSHIPS.—

(i) IN GENERAL.—The Director of the National Science Foundation shall establish a program to award grants to eligible institutions of higher education to recruit and retain tenure-track or tenured faculty in artificial intelligence and related fields.

(ii) USE OF FUNDS.—An institution of higher education shall use grant funds provided under clause (i) for the purposes of—

(I) recruiting new tenure-track or tenured faculty members that conduct research and teaching

in artificial intelligence and related fields and research areas, including technology ethics; and

(II) paying salary and benefits for the academic year of newly recruited tenure-track or tenured faculty members for a duration of up to three years.

(iii) ELIGIBLE INSTITUTIONS OF HIGHER EDUCATION.—For purposes of this subparagraph, an eligible institution of higher education is—

(I) a Historically Black College and University (within the meaning of the term "part B institution" under section 322 of the Higher Education Act of 1965), Tribal College or University, or other minority-serving institution, as defined in section 371(a) of the Higher Education Act of 1965;

(II) an institution classified under the Carnegie Classification of Institutions of Higher Education as a doctorate-granting university with a high level of research activity; or

(III) an institution located in a State jurisdiction eligible to participate in the National Science Foundation's Established Program to Stimulate Competitive Research.

(B) FACULTY TECHNOLOGY ETHICS FELLOWSHIPS.—

(i) IN GENERAL.—The Director of the National Science Foundation shall establish a program to award fellowships to tenure-track and tenured faculty in social and behavioral sciences, ethics, law, and related fields to develop new research projects and partnerships in technology ethics.

(ii) PURPOSES.—The purposes of such fellowships are to enable researchers in social and behavioral sciences, ethics, law, and related fields to establish new research and education partnerships with researchers in artificial intelligence and related fields; learn new techniques and acquire systematic knowledge in artificial intelligence and related fields; and mentor and advise graduate students and postdocs pursuing research in technology ethics.

(iii) USES OF FUNDS.—A fellowship may include salary and benefits for up to one academic year, expenses to support coursework or equivalent training in artificial intelligence systems, and additional such expenses that the Director deems appropriate.

(C) UPDATE TO ROBERT NOYCE TEACHER SCHOLARSHIP PROGRAM.—Section 10(i)(5) of the National Science Foundation Authorization Act of 2002 (42 U.S.C. 1862n–1(i)(5)) is amended by inserting "and artificial intelligence" after "computer science".

(3) UPDATE TO ADVANCED TECHNOLOGICAL EDUCATION PROGRAM.—

(A) IN GENERAL.—Section 3(b) of the Scientific and Advanced-Technology Act of 1992 (42 U.S.C. 1862(i)) is amended by striking "10" and inserting "12".

(B) ARTIFICIAL INTELLIGENCE CENTERS OF EXCELLENCE.—The Director of the National Science Foundation shall establish national centers of scientific and technical

education to advance education and workforce development in areas related to artificial intelligence pursuant to section 3 of the Scientific and Advanced-Technology Act of 1992 (42 U.S.C. 1862(i)). Activities of such centers may include—

Evaluations.

(i) the development, dissemination, and evaluation of curriculum and other educational tools and methods in artificial intelligence related fields and research areas, including technology ethics;

(ii) the development and evaluation of artificial intelligence related certifications for 2-year programs; and

(iii) interdisciplinary science and engineering research in employment-based adult learning and career retraining related to artificial intelligence fields.

(f) NATIONAL SCIENCE FOUNDATION PILOT PROGRAM OF GRANTS FOR RESEARCH IN RAPIDLY EVOLVING, HIGH PRIORITY TOPICS.—

Assessment.

(1) PILOT PROGRAM REQUIRED.—The Director of the National Science Foundation shall establish a pilot program to assess the feasibility and advisability of awarding grants for the conduct of research in rapidly evolving, high priority topics using funding mechanisms that require brief project descriptions and internal merit review, and that may include accelerated external review.

(2) DURATION.—

(A) IN GENERAL.—The Director shall carry out the pilot program required by paragraph (1) during the 5-year period beginning on the date of the enactment of this Act.

(B) ASSESSMENT AND CONTINUATION AUTHORITY.—After the period set forth in paragraph (2)(A)—

(i) the Director shall assess the pilot program; and

Determination.

(ii) if the Director determines that it is both feasible and advisable to do so, the Director may continue the pilot program.

(3) GRANTS.—In carrying out the pilot program, the Director shall award grants for the conduct of research in topics selected by the Director in accordance with paragraph (4).

(4) TOPIC SELECTION.—The Director shall select topics for research under the pilot program in accordance with the following:

(A) The Director shall select artificial intelligence as the initial topic for the pilot program.

Determination.

(B) The Director may select additional topics that the Director determines are—

(i) rapidly evolving; and

(ii) of high importance to the economy and security of the United States.

(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this section—

(1) $868,000,000 for fiscal year 2021;
(2) $911,400,000 for fiscal year 2022;
(3) $956,970,000 for fiscal year 2023;
(4) $1,004,820,000 for fiscal year 2024; and
(5) $1,055,060,000 for fiscal year 2025.

TITLE LV—DEPARTMENT OF ENERGY ARTIFICIAL INTELLIGENCE RESEARCH PROGRAM

SEC. 5501. DEPARTMENT OF ENERGY ARTIFICIAL INTELLIGENCE RESEARCH PROGRAM. 15 USC 9461.

(a) IN GENERAL.—The Secretary shall carry out a cross-cutting research and development program to advance artificial intelligence tools, systems, capabilities, and workforce needs and to improve the reliability of artificial intelligence methods and solutions relevant to the mission of the Department. In carrying out this program, the Secretary shall coordinate across all relevant offices and programs at the Department, including the Office of Science, the Office of Energy Efficiency and Renewable Energy, the Office of Nuclear Energy, the Office of Fossil Energy, the Office of Electricity, the Office of Cybersecurity, Energy Security, and Emergency Response, the Advanced Research Projects Agency-Energy, and any other relevant office determined by the Secretary. Coordination. Determination.

(b) RESEARCH AREAS.—In carrying out the program under subsection (a), the Secretary shall award financial assistance to eligible entities to carry out research projects on topics including—

(1) the application of artificial intelligence systems to improve large-scale simulations of natural and other phenomena;

(2) the study of applied mathematics, computer science, and statistics, including foundations of methods and systems of artificial intelligence, causal and statistical inference, and the development of algorithms for artificial intelligence systems;

(3) the analysis of existing large-scale datasets from science and engineering experiments and simulations, including energy simulations and other priorities at the Department as determined by the Secretary using artificial intelligence tools and techniques; Analysis. Data. Determination.

(4) the development of operation and control systems that enhance automated, intelligent decisionmaking capabilities;

(5) the development of advanced computing hardware and computer architecture tailored to artificial intelligence systems, including the codesign of networks and computational hardware;

(6) the development of standardized datasets for emerging artificial intelligence research fields and applications, including methods for addressing data scarcity; and Data.

(7) the development of trustworthy artificial intelligence systems, including—

(A) algorithmic explainability;

(B) analytical methods for identifying and mitigating bias in artificial intelligence systems; and

(C) safety and robustness, including assurance, verification, validation, security, and control.

(c) TECHNOLOGY TRANSFER.—In carrying out the program under subsection (a), the Secretary shall support technology transfer of artificial intelligence systems for the benefit of society and United States economic competitiveness.

(d) FACILITY USE AND UPGRADES.—In carrying out the program under subsection (a), the Secretary shall—

(1) make available high-performance computing infrastructure at national laboratories;

(2) make any upgrades necessary to enhance the use of existing computing facilities for artificial intelligence systems, including upgrades to hardware;

(3) establish new computing capabilities necessary to manage data and conduct high performance computing that enables the use of artificial intelligence systems; and

(4) maintain and improve, as needed, networking infrastructure, data input and output mechanisms, and data analysis, storage, and service capabilities.

(e) REPORT ON ETHICS STATEMENTS.—Not later than 6 months after publication of the study described in section 5401(d)(1)(C), the Secretary shall report to Congress on options for requiring an ethics or risk statement as part of all or a subset of applications for research activities funded by the Department of Energy and performed at Department of Energy national laboratories and user facilities.

Review. (f) RISK MANAGEMENT.—The Secretary shall review agency policies for risk management in artificial intelligence related projects and issue as necessary policies and principles that are consistent with the framework developed under section 22A(c) of the National Institute of Standards and Technology Act (as added by section 5301 of this division).

Review. (g) DATA PRIVACY AND SHARING.—The Secretary shall review agency policies for data sharing with other public and private sector organizations and issue as necessary policies and principles that are consistent with the standards and guidelines submitted under section 22A(e) of the National Institute of Standards and Technology Act (as added by section 5301 of this division). In addition, the Secretary shall establish a streamlined mechanism for approving research projects or partnerships that require sharing sensitive public or private data with the Department.

(h) PARTNERSHIPS WITH OTHER FEDERAL AGENCIES.—The Secretary may request, accept, and provide funds from other Federal departments and agencies, State, United States territory, local, or Tribal government agencies, private sector for-profit entities, and nonprofit entities, to be available to the extent provided by appropriations Acts, to support a research project or partnership carried out under this section. The Secretary may not give any special consideration to any agency or entity in return for a donation.

(i) STAKEHOLDER ENGAGEMENT.—In carrying out the activities authorized in this section, the Secretary shall—

(1) collaborate with a range of stakeholders including small businesses, institutes of higher education, industry, and the National Laboratories;

(2) leverage the collective body of knowledge from existing artificial intelligence and machine learning research; and

(3) engage with other Federal agencies, research communities, and potential users of information produced under this section.

(j) DEFINITIONS.—In this section:

(1) SECRETARY.—The term "Secretary" means the Secretary of Energy.

(2) DEPARTMENT.—The term "Department" means the Department of Energy.

(3) NATIONAL LABORATORY.—The term "national laboratory" has the meaning given such term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(4) ELIGIBLE ENTITIES.—The term "eligible entities" means—

(A) an institution of higher education;

(B) a National Laboratory;

(C) a Federal research agency;

(D) a State research agency;

(E) a nonprofit research organization;

(F) a private sector entity; or

(G) a consortium of 2 or more entities described in subparagraphs (A) through (F).

(k) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Department to carry out this section—

(1) $200,000,000 for fiscal year 2021;

(2) $214,000,000 for fiscal year 2022;

(3) $228,980,000 for fiscal year 2023;

(4) $245,000,000 for fiscal year 2024; and

(5) $262,160,000 for fiscal year 2025.

DIVISION F—ANTI-MONEY LAUNDERING

Anti-Money Laundering Act of 2020.

31 USC 5301 note.

SEC. 6001. SHORT TITLE.

This division may be cited as the "Anti-Money Laundering Act of 2020".

31 USC 5311 note.

SEC. 6002. PURPOSES.

The purposes of this division are—

(1) to improve coordination and information sharing among the agencies tasked with administering anti-money laundering and countering the financing of terrorism requirements, the agencies that examine financial institutions for compliance with those requirements, Federal law enforcement agencies, national security agencies, the intelligence community, and financial institutions;

(2) to modernize anti-money laundering and countering the financing of terrorism laws to adapt the government and private sector response to new and emerging threats;

(3) to encourage technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and the financing of terrorism;

(4) to reinforce that the anti-money laundering and countering the financing of terrorism policies, procedures, and controls of financial institutions shall be risk-based;

(5) to establish uniform beneficial ownership information reporting requirements to—

(A) improve transparency for national security, intelligence, and law enforcement agencies and financial institutions concerning corporate structures and insight into the flow of illicit funds through those structures;

(B) discourage the use of shell corporations as a tool to disguise and move illicit funds;

(2) ELEMENTS.—Each report required under paragraph (1) shall include—

(A) a description of the strategic goals of the Office of Technical Assistance in the year preceding submission of the report, including an explanation of how technical assistance provided by the Office in that year advanced those goals;

(B) a description of technical assistance provided by the Office in that year, including the objectives and delivery methods of the assistance;

(C) a list of beneficiaries and providers (other than Office staff) of the technical assistance during that year; and

(D) a description of how—

(i) technical assistance provided by the Office complements, duplicates, or otherwise affects or is affected by technical assistance provided by the international financial institutions (as defined in section 1701(c) of the International Financial Institutions Act (22 U.S.C. 262r(c))); and

(ii) efforts to coordinate the technical assistance described in clause (i).

SEC. 6112. INTERNATIONAL COORDINATION.

31 USC 5311 note.

(a) IN GENERAL.—The Secretary shall work with foreign counterparts of the Secretary, including through bilateral contacts, the Financial Action Task Force, the International Monetary Fund, the World Bank, the Egmont Group of Financial Intelligence Units, the Organisation for Economic Co-operation and Development, the Basel Committee on Banking Supervision, and the United Nations, to promote stronger anti-money laundering frameworks and enforcement of anti-money laundering laws.

(b) SUPPORT FOR STRENGTHENING THE CAPACITY OF THE INTERNATIONAL MONETARY FUND TO PREVENT MONEY LAUNDERING AND THE FINANCING OF TERRORISM.—Section 7125 of the Otto Warmbier North Korea Nuclear Sanctions and Enforcement Act of 2019 (title LXXI of division F of Public Law 116–92; 133 Stat. 2249) is amended—

22 USC 262p–13 note.

(1) in subsection (b), by striking "5" and inserting "6"; and

(2) in subsection (c), by striking "2023" and inserting "2024".

TITLE LXII—MODERNIZING THE ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM SYSTEM

SEC. 6201. ANNUAL REPORTING REQUIREMENTS.

31 USC 5311 note.

(a) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Attorney General, in consultation with the Secretary, Federal law enforcement agencies, the Director of National Intelligence, Federal functional regulators, and the heads of other appropriate Federal agencies, shall submit to the Secretary a report that contains statistics, metrics, and other information on the use of data derived from financial institutions reporting under the Bank Secrecy Act (referred to in this subsection as the "reported data"), including—

Time period. Consultation. Data.

(1) the frequency with which the reported data contains actionable information that leads to—

(A) further procedures by law enforcement agencies, including the use of a subpoena, warrant, or other legal process; or

(B) actions taken by intelligence, national security, or homeland security agencies;

(2) calculations of the time between the date on which the reported data is reported and the date on which the reported data is used by law enforcement, intelligence, national security, or homeland security agencies, whether through the use of—

(A) a subpoena or warrant; or

(B) other legal process or action;

(3) an analysis of the transactions associated with the reported data, including whether—

Analysis.

(A) the suspicious accounts that are the subject of the reported data were held by legal entities or individuals; and

(B) there are trends and patterns in cross-border transactions to certain countries;

(4) the number of legal entities and individuals identified by the reported data;

(5) information on the extent to which arrests, indictments, convictions, criminal pleas, civil enforcement or forfeiture actions, or actions by national security, intelligence, or homeland security agencies were related to the use of the reported data; and

(6) data on the investigations carried out by State and Federal authorities resulting from the reported data.

(b) REPORT.—Beginning with the fifth report submitted under subsection (a), and once every 5 years thereafter, that report shall include a section describing the use of data derived from reporting by financial institutions under the Bank Secrecy Act over the 5 years preceding the date on which the report is submitted, which shall include a description of long-term trends and the use of long-term statistics, metrics, and other information.

Effective date. Time period. Data.

(c) TRENDS, PATTERNS, AND THREATS.—Each report required under subsection (a) and each section included under subsection (b) shall contain a description of retrospective trends and emerging

patterns and threats in money laundering and the financing of terrorism, including national and regional trends, patterns, and threats relevant to the classes of financial institutions that the Attorney General determines appropriate.

(d) USE OF REPORT INFORMATION.—The Secretary shall use the information reported under subsections (a), (b), and (c)—

Assessment.

(1) to help assess the usefulness of reporting under the Bank Secrecy Act to—

(A) criminal and civil law enforcement agencies;

(B) intelligence, defense, and homeland security agencies; and

(C) Federal functional regulators;

(2) to enhance feedback and communications with financial institutions and other entities subject to requirements under the Bank Secrecy Act, including by providing more detail in the reports published and distributed under section 314(d) of the USA PATRIOT Act (31 U.S.C. 5311 note);

(3) to assist FinCEN in considering revisions to the reporting requirements promulgated under section 314(d) of the USA PATRIOT Act (31 U.S.C. 5311 note); and

(4) for any other purpose the Secretary determines is appropriate.

(e) CONFIDENTIALITY.—Any information received by a financial institution under this section shall be subject to confidentiality requirements established by the Secretary.

SEC. 6202. ADDITIONAL CONSIDERATIONS FOR SUSPICIOUS ACTIVITY REPORTING REQUIREMENTS.

Section 5318(g) of title 31, United States Code, is amended by adding at the end the following:

"(5) CONSIDERATIONS IN IMPOSING REPORTING REQUIREMENTS.—

"(A) DEFINITIONS.—In this paragraph, the terms 'Bank Secrecy Act', 'Federal functional regulator', 'State bank supervisor', and 'State credit union supervisor' have the meanings given the terms in section 6003 of the Anti-Money Laundering Act of 2020.

Consultation.

"(B) REQUIREMENTS.—In imposing any requirement to report any suspicious transaction under this subsection, the Secretary of the Treasury, in consultation with the Attorney General, appropriate representatives of State bank supervisors, State credit union supervisors, and the Federal functional regulators, shall consider items that include—

"(i) the national priorities established by the Secretary;

"(ii) the purposes described in section 5311; and

"(iii) the means by or form in which the Secretary shall receive such reporting, including the burdens imposed by such means or form of reporting on persons required to provide such reporting, the efficiency of the means or form, and the benefits derived by the means or form of reporting by Federal law enforcement agencies and the intelligence community in countering financial crime, including money laundering and the financing of terrorism.

"(C) COMPLIANCE PROGRAM.—Reports filed under this subsection shall be guided by the compliance program of a covered financial institution with respect to the Bank Secrecy Act, including the risk assessment processes of the covered institution that should include a consideration of priorities established by the Secretary of the Treasury under section 5318.

"(D) STREAMLINED DATA AND REAL-TIME REPORTING.—

"(i) REQUIREMENT TO ESTABLISH SYSTEM.—In considering the means by or form in which the Secretary of the Treasury shall receive reporting pursuant to subparagraph (B)(iii), the Secretary of the Treasury, acting through the Director of the Financial Crimes Enforcement Network, and in consultation with appropriate representatives of the State bank supervisors, State credit union supervisors, and Federal functional regulators, shall— Consultation.

"(I) establish streamlined, including automated, processes to, as appropriate, permit the filing of noncomplex categories of reports that—

"(aa) reduce burdens imposed on persons required to report; and

"(bb) do not diminish the usefulness of the reporting to Federal law enforcement agencies, national security officials, and the intelligence community in combating financial crime, including the financing of terrorism;

"(II) subject to clause (ii)—

"(aa) permit streamlined, including automated, reporting for the categories described in subclause (I); and

"(bb) establish the conditions under which the reporting described in item (aa) is permitted; and

"(III) establish additional systems and processes as necessary to allow for the reporting described in subclause (II)(aa).

"(ii) STANDARDS.—The Secretary of the Treasury—

"(I) in carrying out clause (i), shall establish standards to ensure that streamlined reports relate to suspicious transactions relevant to potential violations of law (including regulations); and

"(II) in establishing the standards under subclause (I), shall consider transactions, including structured transactions, designed to evade any regulation promulgated under this subchapter, certain fund and asset transfers with little or no apparent economic or business purpose, transactions without lawful purposes, and any other transaction that the Secretary determines to be appropriate.

"(iii) RULE OF CONSTRUCTION.—Nothing in this subparagraph may be construed to preclude the Secretary of the Treasury from—

"(I) requiring reporting as provided for in subparagraphs (B) and (C); or

"(II) notifying Federal law enforcement with respect to any transaction that the Secretary has determined implicates a national priority established by the Secretary.".

31 USC 5318 note.

SEC. 6203. LAW ENFORCEMENT FEEDBACK ON SUSPICIOUS ACTIVITY REPORTS.

(a) FEEDBACK.—

(1) IN GENERAL.—FinCEN shall, to the extent practicable, periodically solicit feedback from individuals designated under section 5318(h)(1)(B) of title 31, United States Code, by a variety of financial institutions representing a cross-section of the reporting industry to review the suspicious activity reports filed by those financial institutions and discuss trends in suspicious activity observed by FinCEN.

(2) COORDINATION WITH FEDERAL FUNCTIONAL REGULATORS AND STATE BANK SUPERVISORS AND STATE CREDIT UNION SUPERVISORS.—FinCEN shall provide any feedback solicited under paragraph (1) to the appropriate Federal functional regulator, State bank supervisor, or State credit union supervisor during the regularly scheduled examination of the applicable financial institution by the Federal functional regulator, State bank supervisor, or State credit union supervisor, as applicable.

(b) DISCLOSURE REQUIRED.—

(1) IN GENERAL.—

(A) PERIODIC DISCLOSURE.—Except as provided in paragraph (2), FinCEN shall, to the extent practicable, periodically disclose to each financial institution, in summary form, information on suspicious activity reports filed that proved useful to Federal or State criminal or civil law enforcement agencies during the period since the most recent disclosure under this paragraph to the financial institution.

(B) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to require the public disclosure of any information filed with the Department of the Treasury under the Bank Secrecy Act.

(2) EXCEPTION FOR ONGOING OR CLOSED INVESTIGATIONS AND TO PROTECT NATIONAL SECURITY.—FinCEN shall not be required to disclose to a financial institution any information under paragraph (1) that relates to an ongoing or closed investigation or implicates the national security of the United States.

Records.

(3) MAINTENANCE OF STATISTICS.—With respect to the actions described in paragraph (1), FinCEN shall keep records of all such actions taken to assist with the production of the reports described in paragraph (5) of section 5318(g) of title 31, United States Code, as added by section 6202 of this division, and for other purposes.

(4) COORDINATION WITH DEPARTMENT OF JUSTICE.—The information disclosed by FinCEN under this subsection shall include information from the Department of Justice regarding—

(A) the review and use by the Department of suspicious activity reports filed by the applicable financial institution during the period since the most recent disclosure under this subsection; and

(B) any trends in suspicious activity observed by the Department.

SEC. 6204. STREAMLINING REQUIREMENTS FOR CURRENCY TRANSACTION REPORTS AND SUSPICIOUS ACTIVITY REPORTS.

Consultation. Regulations.

(a) REVIEW.—The Secretary, in consultation with the Attorney General, Federal law enforcement agencies, the Secretary of Homeland Security, the Federal functional regulators, State bank supervisors, State credit union supervisors, and other relevant stakeholders, shall undertake a formal review of the financial institution reporting requirements relating to currency transaction reports and suspicious activity reports, as in effect on the date of enactment of this Act, including the processes used to submit reports under the Bank Secrecy Act, regulations implementing the Bank Secrecy Act, and related guidance, and propose changes to those reports to reduce any unnecessarily burdensome regulatory requirements and ensure that the information provided fulfills the purposes described in section 5311 of title 31, United States Code, as amended by section 6101(a) of this division.

(b) CONTENTS.—The review required under subsection (a) shall—

(1) rely substantially on information obtained through the BSA Data Value Analysis Project conducted by FinCEN; and

(2) include a review of—

(A) whether the circumstances under which a financial institution determines whether to file a continuing suspicious activity report, including insider abuse, or the processes followed by a financial institution in determining whether to file a continuing suspicious activity report, or both, should be streamlined or otherwise adjusted;

(B) whether different thresholds should apply to different categories of activities;

(C) the fields designated as critical on the suspicious activity report form, the fields on the currency transaction report form, and whether the number or nature of the fields on those forms should be adjusted;

(D) the categories, types, and characteristics of suspicious activity reports and currency transaction reports that are of the greatest value to, and that best support, investigative priorities of law enforcement and national security agencies;

(E) the increased use or expansion of exemption provisions to reduce currency transaction reports that may be of little or no value to the efforts of law enforcement agencies;

(F) the most appropriate ways to promote financial inclusion and address the adverse consequences of financial institutions de-risking entire categories of relationships, including charities, embassy accounts, and money service businesses (as defined in section 1010.100(ff) of title 31, Code of Federal Regulations), and certain groups of correspondent banks without conducting a proper assessment of the specific risk of each individual member of these populations;

(G) the current financial institution reporting requirements under the Bank Secrecy Act and regulations and guidance implementing the Bank Secrecy Act;

(H) whether the process for the electronic submission of reports could be improved for both financial institutions and law enforcement agencies, including by allowing

greater integration between financial institution systems and the electronic filing system to allow for automatic population of report fields and the automatic submission of transaction data for suspicious transactions, without bypassing the obligation of each reporting financial institution to assess the specific risk of the transactions reported;

(I) the appropriate manner in which to ensure the security and confidentiality of personal information;

(J) how to improve the cross-referencing of individuals or entities operating at multiple financial institutions and across international borders;

(K) whether there are ways to improve currency transaction report aggregation for entities with common ownership;

(L) whether financial institutions should be permitted to streamline or otherwise adjust, with respect to particular types of customers or transactions, the process for determining whether activity is suspicious or the information included in the narrative of a suspicious activity report; and

(M) any other matter the Secretary determines is appropriate.

Consultation.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary, in consultation with the Attorney General, Federal law enforcement agencies, the Director of National Intelligence, the Secretary of Homeland Security, and the Federal functional regulators, shall—

Determinations.

(1) submit to Congress a report that contains all findings and determinations made in carrying out the review required under subsection (a); and

Regulations.

(2) propose rulemakings, as appropriate, to implement the findings and determinations described in paragraph (1).

Consultations.
31 USC 5313 note.
Determinations.

SEC. 6205. CURRENCY TRANSACTION REPORTS AND SUSPICIOUS ACTIVITY REPORTS THRESHOLDS REVIEW.

(a) REVIEW OF THRESHOLDS FOR CERTAIN CURRENCY TRANSACTION REPORTS AND SUSPICIOUS ACTIVITY REPORTS.—The Secretary, in consultation with the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Federal functional regulators, State bank supervisors, State credit union supervisors, and other relevant stakeholders, shall review and determine whether the dollar thresholds, including aggregate thresholds, under sections 5313, 5318(g), and 5331 of title 31, United States Code, including regulations issued under those sections, should be adjusted.

(b) CONSIDERATIONS.—In making the determinations required under subsection (a), the Secretary, in consultation with the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Federal functional regulators, State bank supervisors, State credit union supervisors, and other relevant stakeholders, shall—

(1) rely substantially on information obtained through the BSA Data Value Analysis Project conducted by FinCEN and on information obtained through the Currency Transaction Report analyses conducted by the Comptroller General of the United States; and

(2) consider—

(A) the effects that adjusting the thresholds would have on law enforcement, intelligence, national security, and homeland security agencies;

(B) the costs likely to be incurred or saved by financial institutions from any adjustment to the thresholds;

(C) whether adjusting the thresholds would better conform the United States with international norms and standards to counter money laundering and the financing of terrorism;

(D) whether currency transaction report thresholds should be tied to inflation or otherwise be adjusted based on other factors consistent with the purposes of the Bank Secrecy Act;

(E) any other matter that the Secretary determines is appropriate.

(c) REPORT AND RULEMAKINGS.—Not later than 1 year after the date of enactment of this Act, the Secretary, in consultation with the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Federal functional regulators, State bank supervisors, State credit union supervisors, and other relevant stakeholders, shall—

(1) publish a report of the findings from the review required under subsection (a); and — Publication.

(2) propose rulemakings, as appropriate, to implement the findings and determinations described in paragraph (1).

(d) UPDATES.—Not less frequently than once every 5 years during the 10-year period beginning on the date of enactment of this Act, the Secretary shall— Time periods. Effective date.

(1) evaluate findings and rulemakings described in subsection (c); and — Evaluations.

(2) transmit a written summary of the evaluation to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate; and — Summary.

(3) propose rulemakings, as appropriate, in response to the evaluation required under paragraph (1). — Regulations.

SEC. 6206. SHARING OF THREAT PATTERN AND TREND INFORMATION.

Section 5318(g) of title 31, United States Code, as amended by section 6202 of this division, is amended by adding at the end the following:

"(6) SHARING OF THREAT PATTERN AND TREND INFORMATION.—

"(A) DEFINITIONS.—In this paragraph—

"(i) the terms 'Bank Secrecy Act' and 'Federal functional regulator' have the meanings given the terms in section 6003 of the Anti-Money Laundering Act of 2020; and

"(ii) the term 'typology' means a technique to launder money or finance terrorism.

"(B) SUSPICIOUS ACTIVITY REPORT ACTIVITY REVIEW.— Not less frequently than semiannually, the Director of the Financial Crimes Enforcement Network shall publish threat pattern and trend information to provide meaningful information about the preparation, use, and value of reports filed under this subsection by financial institutions, as — Time period. Publication.

well as other reports filed by financial institutions under the Bank Secrecy Act.

"(C) INCLUSION OF TYPOLOGIES.—In each publication published under subparagraph (B), the Director shall provide financial institutions and the Federal functional regulators with typologies, including data that can be adapted in algorithms if appropriate, relating to emerging money laundering and terrorist financing threat patterns and trends.

"(7) RULES OF CONSTRUCTION.—Nothing in this subsection may be construed as precluding the Secretary of the Treasury from—

"(A) requiring reporting as provided under subparagraphs (A) and (B) of paragraph (6); or

"(B) notifying a Federal law enforcement agency with respect to any transaction that the Secretary has determined directly implicates a national priority established by the Secretary.".

SEC. 6207. SUBCOMMITTEE ON INNOVATION AND TECHNOLOGY.

Section 1564 of the Annunzio-Wylie Anti-Money Laundering Act (31 U.S.C. 5311 note) is amended by adding at the end the following:

"(d) SUBCOMMITTEE ON INNOVATION AND TECHNOLOGY.—

"(1) DEFINITIONS.—In this subsection, the terms 'Bank Secrecy Act', 'State bank supervisor', and 'State credit union supervisor' have the meanings given the terms in section 6003 of the Anti-Money Laundering Act of 2020.

"(2) ESTABLISHMENT.—There shall be within the Bank Secrecy Act Advisory Group a subcommittee to be known as the 'Subcommittee on Innovation and Technology' to—

"(A) advise the Secretary of the Treasury regarding means by which the Department of the Treasury, FinCEN, the Federal functional regulators, State bank supervisors, and State credit union supervisors, as appropriate, can most effectively encourage and support technological innovation in the area of anti-money laundering and countering the financing of terrorism and proliferation; and

"(B) reduce, to the extent practicable, obstacles to innovation that may arise from existing regulations, guidance, and examination practices related to compliance of financial institutions with the Bank Secrecy Act.

"(3) MEMBERSHIP.—

Determination.

"(A) IN GENERAL.—The subcommittee established under paragraph (1) shall consist of the representatives of the heads of the Federal functional regulators, including, as appropriate, the Bank Secrecy Act Innovation Officers as established in section 6208 of the Anti-Money Laundering Act of 2020, a representative of State bank supervisors, a representative of State credit union supervisors, representatives of a cross-section of financial institutions subject to the Bank Secrecy Act, law enforcement, FinCEN, and any other representative as determined by the Secretary of the Treasury.

"(B) REQUIREMENTS.—Each agency representative described in subparagraph (A) shall be an individual who

has demonstrated knowledge and competence concerning the application of the Bank Secrecy Act.

"(4) SUNSET.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), the Subcommittee on Innovation and Technology shall terminate on the date that is 5 years after the date of enactment of this subsection.

"(B) EXCEPTION.—The Secretary of the Treasury may renew the Subcommittee on Innovation for 1-year periods beginning on the date that is 5 years after the date of enactment of this subsection.". Renewal. Time periods. Effective date.

SEC. 6208. ESTABLISHMENT OF BANK SECRECY ACT INNOVATION OFFICERS. 31 USC 5311 note.

(a) APPOINTMENT OF OFFICERS.—Not later than 1 year after the effective date of the regulations promulgated under subsection (d) of section 310 of title 31, United States Code, as added by section 6103 of this division, an Innovation Officer shall be appointed within FinCEN and each Federal functional regulator. Deadline.

(b) INNOVATION OFFICER.—The Innovation Officer shall be appointed by, and report to, the Director of FinCEN or the head of the Federal functional regulator, as applicable.

(c) DUTIES.—Each Innovation Officer, in coordination with other Innovation Officers and the agencies of the Innovation Officers, shall—

(1) provide outreach to law enforcement agencies, State bank supervisors, financial institutions and associations of financial institutions, agents of financial institutions, and other persons (including service providers, vendors and technology companies) with respect to innovative methods, processes, and new technologies that may assist in compliance with the requirements of the Bank Secrecy Act;

(2) provide technical assistance or guidance relating to the implementation of responsible innovation and new technology by financial institutions and associations of financial institutions, agents of financial institutions, and other persons (including service providers, vendors and technology companies), in a manner that complies with the requirements of the Bank Secrecy Act;

(3) if appropriate, explore opportunities for public-private partnerships; and

(4) if appropriate, develop metrics of success.

SEC. 6209. TESTING METHODS RULEMAKING.

(a) IN GENERAL.—Section 5318 of title 31, United States Code is amended by adding at the end the following:

"(o) TESTING.—

"(1) IN GENERAL.—The Secretary of the Treasury, in consultation with the head of each agency to which the Secretary has delegated duties or powers under subsection (a), shall issue a rule to specify with respect to technology and related technology internal processes designed to facilitate compliance with the requirements under this subchapter, the standards by which financial institutions are to test the technology and related technology internal processes. Consultation. Compliance.

"(2) STANDARDS.—The standards described in paragraph (1) may include—

"(A) an emphasis on using innovative approaches such as machine learning or other enhanced data analytics processes;

"(B) risk-based testing, oversight, and other risk management approaches of the regime, prior to and after implementation, to facilitate calibration of relevant systems and prudently evaluate and monitor the effectiveness of their implementation;

Criteria.

"(C) specific criteria for when and how risk-based testing against existing processes should be considered to test and validate the effectiveness of relevant systems and situations and standards for when other risk management processes, including those developed by or through third party risk and compliance management systems, and oversight may be more appropriate;

"(D) specific standards for a risk governance framework for financial institutions to provide oversight and to prudently evaluate and monitor systems and testing processes both pre- and post-implementation;

Requirements.

"(E) requirements for appropriate data privacy and information security; and

Requirements.

"(F) a requirement that the system configurations, including any applicable algorithms and any validation of those configurations used by the regime be disclosed to the Financial Crimes Enforcement Network and the appropriate Federal functional regulator upon request.

"(3) CONFIDENTIALITY OF ALGORITHMS.—

Disclosure.

"(A) IN GENERAL.—If a financial institution or any director, officer, employee, or agent of any financial institution, voluntarily or pursuant to this subsection or any other authority, discloses the algorithms of the financial institution to a government agency, the algorithms and any materials associated with the creation or adaption of such algorithms shall be considered confidential and not subject to public disclosure.

"(B) FREEDOM OF INFORMATION ACT.—Section 552(a)(3) of title 5 (commonly known as the 'Freedom of Information Act') shall not apply to any request for algorithms described in subparagraph (A) and any materials associated with the creation or adaptation of the algorithms.

"(4) DEFINITION.—In this subsection, the term 'Federal functional regulator' means—

"(A) the Board of Governors of the Federal Reserve System;

"(B) the Office of the Comptroller of the Currency;

"(C) the Federal Deposit Insurance Corporation;

"(D) the National Credit Union Administration;

"(E) the Securities and Exchange Commission; and

"(F) the Commodity Futures Trading Commission.".

12 USC 3305 note.

(b) UPDATE OF MANUAL.—The Financial Institutions Examination Council shall ensure that any manual prepared by the Council is—

(1) updated to reflect the rulemaking required by subsection (o) section 5318 of title 31, United States Code, as added by subsection (a) of this section; and

(2) consistent with relevant FinCEN and Federal functional regulator guidance, including the December 2018 Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing.

SEC. 6210. FINANCIAL TECHNOLOGY ASSESSMENT.

Consultations.

(a) IN GENERAL.—The Secretary, in consultation with financial regulators, technology experts, national security experts, law enforcement, and any other group the Secretary determines is appropriate, shall analyze the impact of financial technology on financial crimes compliance, including with respect to money laundering, the financing of terrorism, proliferation finance, serious tax fraud, trafficking, sanctions evasion, and other illicit finance.

Determination.

(b) COORDINATION.—In carrying out the duties required under this section, the Secretary shall consult with relevant agency officials and consider other interagency efforts and data relating to examining the impact of financial technology, including activities conducted by—

Data.

(1) cyber security working groups at the Department of the Treasury;

(2) cyber security experts identified by the Attorney General and the Secretary of Homeland Security;

(3) the intelligence community; and

(4) the Financial Stability Oversight Council.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to the Committee on Banking, Housing, and Urban Affairs and the Committee on Foreign Relations of the Senate and the Committee on Financial Services and the Committee on Foreign Affairs of the House of Representatives a report containing any findings under subsection (a), including legislative and administrative recommendations.

Recommendations.

SEC. 6211. FINANCIAL CRIMES TECH SYMPOSIUM.

31 USC 5311 note.

(a) PURPOSE.—The purposes of this section are to—

(1) promote greater international collaboration in the effort to prevent and detect financial crimes and suspicious activities; and

(2) facilitate the investigation, development, and timely adoption of new technologies aimed at preventing and detecting financial crimes and other illicit activities.

(b) PERIODIC MEETINGS.—The Secretary shall, in coordination with the Subcommittee on Innovation and Technology established under subsection (d) of section 1564 of the Annunzio-Wylie Anti-Money Laundering Act, as added by section 6207 of this division, periodically convene a global anti-money laundering and financial crime symposium focused on how new technology can be used to more effectively combat financial crimes and other illicit activities.

Coordination.

(c) ATTENDEES.—Attendees at each symposium convened under this section shall include domestic and international financial regulators, senior executives from regulated firms, technology providers, representatives from law enforcement and national security agencies, academic and other experts, and other individuals that the Secretary determines are appropriate.

(d) PANELS.—At each symposium convened under this section, the Secretary shall convene panels in order to review new technologies and permit attendees to demonstrate proof of concept.

Review.

(e) IMPLEMENTATION AND REPORTS.—The Secretary shall, to the extent practicable and necessary, work to provide policy clarity, which may include providing reports or guidance to stakeholders, regarding innovative technologies and practices presented at each symposium convened under this section, to the extent that those technologies and practices further the purposes of this section.

Deadline.

(f) FINCEN BRIEFING.—Not later than 90 days after the date of enactment of this Act, the Director of FinCEN shall brief the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives on the use of emerging technologies, including—

(1) the status of implementation and internal use of emerging technologies, including artificial intelligence, digital identity technologies, distributed ledger technologies, and other innovative technologies within FinCEN;

(2) whether artificial intelligence, digital identity technologies, distributed ledger technologies, and other innovative technologies can be further leveraged to make data analysis by FinCEN more efficient and effective;

(3) whether FinCEN could better use artificial intelligence, digital identity technologies, distributed ledger technologies, and other innovative technologies to—

(A) more actively analyze and disseminate the information FinCEN collects and stores to provide investigative leads to Federal, State, Tribal, and local law enforcement agencies and other Federal agencies; and

(B) better support ongoing investigations by FinCEN when referring a case to the agencies described in subparagraph (A);

(4) with respect to each of paragraphs (1), (2), and (3), any best practices or significant concerns identified by the Director, and their applicability to artificial intelligence, digital identity technologies, distributed ledger technologies, and other innovative technologies with respect to United States efforts to combat money laundering and other forms of illicit finance;

Recommendations.

(5) any policy recommendations that could facilitate and improve communication and coordination between the private sector, FinCEN, and the agencies described in paragraph (3) through the implementation of innovative approaches to meet the obligations of the agencies under the Bank Secrecy Act and anti-money laundering compliance; and

(6) any other matter the Director determines is appropriate.

SEC. 6212. PILOT PROGRAM ON SHARING OF INFORMATION RELATED TO SUSPICIOUS ACTIVITY REPORTS WITHIN A FINANCIAL GROUP.

(a) SHARING WITH FOREIGN BRANCHES AND AFFILIATES.—Section 5318(g) of title 31, United States Code, as amended by sections 6202 and 6206 of this division, is amended by adding at the end the following:

"(8) PILOT PROGRAM ON SHARING WITH FOREIGN BRANCHES, SUBSIDIARIES, AND AFFILIATES.—

"(A) IN GENERAL.—

Deadline. Regulations. Coordination.

"(i) ISSUANCE OF RULES.—Not later than 1 year after the date of enactment of this paragraph, the

(B) the degree of reliance by financial institutions on information provided by FinCEN for purposes of obtaining and updating beneficial ownership information;

(C) strategies to improve the accuracy, completeness, and timeliness of the beneficial ownership information reported to the Secretary; and

(D) any other matter that the Secretary determines is appropriate.

TITLE LXV—MISCELLANEOUS

SEC. 6501. INVESTIGATIONS AND PROSECUTION OF OFFENSES FOR VIOLATIONS OF THE SECURITIES LAWS.

(a) IN GENERAL.—Section 21(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78u(d)) is amended—

(1) in paragraph (3)—

(A) in the paragraph heading—

(i) by inserting "CIVIL" before "MONEY PENALTIES"; and

(ii) by striking "IN CIVIL ACTIONS" and inserting "AND AUTHORITY TO SEEK DISGORGEMENT";

(B) in subparagraph (A), by striking "jurisdiction to impose" and all that follows through the period at the end and inserting the following: "jurisdiction to—

"(i) impose, upon a proper showing, a civil penalty to be paid by the person who committed such violation; and

"(ii) require disgorgement under paragraph (7) of any unjust enrichment by the person who received such unjust enrichment as a result of such violation."; and

(C) in subparagraph (B)—

(i) in clause (i), in the first sentence, by striking "the penalty" and inserting "a civil penalty imposed under subparagraph (A)(i)";

(ii) in clause (ii), by striking "amount of penalty" and inserting "amount of a civil penalty imposed under subparagraph (A)(i)"; and

(iii) in clause (iii), in the matter preceding item (aa), by striking "amount of penalty for each such violation" and inserting "amount of a civil penalty imposed under subparagraph (A)(i) for each violation described in that subparagraph";

(2) in paragraph (4), by inserting "under paragraph (7)" after "funds disgorged"; and

(3) by adding at the end the following:

"(7) DISGORGEMENT.—In any action or proceeding brought by the Commission under any provision of the securities laws, the Commission may seek, and any Federal court may order, disgorgement.

Deadlines.

"(8) LIMITATIONS PERIODS.—

"(A) DISGORGEMENT.—The Commission may bring a claim for disgorgement under paragraph (7)—

"(i) not later than 5 years after the latest date of the violation that gives rise to the action or proceeding in which the Commission seeks the claim occurs; or

"(ii) not later than 10 years after the latest date of the violation that gives rise to the action or proceeding in which the Commission seeks the claim if the violation involves conduct that violates—

"(I) section 10(b);

"(II) section 17(a)(1) of the Securities Act of 1933 (15 U.S.C. 77q(a)(1));

"(III) section 206(1) of the Investment Advisers Act of 1940 (15 U.S.C. 80b–6(1)); or

"(IV) any other provision of the securities laws for which scienter must be established.

"(B) EQUITABLE REMEDIES.—The Commission may seek a claim for any equitable remedy, including for an injunction or for a bar, suspension, or cease and desist order, not later than 10 years after the latest date on which a violation that gives rise to the claim occurs.

"(C) CALCULATION.—For the purposes of calculating any limitations period under this paragraph with respect to an action or claim, any time in which the person against which the action or claim, as applicable, is brought is outside of the United States shall not count towards the accrual of that period.

"(9) RULE OF CONSTRUCTION.—Nothing in paragraph (7) may be construed as altering any right that any private party may have to maintain a suit for a violation of this Act.".

Effective date.
15 USC 78u note.

(b) APPLICABILITY.—The amendments made by subsection (a) shall apply with respect to any action or proceeding that is pending on, or commenced on or after, the date of enactment of this Act.

SEC. 6502. GAO AND TREASURY STUDIES ON BENEFICIAL OWNERSHIP INFORMATION REPORTING REQUIREMENTS.

Assessments.

(a) EFFECTIVENESS OF INCORPORATION PRACTICES STUDY.—Not later than 2 years after the effective date of the regulations promulgated under section 5336(b)(4) of title 31, United States Code, as added by section 6403(a) of this division, the Comptroller General of the United States shall conduct a study and submit to Congress a report assessing the effectiveness of incorporation practices implemented under this division, and the amendments made by this division, in—

(1) providing national security, intelligence, and law enforcement agencies with prompt access to reliable, useful, and complete beneficial ownership information; and

(2) strengthening the capability of national security, intelligence, and law enforcement agencies to—

(A) combat incorporation abuses and civil and criminal misconduct; and

(B) detect, prevent, or prosecute money laundering, the financing of terrorism, proliferation finance, serious tax fraud, or other crimes.

(b) USING TECHNOLOGY TO AVOID DUPLICATIVE LAYERS OF REPORTING OBLIGATIONS AND INCREASE ACCURACY OF BENEFICIAL OWNERSHIP INFORMATION.—

(1) IN GENERAL.—The Secretary, in consultation with the Attorney General, shall conduct a study to evaluate— Consultation. Evaluation.

(A) the effectiveness of using FinCEN identifiers, as defined in section 5336 of title 31, United States Code, as added by section 6403(a) of this division, or other simplified reporting methods in order to facilitate a simplified beneficial ownership regime for reporting companies;

(B) whether a reporting regime, whereby only company shareholders are reported within the ownership chain of a reporting company, could effectively track beneficial ownership information and increase information to law enforcement;

(C) the costs associated with imposing any new verification requirements on FinCEN; and Costs.

(D) the resources necessary to implement any such changes.

(2) FINDINGS.—The Secretary shall submit to the relevant committees of jurisdiction—

(A) the findings of the study conducted under paragraph (1); and

(B) recommendations for carrying out the findings described in subparagraph (A). Recommendations.

(c) EXEMPT ENTITIES.—Not later than 2 years after the effective date of regulations promulgated under section 5336(b)(4) of title 31, United States Code, as added by section 6403(a) of this division, the Comptroller General of the United States, in consultation with the Secretary, Federal functional regulators, the Attorney General, the Secretary of Homeland Security, and the intelligence community, shall conduct a study and submit to Congress a report that— Consultation.

(1) reviews the regulated status, related reporting requirements, quantity, and structure of each class of corporations, limited liability companies, and similar entities that have been explicitly excluded from the definition of reporting company and the requirement to report beneficial ownership information under section 5336 of title 31, United States Code, as added by section 6403(a) of this division; Reviews.

(2) assesses the extent to which any excluded entity or class of entities described in paragraph (1) pose significant risks of money laundering, the financing of terrorism, proliferation finance, serious tax fraud, and other financial crime; and Assessments.

(3) identifies other policy areas related to the risks of exempt entities described in paragraph (1) for Congress to consider as Congress is conducting oversight of the new beneficial ownership information reporting requirements established by this division and amendments made by this division.

(d) OTHER LEGAL ENTITIES STUDY.—Not later than 2 years after the effective date of the regulations promulgated under section

5336(b)(4) of title 31, United States Code, as added by section 6403(a) of this division, the Comptroller General of the United States shall conduct a study and submit to Congress a report—

(1) identifying each State that has procedures that enable persons to form or register under the laws of the State partnerships, trusts, or other legal entities, and the nature of those procedures;

(2) identifying each State that requires persons seeking to form or register partnerships, trusts, or other legal entities under the laws of the State to provide beneficial owners (as defined in section 5336(a) of title 31, United States Code, as added by section 6403 of this division) or beneficiaries of those entities, and the nature of the required information;

Evaluations.

(3) evaluating whether the lack of available beneficial ownership information for partnerships, trusts, or other legal entities—

(A) raises concerns about the involvement of those entities in terrorism, money laundering, tax evasion, securities fraud, or other misconduct; and

(B) has impeded investigations into entities suspected of the misconduct described in subparagraph (A);

Evaluations.

(4) evaluating whether the failure of the United States to require beneficial ownership information for partnerships and trusts formed or registered in the United States has elicited international criticism; and

(5) including what steps, if any, the United States has taken, is planning to take, or should take in response to the criticism described in paragraph (4).

SEC. 6503. GAO STUDY ON FEEDBACK LOOPS.

(a) DEFINITION.—In this section, the term "feedback loop" means feedback provided by the United States Government to relevant parties.

(b) STUDY.—The Comptroller General of the United States shall conduct a study on—

(1) best practices within the United States Government for feedback loops, including regulated private entities, on the usage and usefulness of personally identifiable information, sensitive-but-unclassified data, or similar information provided by the parties to United States Government users of the information and data, including law enforcement agencies and regulators; and

(2) any practice or standard inside or outside the United States for providing feedback through sensitive information and public-private partnership information sharing efforts, specifically related to efforts to combat money laundering and other forms of illicit finance.

(c) REPORT.—Not later than 18 months after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives a report containing—

Determinations.

(1) all findings and determinations made in carrying out the study required under subsection (b);

(2) with respect to each of paragraphs (1) and (2) of subsection (b), any best practice or significant concern identified by the Comptroller General, and the applicability to public-

private partnerships and feedback loops with respect to efforts by the United States Government to combat money laundering and other forms of illicit finance; and

(3) recommendations of the Comptroller General to reduce or eliminate any unnecessary collection by the United States Government of the information described in subsection (b)(1). Recommendations.

SEC. 6504. GAO CTR STUDY AND REPORT.

The Comptroller General of the United States shall—

(1) not later than January 1, 2025, commence a study of currency transaction reports, which shall include— Analyses.

(A) a review, carried out in consultation with the Secretary, FinCEN, the Attorney General, the State attorneys general, and State, Tribal, and local law enforcement, of the effectiveness of the currency transaction reporting regime in effect as of the date of the study; Review. Consultation.

(B) an analysis of the importance of currency transaction reports to law enforcement; and

(C) an analysis of the effects of raising the currency transaction report threshold; and

(2) not later than December 31, 2025, submit to the Secretary and Congress a report that includes—

(A) all findings and determinations made in carrying out the study required under paragraph (1); and Determinations.

(B) recommendations for improving the currency transaction reporting regime. Recommendations.

SEC. 6505. GAO STUDIES ON TRAFFICKING.

(a) DEFINITION OF HUMAN TRAFFICKING.—In this section, the term "human trafficking" has the meaning given the term "severe forms of trafficking in persons" in section 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102).

(b) GAO STUDY AND REPORT ON STOPPING TRAFFICKING, ILLICIT FLOWS, LAUNDERING, AND EXPLOITATION.—

(1) STUDY.—The Comptroller General of the United States shall carry out a study, in consultation with law enforcement, relevant Federal agencies, appropriate private sector stakeholders (including financial institutions and data and technology companies), academic and other research organizations (including survivor and victim advocacy organizations), and any other group that the Comptroller General determines is appropriate on— Consultation. Determination.

(A) the major trafficking routes used by transnational criminal organizations, terrorists, and others, and to what extent the trafficking routes for people (including children), drugs, weapons, cash, child sexual exploitation materials, or other illicit goods are similar, related, or contiguous;

(B) commonly used methods to launder and move the proceeds of trafficking;

(C) the types of suspicious financial activity that are associated with illicit trafficking networks, and how financial institutions identify and report such activity;

(D) the nexus between the identities and finances of trafficked persons and fraud;

(E) the tools, guidance, training, partnerships, supervision, or other mechanisms that Federal agencies, including FinCEN, the Federal financial regulators, and

law enforcement, provide to help financial institutions identify techniques and patterns of transactions that may involve the proceeds of trafficking;

(F) what steps financial institutions are taking to detect and prevent bad actors who are laundering the proceeds of illicit trafficking, including data analysis, policies, training procedures, rules, and guidance;

(G) what role gatekeepers, such as lawyers, notaries, accountants, investment advisors, logistics agents, and trust and company service providers, play in facilitating trafficking networks and the laundering of illicit proceeds; and

(H) the role that emerging technologies, including artificial intelligence, digital identity technologies, distributed ledger technologies, virtual assets, and related exchanges and online marketplaces, and other innovative technologies, can play in assisting with and potentially enabling the laundering of proceeds from trafficking.

(2) REPORT TO CONGRESS.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives a report—

(A) summarizing the results of the study required under paragraph (1); and

(B) that contains any recommendations for legislative or regulatory action that would improve the efforts of Federal agencies to combat trafficking or the laundering of proceeds from such activity.

(c) GAO STUDY AND REPORT ON FIGHTING ILLICIT NETWORKS AND DETECTING TRAFFICKING.—

(1) STUDY.—The Comptroller General of the United States shall conduct a study on how a range of payment systems and methods, including virtual currencies in online marketplaces, are used to facilitate human trafficking and drug trafficking, which shall consider—

(A) how online marketplaces, including the dark web, may be used as platforms to buy, sell, or facilitate the financing of goods or services associated with human trafficking or drug trafficking, specifically, opioids and synthetic opioids, including fentanyl, fentanyl analogues, and any precursor chemical associated with manufacturing fentanyl or fentanyl analogues, destined for, originating from, or within the United States;

(B) how financial payment methods, including virtual currencies and peer-to-peer mobile payment services, may be utilized by online marketplaces to facilitate the buying, selling, or financing of goods and services associated with human trafficking or drug trafficking destined for, originating from, or within the United States;

(C) how virtual currencies may be used to facilitate the buying, selling, or financing of goods and services associated with human trafficking or drug trafficking, destined for, originating from, or within the United States, when an online platform is not otherwise involved;

(D) how illicit funds that have been transmitted online and through virtual currencies are repatriated into the

formal banking system of the United States through money laundering or other means;

(E) the participants, including State and non-State actors, throughout the entire supply chain that may participate in or benefit from the buying, selling, or financing of goods and services associated with human trafficking or drug trafficking, including through online marketplaces or using virtual currencies, destined for, originating from, or within the United States;

(F) Federal and State agency efforts to impede the buying, selling, or financing of goods and services associated with human trafficking or drug trafficking destined for, originating from, or within the United States, including efforts to prevent the proceeds from human trafficking or drug trafficking from entering the United States banking system;

(G) how virtual currencies and their underlying technologies can be used to detect and deter these illicit activities; and

(H) to what extent immutability and traceability of virtual currencies can contribute to the tracking and prosecution of illicit funding.

(2) REPORT TO CONGRESS.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives a report—

(A) summarizing the results of the study required under paragraph (1); and Summaries.

(B) that contains any recommendations for legislative or regulatory action that would improve the efforts of Federal agencies to impede the use of virtual currencies and online marketplaces in facilitating human trafficking and drug trafficking. Recommendations.

SEC. 6506. TREASURY STUDY AND STRATEGY ON TRADE-BASED MONEY LAUNDERING.

(a) STUDY REQUIRED.—

(1) IN GENERAL.—The Secretary shall carry out a study, in consultation with appropriate private sector stakeholders, academic and other international trade experts, and Federal agencies, on trade-based money laundering. Consultation.

(2) CONTRACTING AUTHORITY.—The Secretary may enter into a contract with a private third-party entity to carry out the study required by paragraph (1).

(b) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to Congress a report that includes—

(A) all findings and determinations made in carrying out the study required under subsection (a); and Determinations.

(B) proposed strategies to combat trade-based money laundering.

(2) CLASSIFIED ANNEX.—The report required under paragraph (1)—

(A) shall be submitted in unclassified form; and

(B) may include a classified annex.

SEC. 6507. TREASURY STUDY AND STRATEGY ON MONEY LAUNDERING BY THE PEOPLE'S REPUBLIC OF CHINA.

(a) STUDY.—The Secretary shall carry out a study, which shall rely substantially on information obtained through the trade-based money laundering analyses conducted by the Comptroller General of the United States, on—

(1) the extent and effect of illicit finance risk relating to the Government of the People's Republic of China and Chinese firms, including financial institutions;

Assessment.

(2) an assessment of the illicit finance risks emanating from the People's Republic of China;

(3) those risks allowed, directly or indirectly, by the Government of the People's Republic of China, including those enabled by weak regulatory or administrative controls of that government; and

(4) the ways in which the increasing amount of global trade and investment by the Government of the People's Republic of China and Chinese firms exposes the international financial system to increased risk relating to illicit finance.

(b) STRATEGY TO COUNTER CHINESE MONEY LAUNDERING.—Upon the completion of the study required under subsection (a), the Secretary, in consultation with such other Federal agencies as the Secretary determines appropriate, shall develop a strategy to combat Chinese money laundering activities.

Consultation. Determination.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to Congress a report containing—

(1) all findings and determinations made in carrying out the study required under subsection (a); and

(2) the strategy developed under subsection (b).

(d) CLASSIFIED ANNEX.—The report required by subsection (c)—

(1) shall be submitted in unclassified form; and

(2) may include a classified annex.

SEC. 6508. TREASURY AND JUSTICE STUDY ON THE EFFORTS OF AUTHORITARIAN REGIMES TO EXPLOIT THE FINANCIAL SYSTEM OF THE UNITED STATES.

Deadline. Consultation.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary and the Attorney General, in consultation with the heads of other relevant national security, intelligence, and law enforcement agencies, shall conduct a study that considers how authoritarian regimes in foreign countries and their proxies use the financial system of the United States to—

(1) conduct political influence operations;

(2) sustain kleptocratic methods of maintaining power;

(3) export corruption;

(4) fund nongovernmental organizations, media organizations, or academic initiatives in the United States to advance the interests of those regimes; and

(5) otherwise undermine democratic governance in the United States and the partners and allies of the United States.

(b) REPORT.—Not later than 2 years after the date of enactment of this Act, the Secretary shall submit to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives a report that contains—

(1) the results of the study required under subsection (a); and

(2) any recommendations for legislative or regulatory action, or steps to be taken by United States financial institutions, that would address exploitation of the financial system of the United States by foreign authoritarian regimes. Recommendations.

SEC. 6509. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—Subsection (l) of section 310, of title 31, United States Code, as redesignated by section 6103(1) of this division, is amended by striking paragraph (1) and inserting the following:

"(1) IN GENERAL.—There are authorized to be appropriated to FinCEN to carry out this section, to remain available until expended—

"(A) $136,000,000 for fiscal year 2021;

"(B) $60,000,000 for fiscal year 2022; and

"(C) $35,000,000 for each of fiscal years 2023 through 2026.".

(b) BENEFICIAL OWNERSHIP INFORMATION REPORTING REQUIREMENTS.—Section 5336 of title 31, United States Code, as added by section 6403(a) of this division, is amended by adding at the end the following:

"(j) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to FinCEN for each of the 3 fiscal years beginning on the effective date of the regulations promulgated under subsection (b)(4), such sums as may be necessary to carry out this section, including allocating funds to the States to pay reasonable costs relating to compliance with the requirements of such section.".

SEC. 6510. DISCRETIONARY SURPLUS FUNDS. 12 USC 289 note.

The dollar amount specified under section 7(a)(3)(A) of the Federal Reserve Act (12 U.S.C. 289(a)(3)(A)) is reduced by $40,000,000.

SEC. 6511. SEVERABILITY. 31 USC 5311 note.

If any provision of this division, an amendment made by this division, or the application of such provision or amendment to any person or circumstance is held to be unconstitutional, the remainder of this division, the amendments made by this division, and the application of the provisions of such to any person or circumstance shall not be affected thereby.

DIVISION G—ELIJAH E. CUMMINGS COAST GUARD AUTHORIZATION ACT OF 2020

Elijah E. Cummings Coast Guard Authorization Act of 2020.

SEC. 8001. SHORT TITLE.

This division may be cited as the "Elijah E. Cummings Coast Guard Authorization Act of 2020".

SEC. 8002. DEFINITION OF COMMANDANT. 14 USC 106 note.

In this division, the term "Commandant" means the Commandant of the Coast Guard.

(1) Subtitle IV of title 46, United States Code, is amended by adding at the end the following:

"PART D—FEDERAL MARITIME COMMISSION

46 USC 46101 prec.

"CHAPTER 461—FEDERAL MARITIME COMMISSION".

46 USC 46101 prec.

(2) Chapter 3 of title 46, United States Code, is redesignated as chapter 461 of part D of subtitle IV of such title and transferred to appear in such part.

46 USC 46101 prec.

(3) Sections 301 through 308 of such title are redesignated as sections 46101 through 46108, respectively, of such title.

(b) CONFORMING AMENDMENTS.—

(1) Section 46101(c)(3)(A)(v) of title 46, United States Code, as so redesignated, is amended by striking "304" and inserting "46104".

(2) section 322(b) of the Coast Guard Personnel and Maritime Safety Act of 2002 (31 U.S.C. 1113 note) is amended by striking "208 of the Merchant Marine Act, 1936 (46 App. U.S.C. 1118)" and inserting "46106(a) of title 46, United States Code".

(3) Section 1031(23) of the National Defense Authorization Act for Fiscal Year 2000 (31 U.S.C. 1113 note) is amended by striking "208, 901(b)(2), and 1211 of the Merchant Marine Act, 1936 (46 App. U.S.C. 1118, 1241(b)(2), 1291)" and inserting "44106(a) and 55305(d) of title 46, United States Code".

(4) The analysis for subtitle I of title 46, United States Code, is amended by striking the item relating to chapter 3.

46 USC 101 prec.

(5) The analysis for subtitle IV of such title is amended by adding at the end the following:

46 USC 40101 prec.

"Part D—Federal Maritime Commission

"461. Federal Maritime Commission ..... 46101".

(6) The analysis for chapter 461 of part D of subtitle IV of such title, as so redesignated, is amended to read as follows:

46 USC 46101 prec.

"Sec.
"46101. General organization.
"46102. Quorum.
"46103. Meetings.
"46104. Delegation of authority.
"46105. Regulations.
"46106. Annual report.
"46107. Expenditures.
"46108. Authorization of appropriations.".

(c) TECHNICAL CORRECTION.—Section 46103(c)(3) of title 46, United States Code, as so redesignated, is amended by striking "555b(c)" and inserting "552b(c)".

DIVISION H—OTHER MATTERS

TITLE XC—HOMELAND SECURITY MATTERS

Sec. 9001. Department of Homeland Security CISA Director.
Sec. 9002. Sector risk management agencies.

SEC. 9001. DEPARTMENT OF HOMELAND SECURITY CISA DIRECTOR.

(a) IN GENERAL.—Subsection (b) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended by—

(1) redesignating paragraph (2) as paragraph (3); and

(2) inserting after paragraph (1) the following new paragraph:

"(2) QUALIFICATIONS.—

Appointment.

"(A) IN GENERAL.—The Director shall be appointed from among individuals who have—

"(i) extensive knowledge in at least two of the areas specified in subparagraph (B); and

"(ii) not fewer than five years of demonstrated experience in efforts to foster coordination and collaboration between the Federal Government, the private sector, and other entities on issues related to cybersecurity, infrastructure security, or security risk management.

"(B) SPECIFIED AREAS.—The areas specified in this subparagraph are the following:

"(i) Cybersecurity.

"(ii) Infrastructure security.

"(iii) Security risk management.".

(b) AMENDMENT TO POSITION LEVEL OF CISA DIRECTOR.—Subchapter II of chapter 53 of title 5, United States Code, is amended—

(1) in section 5313, by inserting after "Administrator of the Transportation Security Administration." the following:

"Director, Cybersecurity and Infrastructure Security Agency."; and

(2) in section 5314, by striking "Director, Cybersecurity and Infrastructure Security Agency.".

(c) EXECUTIVE ASSISTANT DIRECTOR FOR CYBERSECURITY.—

(1) IN GENERAL.—Section 2203 of the Homeland Security Act of 2002 (6 U.S.C. 653) is amended—

(A) in subsection (a)—

(i) in paragraph (2)—

(I) in the heading, by striking "ASSISTANT DIRECTOR.—" and inserting "EXECUTIVE ASSISTANT DIRECTOR.—"; and

(II) in the matter preceding subparagraph (A)—

(aa) by striking "Assistant Director for Cybersecurity" and inserting "Executive Assistant Director for Cybersecurity"; and

(bb) by striking "the 'Assistant Director' and inserting 'the Executive Assistant Director'"; and

(ii) in paragraph (3)—

(I) by inserting "or Assistant Director for Cybersecurity" after "Assistant Secretary for Cybersecurity and Communications"; and

(II) by striking "Assistant Director for Cybersecurity." and inserting "Executive Assistant Director for Cybersecurity."; and

(B) in subsection (b), in the matter preceding paragraph (1), by striking "Assistant Director" and inserting "Executive Assistant Director".

(2) CONTINUATION IN OFFICE.—The individual serving as the Assistant Director for Cybersecurity of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security on the day before the date of enactment of this Act may serve as the Executive Assistant Director for Cybersecurity on and after that date without the need for renomination or reappointment. 6 USC 653 note.

(d) EXECUTIVE ASSISTANT DIRECTOR FOR INFRASTRUCTURE SECURITY.—

(1) IN GENERAL.—Section 2204 of the Homeland Security Act of 2002 (6 U.S.C. 654) is amended—

(A) in subsection (a)—

(i) in paragraph (2)—

(I) in the heading, by striking "ASSISTANT DIRECTOR.—" and inserting "EXECUTIVE ASSISTANT DIRECTOR.—"; and

(II) in the matter preceding subparagraph (A)—

(aa) by striking "Assistant Director for Infrastructure Security" and inserting "Executive Assistant Director for Infrastructure Security"; and

(bb) by striking "the 'Assistant Director' and inserting 'the Executive Assistant Director'"; and

(ii) in paragraph (3)—

(I) by inserting "or Assistant Director for Infrastructure Security" after "Assistant Secretary for Infrastructure Protection"; and

(II) by striking "Assistant Director for Infrastructure Security." and inserting "Executive Assistant Director for Infrastructure Security."; and

(B) in subsection (b), by striking "Assistant Director" in the matter preceding paragraph (1) and inserting "Executive Assistant Director".

(2) CONTINUATION IN OFFICE.—The individual serving as the Assistant Director for Infrastructure Security of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security on the day before the date of enactment of this Act may serve as the Executive Assistant Director for Infrastructure Security on and after that date without the need for renomination or reappointment. 6 USC 654 note.

(e) EXECUTIVE ASSISTANT DIRECTOR FOR EMERGENCY COMMUNICATIONS.—

(1) IN GENERAL.—Section 1801 of the Homeland Security Act of 2002 (6 U.S.C. 571) is amended—

(A) in subsection (b)—

(i) in the heading, by striking "ASSISTANT DIRECTOR.—" and inserting "EXECUTIVE ASSISTANT DIRECTOR.—";

(ii) in the first sentence, by striking "Assistant Director for Emergency Communications." and inserting "Executive Assistant Director for Emergency Communications (in this section referred to as the 'Executive Assistant Director')."; and

(iii) in the second and third sentences, by striking "Assistant Director" both places such term appears and inserting "Executive Assistant Director"; and

(B) in subsection (c), in the matter preceding paragraph (1), by striking "Assistant Director for Emergency Communications" and inserting "Executive Assistant Director";

(C) in subsection (d), in the matter preceding paragraph (1), by striking "Assistant Director for Emergency Communications" and inserting "Executive Assistant Director";

(D) in subsection (e), in the matter preceding paragraph (1), by striking "Assistant Director for Emergency Communications" and inserting "Executive Assistant Director"; and

(E) by adding at the end the following new subsection:

"(g) REFERENCE.—Any reference to the Assistant Director for Emergency Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Executive Assistant Director for Emergency Communications.".

6 USC 571 note.

(2) CONTINUATION IN OFFICE.—The individual serving as the Assistant Director for Emergency Communications of the Department of Homeland Security on the day before the date of enactment of this Act may serve as the Executive Assistant Director for Emergency Communications on and after that date.

6 USC 652a.

SEC. 9002. SECTOR RISK MANAGEMENT AGENCIES.

(a) DEFINITIONS.—In this section:

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

(A) the Committee on Homeland Security and the Committee on Armed Services in the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services in the Senate.

(2) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(3) DEPARTMENT.—The term "Department" means the Department of Homeland Security.

(4) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency of the Department.

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "information sharing and analysis organization" has the meaning given that term in section 2222(5) of the Homeland Security Act of 2002 (6 U.S.C. 671(5)).

(6) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

(7) SECTOR RISK MANAGEMENT AGENCY.—The term "sector risk management agency" has the meaning given the term

"Sector-Specific Agency" in section 2201(5) of the Homeland Security Act of 2002 (6 U.S.C. 651(5)).

(b) CRITICAL INFRASTRUCTURE SECTOR DESIGNATION.—

(1) INITIAL REVIEW.—Not later than 180 days after the date of the enactment of this section, the Secretary, in consultation with the heads of Sector Risk Management Agencies, shall— Deadline.

(A) review the current framework for securing critical infrastructure, as described in section 2202(c)(4) of the Homeland Security Act (6 U.S.C. 652(c)(4)) and Presidential Policy Directive 21; and

(B) submit to the President and appropriate congressional committees a report that includes— Reports. Recommendations.

(i) information relating to—

(I) the analysis framework or methodology used to— Analysis.

(aa) evaluate the current framework for securing critical infrastructure referred to in subparagraph (A); and Evaluation.

(bb) develop recommendations to—

(AA) revise the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(BB) identify and designate any subsectors of such sectors;

(II) the data, metrics, and other information used to develop the recommendations required under clause (ii); and Data.

(ii) recommendations relating to—

(I) revising— Lists.

(aa) the current framework for securing critical infrastructure referred to in subparagraph (A);

(bb) the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(cc) the identification and designation of any subsectors of such sectors; and

(II) any revisions to the list of designated Federal departments or agencies that serve as the Sector Risk Management Agency for a sector or subsector of such section, necessary to comply with paragraph (3)(B).

(2) PERIODIC EVALUATION BY THE SECRETARY.—At least once every five years, the Secretary, in consultation with the Director and the heads of Sector Risk Management Agencies, shall— Consultation.

(A) evaluate the current list of designated critical infrastructure sectors and subsectors of such sectors and the appropriateness of Sector Risk Management Agency designations, as set forth in Presidential Policy Directive 21, any successor or related document, or policy; and

(B) recommend, as appropriate, to the President— Recommendation.

List.

(i) revisions to the current list of designated critical infrastructure sectors or subsectors of such sectors; and

(ii) revisions to the designation of any Federal department or agency designated as the Sector Risk Management Agency for a sector or subsector of such sector.

Deadline.

(3) REVIEW AND REVISION BY THE PRESIDENT.—Not later than 180 days after the Secretary submits a recommendation pursuant to paragraph (1) or (2), the President shall—

(A) review the recommendation and revise, as appropriate, the designation of a critical infrastructure sector or subsector or the designation of a Sector Risk Management Agency; and

Reports.

(B) submit to the appropriate congressional committees, the Majority and Minority Leaders of the Senate, and the Speaker and Minority Leader of the House of Representatives, a report that includes—

(i) an explanation with respect to the basis for accepting or rejecting the recommendations of the Secretary; and

Analysis.

(ii) information relating to the analysis framework, methodology, metrics, and data used to—

Evaluation.

(I) evaluate the current framework for securing critical infrastructure referred to in paragraph (1)(A); and

Recommendations.

(II) develop—

(aa) recommendations to revise—

List.

(AA) the list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(BB) the designation of any subsectors of such sectors; and

(bb) the recommendations of the Secretary.

Federal Register, publication.

(4) PUBLICATION.—Any designation of critical infrastructure sectors shall be published in the Federal Register.

(c) SECTOR RISK MANAGEMENT AGENCIES.—

(1) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 is amended by adding at the end the following new section:

Coordination.
6 USC 665d.

"SEC. 2215. SECTOR RISK MANAGEMENT AGENCIES.

"(a) IN GENERAL.—Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency, in coordination with the Director, shall—

"(1) provide specialized sector-specific expertise to critical infrastructure owners and operators within its designated critical infrastructure sector or subsector of such sector; and

"(2) support programs and associated activities of such sector or subsector of such sector.

"(b) IMPLEMENTATION.—In carrying out this section, Sector Risk Management Agencies shall—

"(1) coordinate with the Department and, as appropriate, other relevant Federal departments and agencies;

"(2) collaborate with critical infrastructure owners and operators within the designated critical infrastructure sector or subsector of such sector; and

"(3) coordinate with independent regulatory agencies, and State, local, Tribal, and territorial entities, as appropriate.

"(c) RESPONSIBILITIES.—Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency shall utilize its specialized expertise regarding its designated critical infrastructure sector or subsector of such sector and authorities under applicable law to—

"(1) support sector risk management, in coordination with the Director, including—

"(A) establishing and carrying out programs to assist critical infrastructure owners and operators within the designated sector or subsector of such sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector of such sector; and

"(B) recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets;

"(2) assess sector risk, in coordination with the Director, including—

"(A) identifying, assessing, and prioritizing risks within the designated sector or subsector of such sector, considering physical security and cybersecurity threats, vulnerabilities, and consequences; and

"(B) supporting national risk assessment efforts led by the Department;

"(3) sector coordination, including—

"(A) serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title;

"(B) serving as the Federal Government coordinating council chair for the designated sector or subsector of such sector; and

"(C) participating in cross-sector coordinating councils, as appropriate;

"(4) facilitating, in coordination with the Director, the sharing with the Department and other appropriate Federal department of information regarding physical security and cybersecurity threats within the designated sector or subsector of such sector, including—

"(A) facilitating, in coordination with the Director, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through information sharing and analysis organizations and the national cybersecurity and communications integration center established pursuant to section 2209;

"(B) facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of such sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate;

"(C) providing the Director, and facilitating awareness within the designated sector or subsector of such sector, of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector; and

"(D) supporting the reporting requirements of the Department under applicable law by providing, on an annual basis, sector-specific critical infrastructure information;

"(5) supporting incident management, including—

"(A) supporting, in coordination with the Director, incident management and restoration efforts during or following a security incident; and

"(B) supporting the Director, upon request, in national cybersecurity asset response activities for critical infrastructure; and

"(6) contributing to emergency preparedness efforts, including—

"(A) coordinating with critical infrastructure owners and operators within the designated sector or subsector of such sector and the Director in the development of planning documents for coordinated action in the event of a natural disaster, act of terrorism, or other man-made disaster or emergency;

"(B) participating in and, in coordination with the Director, conducting or facilitating, exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector or subsector of such sector; and

"(C) supporting the Department and other Federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector or subsector or such sector.".

(2) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 is amended—

6 USC 195f.

(A) in section 320—

(i) in subsection (d)(3)(C), by striking "Sector-Specific Agency" and inserting "Sector Risk Management Agency"; and

(ii) in subsection (e)(1), by striking "Sector-Specific Agency" and inserting "Sector Risk Management Agency";

6 USC 321m.

(B) in section 524—

(i) in subsection (b)(2)(E)(i)(II), by striking "sector-specific agency" and inserting "Sector Risk Management Agency"; and

(ii) in subsection (c)(1)(B), by striking "sector-specific agency" and inserting "Sector Risk Management Agency";

6 USC 651.

(C) in section 2201(5)—

(i) in the paragraph heading, by striking "SECTOR-SPECIFIC AGENCY" and inserting "SECTOR RISK MANAGEMENT AGENCY"; and

(ii) by striking "Sector-Specific Agency" and inserting "Sector Risk Management Agency";

(D) in section 2202(i), by striking "Sector-Specific Agency" and inserting "Sector Risk Management Agency"; and 6 USC 652.

(E) in section 2214(c)(4), by striking "sector-specific agency" and inserting "Sector Risk Management Agency". 6 USC 664.

(3) REFERENCES.—Any reference to a Sector Specific Agency (including any permutations or conjugations thereof) in any law, regulation, map, document, record, or other paper of the United States shall be deemed to—

(A) be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector; and

(B) have the meaning give such term in section 2201(5) of the Homeland Security Act of 2002.

(4) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2214 the following new item:

"Sec. 2215. Sector Risk Management Agencies.".

(d) REPORT AND AUDITING.—Not later than two years after the date of the enactment of this Act and every four years thereafter for 12 years, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the effectiveness of Sector Risk Management Agencies in carrying out their responsibilities under section 2215 of the Homeland Security Act of 2002, as added by this section. Time period.

SEC. 9003. REVIEW AND ANALYSIS OF INLAND WATERS SEAPORT SECURITY.

(a) SEAPORT CARGO REVIEW.—

(1) ELEMENTS.—The Secretary of Homeland Security shall conduct a review of all Great Lakes and selected inland waters seaports that receive international cargo—

(A) to determine, for each such seaport— Determination.

(i) the current screening capability, including the types and numbers of screening equipment and whether such equipment is physically located at a seaport or assigned and available in the area and made available to use;

(ii) the number of U.S. Customs and Border Protection personnel assigned from a Field Operations office, broken out by role;

(iii) the expenditures for procurement and overtime incurred by U.S. Customs and Border Protection during the most recent fiscal year;

(iv) the types of cargo received, such as containerized, break-bulk, and bulk;

(v) the legal entity that owns the seaport;

(vi) a description of the use of space at the seaport by U.S. Customs and Border Protection, including—

(I) whether U.S. Customs and Border Protection or the General Services Administration owns or leases any facilities at the seaport; and

(II) if U.S. Customs and Border Protection is provided space at the seaport, a description of

such space, including the number of workstations; and

(vii) the current cost-sharing arrangement for screening technology or reimbursable services;

(B) to identify, for each Field Operations office—

(i) any ports of entry that are staffed remotely from service ports;

(ii) the distance of each such service port from the corresponding ports of entry; and

(iii) the number of officers and the types of equipment U.S. Customs and Border Protection uses to screen cargo entering or exiting through such ports; and

Assessment.

(C) that includes a threat assessment of incoming containerized and noncontainerized cargo at Great Lakes seaports and selected inland waters seaports.

(2) SEAPORT SELECTION.—In selecting seaports on inland waters to include in the review under paragraph (1), the Secretary of Homeland Security shall ensure that the inland waters seaports are—

(A) equal in number to the Great Lakes seaports included in the review;

(B) comparable to Great Lakes seaports included in the review, as measured by number of imported shipments arriving at the seaport each year; and

(C) covered by at least the same number of Field Operations offices as the Great Lakes seaports included in the review, but are not covered by the same Field Operations offices as such Great Lakes seaports.

(3) REPORT REQUIRED.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the appropriate congressional committees a report containing—

(i) the results of the review conducted pursuant to paragraph (1); and

(ii) an explanation of the methodology used for such review regarding the screening practices for foreign cargo arriving at seaports on the Great Lakes and inland waters.

Classified information.

(B) FORM.—The report required under subparagraph (A) shall be submitted in unclassified form, to the maximum extent possible, but may include a classified annex, if necessary.

(b) INLAND WATERS THREAT ANALYSIS.—

Deadline.

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the appropriate congressional committees an inland waters threat analysis containing an identification and description of—

(A) current and potential terrorism and criminal threats posed by individuals and groups seeking—

(i) to enter the United States through inland waters; or

(ii) to exploit security vulnerabilities on inland waters;

(B) security challenges at inland waters ports of the United States regarding—

(i) terrorism and instruments of terror entering the United States; or

(ii) criminal activity, as measured by the total flow of illegal goods and illicit drugs, related to the inland waters;

(C) security mitigation efforts with respect to the inland waters—

(i) to prevent terrorists and instruments of terror from entering the United States; or

(ii) to reduce criminal activity related to the inland waters;

(D) vulnerabilities related to cooperation between State, local, tribal, and territorial law enforcement, or international agreements, that hinder effective security, counterterrorism, anti-trafficking efforts, and the flow of legitimate trade with respect to inland waters; and

(E) metrics and performance measures used by the Secretary of Homeland Security to evaluate inland waters security, as appropriate.

(2) ANALYSIS REQUIREMENTS.—In preparing the threat analysis required under paragraph (1), the Secretary of Homeland Security shall consider and examine— Examination.

(A) technology needs and challenges;

(B) personnel needs and challenges;

(C) the roles of State, local, tribal, and territorial law enforcement, private sector partners, and the public, relating to inland waters security;

(D) the need for cooperation among Federal, State, local, tribal, territorial, and international partner law enforcement, private sector partners, and the public, relating to inland waters security; and

(E) the challenges posed by geography with respect to inland waters security.

(3) FORM.—The Secretary of Homeland Security shall submit the threat analysis required under paragraph (1) in unclassified form, to the maximum extent possible, but may include a classified annex, if necessary. Classified information.

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

(1) the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives; and

(2) the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate.

SEC. 9004. DEPARTMENT OF HOMELAND SECURITY REPORTS ON DIGITAL CONTENT FORGERY TECHNOLOGY.

(a) REPORTS REQUIRED.—Not later than one year after the date of enactment of this Act, and annually thereafter for 5 years, the Secretary of Homeland Security, acting through the Under Time period. Consultation.

Secretary for Science and Technology of the Department of Homeland Security, and with respect to paragraphs (6) and (7) of subsection (b), in consultation with the Director of National Intelligence, shall submit to Congress a report on the state of digital content forgery technology.

Assessments.

(b) CONTENTS.—Each report produced under subsection (a) shall include the following:

(1) An assessment of the underlying technologies used to create or propagate digital content forgeries, including the evolution of such technologies and patterns of dissemination of such technologies.

(2) A description of the types of digital content forgeries, including those used to commit fraud, cause harm, harass, coerce, or silence vulnerable groups or individuals, or violate civil rights recognized under Federal law.

(3) An assessment of how foreign governments, and the proxies and networks thereof, use, or could use, digital content forgeries to harm national security.

(4) An assessment of how non-governmental entities in the United States use, or could use, digital content forgeries.

(5) An assessment of the uses, applications, dangers, and benefits, including the impact on individuals, of deep learning or digital content forgery technologies used to generate realistic depictions of events that did not occur.

Analysis. Determination. Recommendations.

(6) An analysis of the methods used to determine whether content is created by digital content forgery technology, and an assessment of any effective heuristics used to make such a determination, as well as recommendations on how to identify and address suspect content and elements to provide warnings to users of such content.

(7) A description of the technological countermeasures that are, or could be, used to address concerns with digital content forgery technology.

(8) Any additional information the Secretary determines appropriate.

(c) CONSULTATION AND PUBLIC HEARINGS.—In producing each report required under subsection (a), the Secretary may—

(1) consult with any other agency of the Federal Government that the Secretary considers necessary; and

(2) conduct public hearings to gather, or otherwise allow interested parties an opportunity to present, information and advice relevant to the production of the report.

Classified information.

(d) FORM OF REPORT.—Each report required under subsection (a) shall be produced in unclassified form, but may contain a classified annex.

(e) APPLICABILITY OF OTHER LAWS.—

(1) FOIA.—Nothing in this section, or in a report produced under this section, may be construed to allow the disclosure of information or a record that is exempt from public disclosure under section 552 of title 5, United States Code (commonly known as the "Freedom of Information Act").

(2) PAPERWORK REDUCTION ACT.—Subchapter I of chapter 35 of title 44, United States Code (commonly known as the "Paperwork Reduction Act"), shall not apply to this section.

(f) DIGITAL CONTENT FORGERY DEFINED.—In this section, the term "digital content forgery technology" means the use of emerging technologies, including artificial intelligence and machine learning

techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead.

SEC. 9005. GAO STUDY OF CYBERSECURITY INSURANCE.

(a) STUDY.—The Comptroller General of the United States shall conduct a study to assess and analyze the state and availability of insurance coverage in the United States for cybersecurity risks, including by— Assessment. Analysis.

(1) identifying the number and dollar volume of cyber insurance policies currently in force and the percentage of businesses, and specifically small businesses, that have cyber insurance coverage;

(2) assessing the extent to which States have established minimum standards for the scope of cyber insurance policies; and

(3) identifying any barriers to modeling and underwriting cybersecurity risks.

(b) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General shall submit to Congress a report setting forth the findings and conclusions of the study conducted under subsection (a), including—

(1) recommendations on whether intervention by the Federal Government would help facilitate the growth and development of insurers offering coverage for cybersecurity risks; and Recommendations.

(2) a discussion of the availability and affordability of such coverage and policyholder education regarding such coverage.

SEC. 9006. STRATEGY TO SECURE EMAIL.

Recommendations. Deadline. Standards.

(a) IN GENERAL.—Not later than December 31, 2021, the Secretary of Homeland Security shall develop and submit to Congress a strategy, including recommendations, to implement across all United States-based email providers Domain-based Message Authentication, Reporting, and Conformance standard at scale.

(b) ELEMENTS.—The strategy required under subsection (a) shall include the following:

(1) A recommendation for the minimum-size threshold for United States-based email providers for applicability of Domain-based Message Authentication, Reporting, and Conformance.

(2) A description of the security and privacy benefits of implementing the Domain-based Message Authentication, Reporting, and Conformance standard at scale, including recommendations for national security exemptions, as appropriate, as well as the burdens of such implementation and an identification of the entities on which such burdens would most likely fall.

(3) An identification of key United States and international stakeholders associated with such implementation.

(4) An identification of any barriers to such implementation, including a cost-benefit analysis where feasible.

(5) An initial estimate of the total cost to the Federal Government and implementing entities in the private sector of such implementation, including recommendations for defraying such costs, if applicable. Cost estimate.

(c) CONSULTATION.—In developing the strategy and recommendations under subsection (a), the Secretary of Homeland Security may, as appropriate, consult with representatives from the information technology sector.

(d) DEFINITION.—In this section, the term "Domain-based Message Authentication, Reporting, and Conformance" means an email authentication, policy, and reporting protocol that verifies the authenticity of the sender of an email and blocks and reports to the sender fraudulent accounts.

SEC. 9007. DEPARTMENT OF HOMELAND SECURITY LARGE-SCALE NON-INTRUSIVE INSPECTION SCANNING PLAN.

Deadline.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a plan for increasing to 100 percent the rate of high-throughput scanning of commercial and passenger vehicles and freight rail traffic entering the United States at land ports of entry and rail-border crossings along the border using large-scale non-intrusive inspection systems or similar technology to enhance border security.

(b) BASELINE INFORMATION.—The plan under subsection (a) shall include, at a minimum, the following information regarding large-scale non-intrusive inspection systems or similar technology operated by U.S. Customs and Border Protection at land ports of entry and rail-border crossings as of the date of the enactment of this Act:

Inventory.

(1) An inventory of large-scale non-intrusive inspection systems or similar technology in use at each land port of entry.

(2) For each system or technology identified in the inventory under paragraph (1)—

(A) the scanning method of such system or technology;

(B) the location of such system or technology at each land port of entry that specifies whether in use in pre-primary, primary, or secondary inspection area, or some combination of such areas;

(C) the percentage of commercial and passenger vehicles and freight rail traffic scanned by such system or technology;

(D) seizure data directly attributed to scanned commercial and passenger vehicles and freight rail traffic; and

(E) the number of personnel required to operate each system or technology.

(3) Information regarding the continued use of other technology and tactics used for scanning, such as canines and human intelligence in conjunction with large scale, nonintrusive inspection systems.

(c) ELEMENTS.—The plan under subsection (a) shall include the following elements:

Deadline.

(1) Benchmarks for achieving incremental progress towards 100 percent high-throughput scanning within the next 6 years of commercial and passenger vehicles and freight rail traffic entering the United States at land ports of entry and rail-border crossings along the border with corresponding projected incremental improvements in scanning rates by fiscal year and rationales for the specified timeframes for each land port of entry.

Cost estimates.

(2) Estimated costs, together with an acquisition plan, for achieving the 100 percent high-throughput scanning rate within the timeframes specified in paragraph (1), including acquisition,

operations, and maintenance costs for large-scale, nonintrusive inspection systems or similar technology, and associated costs for any necessary infrastructure enhancements or configuration changes at each port of entry. Such acquisition plan shall promote, to the extent practicable, opportunities for entities that qualify as small business concerns (as defined under section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

(3) Any projected impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on the total number of commercial and passenger vehicles and freight rail traffic entering at land ports of entry and rail-border crossings where such systems are in use, and average wait times at peak and non-peak travel times, by lane type if applicable, as scanning rates are increased.

(4) Any projected impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on land ports of entry and rail-border crossings border security operations as a result of implementation actions, including any changes to the number of U.S. Customs and Border Protection officers or their duties and assignments.

(d) ANNUAL REPORT.—Not later than one year after the submission of the plan under subsection (a), and biennially thereafter for the following six years, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that describes the progress implementing the plan and includes— Time period.

(1) an inventory of large-scale, nonintrusive inspection systems or similar technology operated by U.S. Customs and Border Protection at each land port of entry; Inventory.

(2) for each system or technology identified in the inventory required under paragraph (1)—

(A) the scanning method of such system or technology;

(B) the location of such system or technology at each land port of entry that specifies whether in use in pre-primary, primary, or secondary inspection area, or some combination of such areas;

(C) the percentage of commercial and passenger vehicles and freight rail traffic scanned by such system or technology; and

(D) seizure data directly attributed to scanned commercial and passenger vehicles and freight rail traffic;

(3) the total number of commercial and passenger vehicles and freight rail traffic entering at each land port of entry at which each system or technology is in use, and information on average wait times at peak and non-peak travel times, by lane type if applicable;

(4) a description of the progress towards reaching the benchmarks referred to in subsection (c)(1), and an explanation if any of such benchmarks are not achieved as planned;

(5) a comparison of actual costs (including information on any awards of associated contracts) to estimated costs set forth in subsection (c)(2);

(6) any realized impacts, as identified by the Commissioner of U.S. Customs and Border Protection, on land ports of entry and rail-border crossings operations as a result of implementation actions, including any changes to the number of U.S.

Customs and Border Protection officers or their duties and assignments;

(7) any proposed changes to the plan and an explanation for such changes, including changes made in response to any Department of Homeland Security research and development findings or changes in terrorist or transnational criminal organizations tactics, techniques, or procedures; and

(8) any challenges to implementing the plan or meeting the benchmarks, and plans to mitigate any such challenges.

(e) DEFINITIONS.—In this section:

(1) The term "large-scale, non-intrusive inspection system" means a technology, including x-ray, gamma-ray, and passive imaging systems, capable of producing an image of the contents of a commercial or passenger vehicle or freight rail car in 1 pass of such vehicle or car.

(2) The term "scanning" means utilizing nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a commercial or passenger vehicle or freight rail car.

TITLE XCI—VETERANS AFFAIRS MATTERS

SEC. 9101. MODIFICATION OF LICENSURE REQUIREMENTS FOR DEPARTMENT OF VETERANS AFFAIRS HEALTH CARE PROFESSIONALS PROVIDING TREATMENT VIA TELEMEDICINE.

Section 1730C(b) of title 38, United States Code, is amended to read as follows:

"(b) COVERED HEALTH CARE PROFESSIONALS.—For purposes of this section, a covered health care professional is any of the following individuals:

"(1) A health care professional who—

"(A) is an employee of the Department appointed under section 7306, 7401, 7405, 7406, or 7408 of this title or under title 5;

"(B) is authorized by the Secretary to provide health care under this chapter;

"(C) is required to adhere to all standards for quality relating to the provision of health care in accordance with applicable policies of the Department; and

"(D)(i) has an active, current, full, and unrestricted license, registration, or certification in a State to practice

the health care profession of the health care professional; or

"(ii) with respect to a health care profession listed under section 7402(b) of this title, has the qualifications for such profession as set forth by the Secretary.

"(2) A postgraduate health care employee who—

"(A) is appointed under section 7401(1), 7401(3), or 7405 of this title or title 5 for any category of personnel described in paragraph (1) or (3) of section 7401 of this title;

"(B) must obtain an active, current, full, and unrestricted license, registration, or certification or meet qualification standards set forth by the Secretary within a specified time frame; and

"(C) is under the clinical supervision of a health care professional described in paragraph (1); or

"(3) A health professions trainee who—

"(A) is appointed under section 7405 or 7406 of this title; and

"(B) is under the clinical supervision of a health care professional described in paragraph (1).".

SEC. 9102. ADDITIONAL CARE FOR NEWBORN CHILDREN OF VETERANS.

Section 1786 of title 38, United States Code, is amended—

(1) in subsection (a), by striking "The Secretary" and inserting "Except as provided in subsection (c), the Secretary"; and

(2) by adding at the end the following new subsection:

"(c) EXCEPTION BASED ON MEDICAL NECESSITY.—Pursuant to such regulations as the Secretary shall prescribe to carry out this section, the Secretary may furnish more than seven days of health care services described in subsection (b), and may furnish transportation necessary to receive such services, to a newborn child based on medical necessity if the child is in need of additional care, including if the child has been discharged or released from a hospital and requires readmittance to ensure the health and welfare of the child.". Regulations.

SEC. 9103. EXPANSION OF ELIGIBILITY FOR HUD–VASH.

(a) HUD PROVISIONS.—Section 8(o)(19) of the United States Housing Act of 1937 (42 U.S.C. 1437f(o)(19)) is amended by adding at the end the following new subparagraph:

"(D) VETERAN DEFINED.—In this paragraph, the term 'veteran' has the meaning given that term in section 2002(b) of title 38, United States Code.".

(b) VHA CASE MANAGERS.—Subsection (b) of section 2003 of title 38, United States Code, is amended by adding at the end the following: "In the case of vouchers provided under the HUD–VASH program under section 8(o)(19) of such Act, for purposes of the preceding sentence, the term 'veteran' shall have the meaning given such term in section 2002(b) of this title.". Definition.

(c) ANNUAL REPORTS.—

(1) IN GENERAL.—Not less frequently than once each year, the Secretary of Veterans Affairs shall submit to the Committee on Veterans' Affairs of the Senate and the Committee on Veterans' Affairs of the House of Representatives a report on the homelessness services provided under programs of the Department of Veterans Affairs, including services under HUD– 38 USC 2001 note.

VASH program under section 8(o)(19) of the United States Housing Act of 1937 (42 U.S.C. 1437f(o)(19)).

(2) INCLUDED INFORMATION.—Each such annual report shall include, with respect to the year preceding the submittal of the report, a statement of the number of eligible individuals who were furnished such homelessness services and the number of individuals furnished such services under each such program, disaggregated by the number of men who received such services and the number of women who received such services, and such other information as the Secretary considers appropriate.

SEC. 9104. STUDY ON UNEMPLOYMENT RATE OF WOMEN VETERANS WHO SERVED ON ACTIVE DUTY IN THE ARMED FORCES AFTER SEPTEMBER 11, 2001.

(a) STUDY.—

Deadline. Consultation.

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Veterans Affairs, in consultation with the Bureau of Labor Statistics of the Department of Labor, shall conduct a study on why post-9/11 veterans who are women are at higher risk of unemployment than all other groups of women veterans and their non-veteran counterparts.

(2) CONDUCT OF STUDY.—

(A) IN GENERAL.—The Secretary shall conduct the study under paragraph (1) through the Center for Women Veterans under section 318 of title 38, United States Code.

(B) CONSULTATION.—In carrying out the study conducted under paragraph (1), the Secretary may consult with—

(i) the Department of Labor;

(ii) other Federal agencies, including the Department of Defense, the Office of Personnel Management, and the Small Business Administration;

(iii) foundations; and

(iv) other entities in the private sector.

Analysis.

(3) ELEMENTS OF STUDY.—The study conducted under paragraph (1) shall include, with respect to post-9/11 veterans who are women, an analysis of each of the following:

(A) Rank at the time of separation from the Armed Forces.

(B) Geographic location of residence upon such separation.

(C) Highest level of education achieved as of the time of such separation.

(D) The percentage of such veterans who enrolled in a program of education or an employment training program of the Department of Veterans Affairs or the Department of Labor after such separation.

(E) Industries that have employed such veterans.

(F) Military occupational specialties of such veterans while serving as members of the Armed Forces.

(G) Barriers to employment of such veterans.

(H) Causes of the fluctuations in employment of such veterans.

(I) Employment training programs of the Department of Veterans Affairs or the Department of Labor that are

available to such veterans as of the date of the enactment of this Act.

(J) Economic indicators that affect the unemployment of such veterans.

(K) Health conditions of such veterans that could affect employment.

(L) Whether there are differences in the analyses conducted under subparagraphs (A) through (K) depending on the race of such veterans.

(M) The difference between unemployment rates of post-9/11 veterans who are women compared to unemployment rates of post-9/11 veterans who are men, including an analysis of potential causes of such difference.

(N) Such other matters as the Secretary determines appropriate.

(b) REPORT.—

(1) IN GENERAL.—Not later than 90 days after completing the study under subsection (a), the Secretary shall submit to the Committee on Veterans' Affairs of the Senate and the Committee on Veterans' Affairs of the House of Representatives a report on such study.

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

(A) The analysis conducted under subsection (a)(3).

(B) A description of the methods used to conduct the study under subsection (a).

(C) Such other matters relating to the unemployment rates of post-9/11 veterans who are women as the Secretary considers appropriate.

(c) POST-9/11 VETERAN DEFINED.—In this section, the term "post-9/11 veteran" means a veteran who served on active duty in the Armed Forces on or after September 11, 2001.

SEC. 9105. ACCESS OF VETERANS TO INDIVIDUAL LONGITUDINAL EXPOSURE RECORD.

Website.
38 USC 527 note.

The Secretary of Veterans Affairs shall provide to a veteran read-only access to the documents of the veteran contained in the Individual Longitudinal Exposure Record in a printable format through a portal accessible through an internet website of the Department of Veterans Affairs.

SEC. 9106. DEPARTMENT OF VETERANS AFFAIRS REPORT ON UNDISBURSED FUNDS.

(a) REPORT REQUIRED.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Veterans Affairs shall submit to the Committees on Veterans' Affairs of the Senate and House of Representatives a report on the undisbursed funds of the Department of Veterans Affairs.

(b) ELEMENTS.—The report required under subsection (a) shall include each of the following:

(1) The total quantities and value, for each of the preceding ten fiscal years, of— Time period.

(A) the undisbursed funds in the possession of the Department; and

(B) the undisbursed funds of the Department that were transferred to the Department of Treasury.

Procedures.

(2) The policies and procedures of the Department for managing undisbursed funds and for communicating with veterans, other beneficiaries, and heirs regarding undisbursed funds.

Plans.

(3) The challenges regarding the policies and procedures identified under paragraph (2), any legal barriers to improving such policies and procedures, and the plans of the Secretary for improvement.

(c) REVIEW OF REPORT.—The Comptroller General of the United States shall conduct a review of the report submitted under subsection (a).

(d) UNDISBURSED FUNDS DEFINED.—The term "undisbursed funds"—

(1) means any amount of money that is owed to a beneficiary and that has not been disbursed—

(A) in the case of an amount that is owed by reason of an insurance benefit under chapter 19 of title 38, United States Code, for a period of one year or longer; or

(B) in the case of an amount that is owed by reason of any other benefit under the laws administered by the Secretary of Veterans Affairs, for a period of 30 days or longer; and

(2) does not include any amount of money that—

(A) has not been disbursed due to a contested claim for benefits under the laws administered by the Secretary; or

(B) is in dispute by two or more parties over who is the entitled beneficiary.

California.
38 USC 2400 note.

SEC. 9107. TRANSFER OF MARE ISLAND NAVAL CEMETERY TO SECRETARY OF VETERANS AFFAIRS FOR MAINTENANCE BY NATIONAL CEMETERY ADMINISTRATION.

Contracts.
Effective date.

(a) AGREEMENT.—Beginning on the date that is 180 days after the date on which the Secretary submits the report required by subsection (c)(1), the Secretary of Veterans Affairs shall seek to enter into an agreement with the city of Vallejo, California, under which the city of Vallejo shall transfer to the Secretary all right, title, and interest in the Mare Island Naval Cemetery in Vallejo, California, at no cost to the Secretary. The Secretary shall seek to enter into such agreement before the date that is one year after the date on which such report is submitted.

(b) MAINTENANCE BY NATIONAL CEMETERY ADMINISTRATION.—If the Mare Island Naval Cemetery is transferred to the Secretary of Veterans Affairs pursuant to subsection (a), the National Cemetery Administration shall maintain the cemetery in the same manner as other cemeteries under the jurisdiction of the National Cemetery Administration.

(c) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the Committee on Veterans' Affairs of the Senate and the Committee on Veterans' Affairs of the House of Representatives a report on the feasibility and advisability of exercising the authority to enter into an agreement under subsection (a).

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

Assessment.

(A) An assessment of the feasibility and advisability of entering into such an agreement.

(B) An estimate of the costs, including both direct and indirect costs, that the Department of Veterans Affairs would incur by entering into such an agreement. Cost estimates.

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

(1) it is only potentially advisable and feasible to transfer the Mare Island Naval Cemetery from the city of Vallejo, California, to the Department of Veterans Affairs because the cemetery was previously under the control of the Department of Defense; and

(2) the City of Vallejo should provide in-kind non-monetary contributions for the improvement and maintenance of Mare Island Naval Cemetery, including labor and equipment, to the extent practicable, to the Department of Veterans Affairs, following any transfer of the cemetery to the Department.

SEC. 9108. COMPTROLLER GENERAL REPORT ON DEPARTMENT OF VETERANS AFFAIRS HANDLING OF DISABILITY COMPENSATION CLAIMS BY CERTAIN VETERANS.

Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report containing an evaluation of how the Department of Veterans Affairs has handled claims for disability compensation under the laws administered by the Secretary of Veterans Affairs submitted by veterans who—

(1) have type 1 diabetes; and

(2) have been exposed to an herbicide agent (as defined in section 1116(a)(3) of title 38, United States Code).

SEC. 9109. ADDITIONAL DISEASES ASSOCIATED WITH EXPOSURE TO CERTAIN HERBICIDE AGENTS FOR WHICH THERE IS A PRESUMPTION OF SERVICE CONNECTION FOR VETERANS WHO SERVED IN THE REPUBLIC OF VIETNAM.

Section 1116(a)(2) of title 38, United States Code, is amended by adding at the end the following new subparagraphs:

"(I) Parkinsonism.

"(J) Bladder cancer.

"(K) Hypothyroidism.".

TITLE XCII—COMMUNICATIONS MATTERS

SEC. 9201. RELIABLE EMERGENCY ALERT DISTRIBUTION IMPROVEMENT. 47 USC 1206.

(a) WIRELESS EMERGENCY ALERTS SYSTEM OFFERINGS.—

(1) AMENDMENT.—Section 602(b)(2)(E) of the Warning, Alert, and Response Network Act (47 U.S.C. 1201(b)(2)(E)) is amended—

(A) by striking the second and third sentences; and

(B) by striking "other than an alert issued by the President." and inserting the following: "other than an alert issued by—

"(i) the President; or

"(ii) the Administrator of the Federal Emergency Management Agency.".

Deadline. Consultation.

(2) REGULATIONS.—Not later than 180 days after the date of enactment of this Act, the Commission, in consultation with the Administrator, shall adopt regulations to implement the amendment made by paragraph (1)(B).

(b) STATE EMERGENCY ALERT SYSTEM PLANS AND EMERGENCY COMMUNICATIONS COMMITTEES.—

Deadlines. Regulations.

(1) STATE EMERGENCY COMMUNICATIONS COMMITTEE.—Not later than 180 days after the date of enactment of this Act, the Commission shall adopt regulations that—

(A) encourage the chief executive of each State—

(i) to establish an SECC if the State does not have an SECC; or

Review.

(ii) if the State has an SECC, to review the composition and governance of the SECC;

(B) provide that—

(i) each SECC, not less frequently than annually, shall—

Review. Update.

(I) meet to review and update its State EAS Plan;

Certification.

(II) certify to the Commission that the SECC has met as required under subclause (I); and

(III) submit to the Commission an updated State EAS Plan; and

(ii) not later than 60 days after the date on which the Commission receives an updated State EAS Plan under clause (i)(III), the Commission shall—

Approval.

(I) approve or disapprove the updated State EAS Plan; and

Notification.

(II) notify the chief executive of the State of the Commission's approval or disapproval of such plan, and reason therefor; and

(C) establish a State EAS Plan content checklist for SECCs to use when reviewing and updating a State EAS Plan for submission to the Commission under subparagraph (B)(i).

(2) CONSULTATION.—The Commission shall consult with the Administrator regarding the adoption of regulations under paragraph (1)(C).

(3) DEFINITIONS.—In this subsection—

(A) the term "SECC" means a State Emergency Communications Committee;

(B) the term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States; and

(C) the term "State EAS Plan" means a State Emergency Alert System Plan.

Consultation. Regulations. Records. Examination.

(c) FALSE ALERT REPORTING.—Not later than 180 days after the date of enactment of this Act, the Commission, in consultation with the Administrator, shall complete a rulemaking proceeding to establish a system to receive from the Administrator or State, Tribal, or local governments reports of false alerts under the Emergency Alert System or the Wireless Emergency Alerts System for

the purpose of recording such false alerts and examining the causes of such false alerts.

(d) REPEATING EMERGENCY ALERT SYSTEM MESSAGES FOR NATIONAL SECURITY.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Commission, in consultation with the Administrator, shall complete a rulemaking proceeding to modify the Emergency Alert System to provide for repeating Emergency Alert System messages while an alert remains pending that is issued by— Deadline. Consultations. Regulations.

(A) the President; President.

(B) the Administrator; or

(C) any other entity determined appropriate under the circumstances by the Commission, in consultation with the Administrator. Determination.

(2) SCOPE OF RULEMAKING.—Paragraph (1) shall—

(A) apply to warnings of national security events, meaning emergencies of national significance, such as a missile threat, terror attack, or other act of war or threat to public safety; and Applicability.

(B) not apply to more typical warnings, such as a weather alert, AMBER Alert, or disaster alert.

(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to impair, limit, or otherwise change—

(A) the authority of the President granted by law to alert and warn the public; or

(B) the role of the President as commander-in-chief with respect to the identification, dissemination, notification, or alerting of information of missile threats against the United States, or threats to public safety.

(e) INTERNET AND ONLINE STREAMING SERVICES EMERGENCY ALERT EXAMINATION.—

(1) STUDY.—Not later than 180 days after the date of enactment of this Act, and after providing public notice and opportunity for comment, the Commission shall complete an inquiry to examine the feasibility of updating the Emergency Alert System to enable or improve alerts to consumers provided through the internet, including through streaming services. Deadline. Notice. Public comments.

(2) REPORT.—Not later than 90 days after completing the inquiry under paragraph (1), the Commission shall submit a report on the findings and conclusions of the inquiry to—

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

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

(f) DEFINITIONS.—In this section—

(1) the term "Administrator" means the Administrator of the Federal Emergency Management Agency;

(2) the term "Commission" means the Federal Communications Commission;

(3) the term "Emergency Alert System" means the national public warning system, the rules for which are set forth in part 11 of title 47, Code of Federal Regulations (or any successor regulation); and

(4) the term "Wireless Emergency Alerts System" means the wireless national public warning system established under the Warning, Alert, and Response Network Act (47 U.S.C.

1201 et seq.), the rules for which are set forth in part 10 of title 47, Code of Federal Regulations (or any successor regulation).

47 USC 906.

SEC. 9202. WIRELESS SUPPLY CHAIN INNOVATION AND MULTILATERAL SECURITY.

(a) COMMUNICATIONS TECHNOLOGY SECURITY FUNDS.—

(1) PUBLIC WIRELESS SUPPLY CHAIN INNOVATION FUND.—

(A) ESTABLISHMENT.—

(i) IN GENERAL.—There is established in the Treasury of the United States a trust fund to be known as the "Public Wireless Supply Chain Innovation Fund" (referred to in this paragraph as the "Innovation Fund").

(ii) AVAILABILITY.—

(I) IN GENERAL.—Amounts appropriated to the Innovation Fund shall remain available through the end of the tenth fiscal year beginning after the date on which funds are appropriated to the Fund.

(II) REMAINDER TO TREASURY.—Any amounts remaining in the Innovation Fund after the end of the tenth fiscal year beginning after the date of appropriation shall be deposited in the general fund of the Treasury.

Grants.
Determination.

(B) USE OF FUND.—

(i) IN GENERAL.—Amounts appropriated to the Innovation Fund shall be available to the Secretary, acting through the NTIA Administrator, to make grants on a competitive basis under this paragraph in such amounts as the Secretary, acting through the NTIA Administrator, determines appropriate, subject to clause (ii).

(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 $50,000,000.

Consultation.
Criteria.

(C) ADMINISTRATION OF FUND.—The Secretary, acting through the NTIA Administrator, in consultation with the Commission, the Under Secretary of Commerce for Standards and Technology, the Secretary of Homeland Security, the Secretary of Defense, and the Director of the Intelligence Advanced Research Projects Activity of the Office of the Director of National Intelligence, shall establish criteria for grants awarded under this paragraph, by the NTIA Administrator and administer the Innovation Fund, to support the following:

(i) Promoting and deploying technology, including software, hardware, and microprocessing technology, that will enhance competitiveness in the fifth-generation (commonly known as "5G") and successor wireless technology supply chains that use open and interoperable interface radio access networks.

(ii) Accelerating commercial deployments of 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, 3GPP, the Open-RAN Software Community, or any successor organizations.

(iii) Promoting and deploying compatibility of new 5G equipment with future open standards-based, interoperable equipment.

(iv) Managing integration of multi-vendor network environments.

(v) Identifying objective criteria to define equipment as compliant with open standards for multi-vendor network equipment interoperability.

(vi) Promoting and deploying security features enhancing the integrity and availability of equipment in multi-vendor networks.

(vii) Promoting and deploying network function virtualization to facilitate multi-vendor interoperability and a more diverse vendor market.

(D) NONDUPLICATION.—To the greatest extent practicable, the Secretary, acting through the NTIA Administrator, shall ensure that any research funded by a grant awarded under this paragraph avoids duplication of other Federal or private sector research.

(E) TIMING.—Not later than one year after the date on which funds are appropriated to the Innovation Fund, the Secretary, acting through the NTIA Administrator, shall begin awarding grants under this paragraph. Deadline.

(F) FEDERAL ADVISORY BODY.—

(i) ESTABLISHMENT.—The Secretary, acting through the NTIA Administrator, and in consultation with the Under Secretary of Commerce for Standards and Technology, 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 Secretary and the NTIA Administrator on the administration of the Innovation Fund. Consultation.

(ii) COMPOSITION.—The advisory committee established under clause (i) shall be composed of—

(I) representatives from—

(aa) the Commission;

(bb) the Department of Defense;

(cc) the Intelligence Advanced Research Projects Activity of the Office of the Director of National Intelligence;

(dd) the National Institute of Standards and Technology;

(ee) the Department of State;

(ff) the National Science Foundation;

(gg) the Department of Homeland Security; and

(hh) the National Telecommunications and Information Administration; and

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

(iii) DUTIES.—The advisory committee established under clause (i) shall advise the Secretary and the

NTIA Administrator on technology developments to help inform—

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

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

(G) REPORTS TO CONGRESS.—

(i) INITIAL REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary, acting through the NTIA Administrator, shall submit to the relevant committees of Congress a report with—

Recommendations.

(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 funds.

(ii) ANNUAL REPORT.—For each fiscal year for which amounts in the Innovation Fund are available under this paragraph, the Secretary, acting through the NTIA Administrator, shall submit to Congress a report that—

(I) describes how, and to whom, amounts in the Innovation Fund have been deployed;

(II) details the progress of the Secretary and the NTIA Administrator in meeting the objectives described in subparagraph (C); and

(III) includes any additional information that the Secretary and the NTIA Administrator determine appropriate.

(2) MULTILATERAL TELECOMMUNICATIONS SECURITY FUND.—

(A) ESTABLISHMENT OF FUND.—

(i) IN GENERAL.—There is established in the Treasury of the United States a trust fund to be known as the "Multilateral Telecommunications Security Fund".

(ii) USE OF FUND.—Amounts appropriated to the Multilateral Telecommunications Security Fund shall be available to the Secretary of State to make expenditures under this paragraph in such amounts as the Secretary of State determines appropriate.

(iii) AVAILABILITY.—

(I) IN GENERAL.—Amounts appropriated to the Multilateral Telecommunications Security Fund—

(aa) shall remain available through the end of the tenth fiscal year beginning after the date of appropriation; and

(bb) may only be allocated upon the Secretary of State reaching an arrangement or agreement with foreign government partners to participate in the common funding mechanism described in subparagraph (B).

(II) REMAINDER TO TREASURY.—Any amounts remaining in the Multilateral Telecommunications

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.

(B) ADMINISTRATION OF FUND.—The Secretary of State, in consultation with the NTIA Administrator, the Secretary of Homeland Security, the Secretary of Defense, the Secretary of the Treasury, the Director of National Intelligence, and the Commission, is authorized to establish a common funding mechanism, in coordination with foreign partners, that uses amounts from the Multilateral Telecommunications Security Fund to support the development and adoption of secure and trusted telecommunications technologies. In creating and sustaining a common funding mechanism, the Secretary of State should leverage United States funding in order to secure commitments and contributions from trusted foreign partners such as the United Kingdom, Canada, Australia, New Zealand, and Japan, and should prioritize the following objectives: Consultation.

(i) Advancing research and development of secure and trusted communications technologies.

(ii) Strengthening supply chains.

(iii) Promoting the use of trusted vendors.

(C) ANNUAL REPORT TO CONGRESS.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter for each fiscal year during which amounts in the Multilateral Telecommunications Security Fund are available, the Secretary of State shall submit to the relevant committees of Congress a report on the status and progress of the funding mechanism established under subparagraph (B), including—

(i) any funding commitments from foreign partners, including each specific amount committed;

(ii) governing criteria for use of the Multilateral Telecommunications Security Fund;

(iii) an account of—

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

(II) amounts remaining in the Multilateral Telecommunications Security Fund; and

(III) the progress of the Secretary of State in meeting the objective described in subparagraph (B); and

(iv) additional authorities needed to enhance the effectiveness of the Multilateral Telecommunications Security Fund in achieving the security goals of the United States.

(D) NOTIFICATIONS TO BE PROVIDED BY THE FUND.—

(i) IN GENERAL.—Not later than 15 days prior to the Fund making a financial commitment associated with the provision of expenditures under subparagraph (A)(ii) in an amount in excess of $1,000,000, the Secretary of State shall submit to the appropriate congressional committees a report in writing that contains the information required by clause (ii). Reports.

(ii) INFORMATION REQUIRED.—The information required by this clause includes—

(I) the amount of each such expenditure;

(II) an identification of the recipient or beneficiary; and

(III) a description of the project or activity and the purpose to be achieved of an expenditure by the Fund.

Deadline.

(iii) ARRANGEMENTS OR AGREEMENTS.—The Secretary of State shall notify the appropriate congressional committees not later than 30 days after entering into a new bilateral or multilateral arrangement or agreement described in subparagraph (A)(iii)(I)(bb).

(iv) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this subparagraph, the term "appropriate congressional committees" means—

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

(II) the Committee on Appropriations of the Senate;

(III) the Committee on Foreign Affairs of the House of Representatives; and

(IV) the Committee on Appropriations of the House of Representatives.

(b) PROMOTING UNITED STATES LEADERSHIP IN INTERNATIONAL ORGANIZATIONS AND COMMUNICATIONS STANDARDS-SETTING BODIES.—

(1) IN GENERAL.—The Secretary of State, the Secretary of Commerce, and the Chairman of the Commission, or their designees, shall consider how to enhance representation of the United States at international forums that set standards for 5G networks and for future generations of wireless communications networks, including—

(A) the International Telecommunication Union (commonly known as "ITU");

(B) the International Organization for Standardization (commonly known as "ISO");

(C) the Inter-American Telecommunication Commission (commonly known as "CITEL"); and

(D) the voluntary standards organizations that develop protocols for wireless devices and other equipment, such as the 3GPP and the Institute of Electrical and Electronics Engineers (commonly known as "IEEE").

(2) ANNUAL REPORT.—The Secretary of State, the Secretary of Commerce, and the Chairman of the Commission shall jointly submit to the relevant committees of Congress an annual report on the progress made under paragraph (1).

(c) DEFINITIONS.— In this section:

(1) The term "3GPP" means the Third Generation Partnership Project.

(2) The term "5G network" means a radio network as described by 3GPP Release 15 or higher.

(3) The term "Commission" means the Federal Communications Commission.

(4) The term "NTIA Administrator" means the Assistant Secretary of Commerce for Communications and Information.

(5) The term "Open-RAN" means the Open Radio Access Network approach to standardization adopted by the O-RAN Alliance, Telecom Infra Project, or 3GPP, or any similar set

of open standards for multi-vendor network equipment interoperability.

(6) The term "relevant 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 Committee on Appropriations of the Senate;

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

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

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

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

(K) the Committee on Energy and Commerce of the House of Representatives; and

(L) the Committee on Appropriations of the House of Representatives.

(7) The term "Secretary" means the Secretary of Commerce.

SEC. 9203. SPECTRUM INFORMATION TECHNOLOGY MODERNIZATION EFFORTS.

Reports.
Plans.
47 USC 902 note.
Deadline.
Consultation.

(a) INITIAL INTERAGENCY SPECTRUM INFORMATION TECHNOLOGY COORDINATION.—Not later than 90 days after the date of the enactment of this Act, the Assistant Secretary of Commerce for Communications and Information, in consultation with the Policy and Plans Steering Group, shall identify a process to establish goals, including parameters to measure the achievement of such goals, for the modernization of the infrastructure of covered agencies relating to managing the use of Federal spectrum by such agencies, which shall include—

Standards.
Data.

(1) the standardization of data inputs, modeling algorithms, modeling and simulation processes, analysis tools with respect to Federal spectrum, assumptions, and any other tool to ensure interoperability and functionality with respect to such infrastructure;

(2) other potential innovative technological capabilities with respect to such infrastructure, including cloud-based databases, artificial intelligence technologies, automation, and improved modeling and simulation capabilities;

(3) ways to improve the management of the use of Federal spectrum by covered agencies through such infrastructure, including by—

(A) increasing the efficiency of such infrastructure;

(B) addressing validation of usage with respect to such infrastructure;

(C) increasing the accuracy of such infrastructure;

(D) validating models used by such infrastructure; and

(E) monitoring and enforcing requirements that are imposed on covered agencies with respect to the use of Federal spectrum by covered agencies;

(4) ways to improve the ability of covered agencies to meet mission requirements in congested environments with respect to Federal spectrum, including as part of automated adjustments to operations based on changing conditions in such environments;

(5) the creation of a time-based automated mechanism—

(A) to share Federal spectrum between covered agencies to collaboratively and dynamically increase access to Federal spectrum by such agencies; and

(B) that could be scaled across Federal spectrum; and

(6) the collaboration between covered agencies necessary to ensure the interoperability of Federal spectrum.

(b) SPECTRUM INFORMATION TECHNOLOGY MODERNIZATION.—

(1) IN GENERAL.—Not later than 240 days after the date of the enactment of this Act, the Assistant Secretary of Commerce for Communications and Information shall submit to Congress a report that contains a plan for the National Telecommunications and Information Administration (in this section referred to as the "NTIA") to modernize and automate the infrastructure of the NTIA relating to managing the use of Federal spectrum by covered agencies so as to more efficiently manage such use.

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

Assessment.

(A) an assessment of the current, as of the date on which such report is submitted, infrastructure of the NTIA described in such paragraph;

Acquisition strategy.

(B) an acquisition strategy for the modernized infrastructure of the NTIA described in such paragraph, including how such modernized infrastructure will enable covered agencies to be more efficient and effective in the use of Federal spectrum;

Timeline.

(C) a timeline for the implementation of the modernization efforts described in such paragraph;

(D) plans detailing how the modernized infrastructure of the NTIA described in such paragraph will—

(i) enhance the security and reliability of such infrastructure so that the NTIA is in compliance with the requirements of subchapter II of chapter 35 of title 44, United States Code, with respect to such infrastructure;

(ii) improve data models and analysis tools to increase the efficiency of the spectrum use described in such paragraph;

(iii) enhance automation and workflows, and reduce the scope and level of manual effort, in order to—

(I) administer the management of the spectrum use described in such paragraph; and

(II) improve data quality and processing time; and

(iv) improve the timeliness of spectrum analyses and requests for information, including requests submitted pursuant to section 552 of title 5, United States Code;

(E) an operations and maintenance plan with respect to the modernized infrastructure of the NTIA described in such paragraph;

(F) a strategy for coordination between the covered agencies within the Policy and Plans Steering Group, which shall include— Strategy.

(i) a description of—

(I) such coordination efforts, as in effect on the date on which such report is submitted; and

(II) a plan for coordination of such efforts after the date on which such report is submitted, including with respect to the efforts described in subsection (c);

(ii) a plan for standardizing—

(I) electromagnetic spectrum analysis tools;

(II) modeling and simulation processes and technologies; and

(III) databases to provide technical interference assessments that are usable across the Federal Government as part of a common spectrum management infrastructure for covered agencies; and

(iii) a plan for each covered agency to implement a modernization plan described in subsection (c)(1) that is tailored to the particular timeline of such agency; Plan.

(G) identification of manually intensive processes involved in managing Federal spectrum and proposed enhancements to such processes;

(H) metrics to evaluate the success of the modernization efforts described in such paragraph and any similar future efforts; and Evaluation.

(I) an estimate of the cost of the modernization efforts described in such paragraph and any future maintenance with respect to the modernized infrastructure of the NTIA described in such paragraph, including the cost of any personnel and equipment relating to such maintenance. Cost estimate.

(c) COVERED AGENCY SPECTRUM INFORMATION TECHNOLOGY MODERNIZATION.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the head of each covered agency shall submit to the Assistant Secretary of Commerce for Communications and Information and the Policy and Plans Steering Group a report that describes a plan for such agency to modernize the infrastructure of such agency with respect to the use of Federal spectrum by such agency so that such modernized infrastructure of such agency is interoperable with the modernized infrastructure of the NTIA, as described in subsection (b).

(2) CONTENTS.—Each report submitted by the head of a covered agency under paragraph (1) shall—

(A) include—

(i) an assessment of the current, as of the date on which such report is submitted, management capabilities of such agency with respect to the use of frequencies that are assigned to such agency, which shall include a description of any challenges faced by such agency with respect to such management; Assessment.

Timeline.

(ii) a timeline for completion of the modernization efforts described in such paragraph;

(iii) a description of potential innovative technological capabilities for the management of frequencies that are assigned to such agency, as determined under subsection (a);

(iv) identification of agency-specific requirements or constraints relating to the infrastructure of such agency;

(v) identification of any existing, as of the date on which such report is submitted, systems of such agency that are duplicative of the modernized infrastructure of the NTIA, as described in subsection (b); and

Strategies.

(vi) with respect to the report submitted by the Secretary of Defense—

(I) a strategy for the integration of systems or the flow of data among the Armed Forces, the military departments, the Defense Agencies and Department of Defense Field Activities, and other components of the Department of Defense;

(II) a plan for the implementation of solutions to the use of Federal spectrum by the Department of Defense involving information at multiple levels of classification; and

(III) a strategy for addressing, within the modernized infrastructure of the Department of Defense described in such paragraph, the exchange of information between the Department of Defense and the NTIA in order to accomplish required processing of all Department of Defense domestic spectrum coordination and management activities; and

Classified information.

(B) be submitted in an unclassified format, with a classified annex, as appropriate.

(3) NOTIFICATION OF CONGRESS.—Upon submission of a report under paragraph (1), the head of a covered agency shall notify Congress that such report has been submitted.

Deadlines.

(d) GAO OVERSIGHT.—The Comptroller General of the United States shall—

Review.

(1) not later than 180 days after the date of the enactment of this Act, conduct a review of the infrastructure of covered agencies, as such infrastructure exists on the date of the enactment of this Act;

(2) upon submission of all of the reports required by subsection (c), begin conducting oversight of the implementation of the modernization plans submitted by the Assistant Secretary and covered agencies under subsections (b) and (c), respectively;

Time period.

(3) not later than 2 years after the date on which the Comptroller General begins conducting oversight under paragraph (2), and biennially thereafter until December 31, 2030, submit a report regarding such oversight to—

(A) with respect to the implementation of the modernization plan of the Department of Defense, the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and

(B) with respect to the implementation of the modernization plans of all covered agencies, including the Department of Defense, the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives; and

(4) until December 31, 2030, provide regular briefings to— Briefings.

(A) with respect to the application of this section to the Department of Defense, the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives; and

(B) with respect to the application of this section to all covered agencies, including the Department of Defense, the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives.

(e) DEFINITIONS.—In this section:

(1) The term "covered agency"—

(A) means any Federal entity that the Assistant Secretary of Commerce for Communications and Information determines is appropriate; and

(B) includes the Department of Defense.

(2) The term "Federal entity" has the meaning given such term in section 113(l) of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 923(l)).

(3) The term "Federal spectrum" means frequencies assigned on a primary basis to a covered agency.

(4) The term "infrastructure" means information technology systems and information technologies, tools, and databases.

SEC. 9204. INTERNET OF THINGS. 47 USC 901 note.

(a) DEFINITIONS.—In this section:

(1) COMMISSION.—The term "Commission" means the Federal Communications Commission.

(2) SECRETARY.—The term "Secretary" means the Secretary of Commerce.

(3) STEERING COMMITTEE.—The term "steering committee" means the steering committee established under subsection (b)(5)(A).

(4) WORKING GROUP.—The term "working group" means the working group convened under subsection (b)(1).

(b) FEDERAL WORKING GROUP.—

(1) IN GENERAL.—The Secretary shall convene a working group of Federal stakeholders for the purpose of providing recommendations and a report to Congress relating to the aspects of the Internet of Things described in paragraph (2).

(2) DUTIES.—The working group shall—

(A) identify any Federal regulations, statutes, grant practices, budgetary or jurisdictional challenges, and other sector-specific policies that are inhibiting, or could inhibit, the development or deployment of the Internet of Things;

(B) consider policies or programs that encourage and improve coordination among Federal agencies that have responsibilities that are relevant to the objectives of this section;

(C) consider any findings or recommendations made by the steering committee and, where appropriate, act to implement those recommendations;

(D) examine—

(i) how Federal agencies can benefit from utilizing the Internet of Things;

(ii) the use of Internet of Things technology by Federal agencies as of the date on which the working group performs the examination;

(iii) the preparedness and ability of Federal agencies to adopt Internet of Things technology as of the date on which the working group performs the examination and in the future; and

(iv) any additional security measures that Federal agencies may need to take to—

(I) safely and securely use the Internet of Things, including measures that ensure the security of critical infrastructure; and

(II) enhance the resiliency of Federal systems against cyber threats to the Internet of Things; and

(E) in carrying out the examinations required under subclauses (I) and (II) of subparagraph (D)(iv), ensure to the maximum extent possible the coordination of the current and future activities of the Federal Government relating to security with respect to the Internet of Things.

(3) AGENCY REPRESENTATIVES.—In convening the working group under paragraph (1), the Secretary shall have discretion to appoint representatives from Federal agencies and departments as appropriate and shall specifically consider seeking representation from—

(A) the Department of Commerce, including—

(i) the National Telecommunications and Information Administration;

(ii) the National Institute of Standards and Technology; and

(iii) the National Oceanic and Atmospheric Administration;

(B) the Department of Transportation;

(C) the Department of Homeland Security;

(D) the Office of Management and Budget;

(E) the National Science Foundation;

(F) the Commission;

(G) the Federal Trade Commission;

(H) the Office of Science and Technology Policy;

(I) the Department of Energy; and

(J) the Federal Energy Regulatory Commission.

Consultation.

(4) NONGOVERNMENTAL STAKEHOLDERS.—The working group shall consult with nongovernmental stakeholders with expertise relating to the Internet of Things, including—

(A) the steering committee;

(B) information and communications technology manufacturers, suppliers, service providers, and vendors;

(C) subject matter experts representing industrial sectors other than the technology sector that can benefit from the Internet of Things, including the transportation, energy, agriculture, and health care sectors;

(D) small, medium, and large businesses;
(E) think tanks and academia;
(F) nonprofit organizations and consumer groups;
(G) security experts;
(H) rural stakeholders; and
(I) other stakeholders with relevant expertise, as determined by the Secretary.

(5) STEERING COMMITTEE.—

(A) ESTABLISHMENT.—There is established within the Department of Commerce a steering committee to advise the working group.

(B) DUTIES.—The steering committee shall advise the working group with respect to—

(i) the identification of any Federal regulations, statutes, grant practices, programs, budgetary or jurisdictional challenges, and other sector-specific policies that are inhibiting, or could inhibit, the development of the Internet of Things;

(ii) situations in which the use of the Internet of Things is likely to deliver significant and scalable economic and societal benefits to the United States, including benefits from or to—

(I) smart traffic and transit technologies;
(II) augmented logistics and supply chains;
(III) sustainable infrastructure;
(IV) precision agriculture;
(V) environmental monitoring;
(VI) public safety; and
(VII) health care;

(iii) whether adequate spectrum is available to support the growing Internet of Things and what legal or regulatory barriers may exist to providing any spectrum needed in the future;

(iv) policies, programs, or multi-stakeholder activities that—

(I) promote or are related to the privacy of individuals who use or are affected by the Internet of Things;

(II) may enhance the security of the Internet of Things, including the security of critical infrastructure;

(III) may protect users of the Internet of Things; and

(IV) may encourage coordination among Federal agencies with jurisdiction over the Internet of Things;

(v) the opportunities and challenges associated with the use of Internet of Things technology by small businesses; and

(vi) any international proceeding, international negotiation, or other international matter affecting the Internet of Things to which the United States is or should be a party.

(C) MEMBERSHIP.—The Secretary shall appoint to the steering committee members representing a wide range of stakeholders outside of the Federal Government with expertise relating to the Internet of Things, including— Appointment.

(i) information and communications technology manufacturers, suppliers, service providers, and vendors;

(ii) subject matter experts representing industrial sectors other than the technology sector that can benefit from the Internet of Things, including the transportation, energy, agriculture, and health care sectors;

(iii) small, medium, and large businesses;

(iv) think tanks and academia;

(v) nonprofit organizations and consumer groups;

(vi) security experts;

(vii) rural stakeholders; and

Determination.

(viii) other stakeholders with relevant expertise, as determined by the Secretary.

Recommendations.

(D) REPORT.—Not later than 1 year after the date of enactment of this Act, the steering committee shall submit to the working group a report that includes any findings or recommendations of the steering committee.

(E) INDEPENDENT ADVICE.—

(i) IN GENERAL.—The steering committee shall set the agenda of the steering committee in carrying out the duties of the steering committee under subparagraph (B).

(ii) SUGGESTIONS.—The working group may suggest topics or items for the steering committee to study, and the steering committee shall take those suggestions into consideration in carrying out the duties of the steering committee.

(iii) REPORT.—The steering committee shall ensure that the report submitted under subparagraph (D) is the result of the independent judgment of the steering committee.

(F) NO COMPENSATION FOR MEMBERS.—A member of the steering committee shall serve without compensation.

(G) TERMINATION.—The steering committee shall terminate on the date on which the working group submits the report under paragraph (6).

(6) REPORT TO CONGRESS.—

Recommendations.

(A) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the working group shall submit to Congress a report that includes—

(i) the findings and recommendations of the working group with respect to the duties of the working group under paragraph (2);

(ii) the report submitted by the steering committee under paragraph (5)(D), as the report was received by the working group;

(iii) recommendations for action or reasons for inaction, as applicable, with respect to each recommendation made by the steering committee in the report submitted under paragraph (5)(D); and

(iv) an accounting of any progress made by Federal agencies to implement recommendations made by the working group or the steering committee.

(B) COPY OF REPORT.—The working group shall submit a copy of the report described in subparagraph (A) to—

(i) the Committee on Commerce, Science, and Transportation and the Committee on Energy and Natural Resources of the Senate;

(ii) the Committee on Energy and Commerce of the House of Representatives; and

(iii) any other committee of Congress, upon request to the working group.

(c) ASSESSING SPECTRUM NEEDS.—

(1) IN GENERAL.—The Commission, in consultation with the National Telecommunications and Information Administration, shall issue a notice of inquiry seeking public comment on the current, as of the date of enactment of this Act, and future spectrum needs to enable better connectivity relating to the Internet of Things. Consultation.

(2) REQUIREMENTS.—In issuing the notice of inquiry under paragraph (1), the Commission shall seek comments that consider and evaluate— Evaluation.

(A) whether adequate spectrum is available, or is planned for allocation, for commercial wireless services that could support the growing Internet of Things;

(B) if adequate spectrum is not available for the purposes described in subparagraph (A), how to ensure that adequate spectrum is available for increased demand with respect to the Internet of Things;

(C) what regulatory barriers may exist to providing any needed spectrum that would support uses relating to the Internet of Things; and

(D) what the role of unlicensed and licensed spectrum is and will be in the growth of the Internet of Things.

(3) REPORT.—Not later than 1 year after the date of enactment of this Act, the Commission shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report summarizing the comments submitted in response to the notice of inquiry issued under paragraph (1). Summary.

TITLE XCIII—INTELLIGENCE MATTERS

SEC. 9301. REQUIREMENT FOR FACILITATION OF ESTABLISHMENT OF SOCIAL MEDIA DATA AND THREAT ANALYSIS CENTER.

(a) REQUIREMENT TO FACILITATE ESTABLISHMENT.—Subsection (c)(1) of section 5323 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (division E of Public Law 116–92; 50 U.S.C. 3369) is amended—

(1) by striking "The Director" and inserting "Not later than June 1, 2021, the Director"; and

(2) by striking "may" and inserting "shall".

(b) REPORTING ON FOREIGN MALIGN INFLUENCE CAMPAIGNS ON SOCIAL MEDIA PLATFORMS TARGETING ELECTIONS FOR FEDERAL OFFICE.—Such section is amended—

(1) by redesignating subsections (f) and (g) as subsections (g) and (h), respectively; and

(2) by inserting after subsection (e) the following new subsection (f):

"(f) FOREIGN MALIGN INFLUENCE CAMPAIGNS ON SOCIAL MEDIA PLATFORMS TARGETING ELECTIONS FOR FEDERAL OFFICE.—

"(1) REPORTS.—

"(A) REQUIREMENT.—Not later than 90 days before the date of each regularly scheduled general election for Federal office, the Director of the Center shall submit to the appropriate congressional committees a report on foreign malign influence campaigns on and across social media platforms targeting such election.

"(B) MATTERS INCLUDED.—Each report under subparagraph (A) shall include an analysis of the following:

"(i) The patterns, tools, and techniques of foreign malign influence campaigns across all platforms on social media by a covered foreign country targeting a regularly scheduled general election for Federal office.

"(ii) Inauthentic accounts and 'bot' networks across platforms, including the scale to which such accounts or networks exist, how platforms currently act to remove such accounts or networks, and what percentage of such accounts or networks have been removed during the period covered by the report.

Estimate.

"(iii) The estimated reach and impact of intentional or weaponized disinformation by inauthentic accounts and 'bot' networks, including an analysis of amplification by users and algorithmic distribution.

"(iv) The trends of types of media that are being used for dissemination through foreign malign influence campaigns, including machine-manipulated media, and the intended targeted groups.

"(C) INITIAL REPORT.—Not later than August 1, 2021, the Director of the Center shall submit to the appropriate congressional committees a report under subparagraph (A) addressing the regularly scheduled general election for Federal office occurring during 2020.

Classified information.

"(D) FORM.—Each report under this paragraph shall be submitted in an unclassified form, but may include a classified annex.

Assessments.
Reports.
Coordination.

"(2) BRIEFINGS.—

"(A) REQUIREMENT.—Not later than 30 days after the date on which the Director submits to the appropriate congressional committees a report under paragraph (1), the Director of National Intelligence, in coordination with the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, shall provide to such committees a briefing assessing threats from foreign malign influence campaigns on social media from covered countries to the regularly scheduled general election for Federal office covered by the report.

"(B) MATTERS TO BE INCLUDED.—Each briefing under subparagraph (A) shall include the following:

"(i) The patterns, tools, and techniques of foreign malign influence campaigns across all platforms on

social media by a covered foreign country targeting a regularly scheduled general election for Federal office.

"(ii) An assessment of the findings from the report for which the briefing is provided.

"(iii) The activities and methods used to mitigate the threats associated with such findings by the Department of Defense, the Department of Homeland Security, or other relevant departments or agencies of the Federal Government.

"(iv) The steps taken by departments or agencies of the Federal Government to cooperate with social media companies to mitigate the threats identified.".

(c) DEFINITIONS.—Subsection (h) of such section, as redesignated by subsection (b) of this section, is amended to read as follows:

"(h) DEFINITIONS.—

"(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

"(A) the congressional intelligence committees;

"(B) the Committee on Armed Services, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Foreign Affairs, and the Committee on the Judiciary of the House of Representatives; and

"(C) the Committee on Armed Services, the Committee on Appropriations, the Committee on Homeland Security and Government Affairs, the Committee on Foreign Relations, and the Committee on the Judiciary of the Senate.

"(2) COVERED FOREIGN COUNTRY AND FOREIGN MALIGN INFLUENCE.—The terms 'covered foreign country' and 'foreign malign influence' have the meanings given those terms in section 119C of the National Security Act of 1947 (50 U.S.C. 3059).

"(3) MACHINE-MANIPULATED MEDIA.—The term 'machine-manipulated media' has the meaning given that term in section 5724.".

(d) CONFORMING AMENDMENTS.—

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

(A) in the matter preceding 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 "August 1, 2021".

(2) FUNDING.—Subsection (g) of such section, as redesignated by subsection (b) of this section, is amended by striking "fiscal year 2020 and 2021" and inserting "fiscal year 2021 and 2022".

(3) CLERICAL.—Such section 5323 is further amended—

(A) in the section heading, by striking "**ENCOURAGEMENT OF**"; and

(B) in subsection (c)—

(i) in the subsection heading, by striking "AUTHORITY" and inserting "REQUIREMENT"; and

(ii) in paragraph (1), in the paragraph heading, by striking "AUTHORITY" and inserting "REQUIREMENT".

SEC. 9302. INDEPENDENT STUDY ON IDENTIFYING AND ADDRESSING THREATS THAT INDIVIDUALLY OR COLLECTIVELY AFFECT NATIONAL SECURITY, FINANCIAL SECURITY, OR BOTH.

Deadline. Coordination.

(a) INDEPENDENT STUDY.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Secretary of the Treasury and the heads of other relevant departments and agencies of the Federal Government, shall seek to enter into a contract with a federally funded research and development center under which the center will conduct a study on identifying and addressing threats that individually or collectively affect national security, financial security, or both.

Assessments.

(b) ELEMENTS OF STUDY.—In carrying out the study under subsection (a), the federally funded research and development center selected under such subsection shall—

(1) identify threats that individually or collectively affect national security, financial security, or both, including—

(A) foreign influence in companies seeking to access capital markets by conducting initial public offerings in other countries;

(B) the use of financial instruments, markets, payment systems, or digital assets in ways that appear legitimate but may be part of a foreign malign strategy to weaken or undermine the economic security of the United States; and

(C) any other known or potential threats that individually or collectively affect national security, financial security, or both currently or in the foreseeable future;

(2) assess the extent to which the United States Government is currently able to identify and characterize the threats identified under paragraph (1);

(3) assess the extent to which the United States Government is currently able to address the risk posed by the threats identified under paragraph (1);

(4) assess whether current levels of information sharing and cooperation between the United States Government and allies and partners of the United States have been helpful or can be improved upon in order for the United States Government to identify, characterize, and mitigate the threats identified under paragraph (1); and

Recommendations.

(5) recommend opportunities, and any such authorities or resources required, to improve the efficiency and effectiveness of the United States Government in identifying and countering the threats identified under paragraph (1).

Reports. Classified information.

(c) SUBMISSION TO DIRECTOR OF NATIONAL INTELLIGENCE.—Not later than 180 days after the date of the enactment of this Act, the federally funded research and development center selected to conduct the study under subsection (a) shall submit to the Director of National Intelligence a report on the results of the study in both classified and unclassified form.

(d) SUBMISSION TO CONGRESS.—

Deadline.

(1) IN GENERAL.—Not later than 30 days after the date on which the Director of National Intelligence receives the report under subsection (c), the Director shall submit to the appropriate congressional committees—

(A) a copy of the report, without change, in both classified and unclassified form; and Records.

(B) such comments as the Director, in coordination with the Secretary of the Treasury and the heads of other relevant departments and agencies of the Federal Government, may have with respect to the report. Consultation.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this subsection, the term "appropriate congressional committees" means—

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

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

TITLE XCIV—SCIENCE, SPACE, AND TECHNOLOGY MATTERS

Subtitle A—Cybersecurity Matters

Subtitle B—Other Matters

Subtitle A—Cybersecurity Matters

SEC. 9401. IMPROVING NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION.

(a) PROGRAM IMPROVEMENTS GENERALLY.—Subsection (a) of section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451) is amended—

(1) in paragraph (5), by striking "; and" and inserting a semicolon;

(2) by redesignating paragraph (6) as paragraph (10); and

(3) by inserting after paragraph (5) the following:

"(6) supporting efforts to identify cybersecurity workforce skill gaps in public and private sectors;

"(7) facilitating Federal programs to advance cybersecurity education, training, and workforce development;

Coordination.

"(8) in coordination with the Department of Defense, the Department of Homeland Security, and other appropriate agencies, considering any specific needs of the cybersecurity workforce of critical infrastructure, including cyber physical systems and control systems;

"(9) advising the Director of the Office of Management and Budget, as needed, in developing metrics to measure the effectiveness and effect of programs and initiatives to advance the cybersecurity workforce; and".

(b) STRATEGIC PLAN.—Subsection (c) of such section is amended—

(1) by striking "The Director" and inserting the following: "(1) IN GENERAL.—The Director"; and

(2) by adding at the end the following:

"(2) REQUIREMENT.—The strategic plan developed and implemented under paragraph (1) shall include an indication of how the Director will carry out this section.".

15 USC 7451 note.

(c) CYBERSECURITY CAREER PATHWAYS.—

Deadline. Coordination. Consultation.

(1) IDENTIFICATION OF MULTIPLE CYBERSECURITY CAREER PATHWAYS.—In carrying out subsection (a) of such section and not later than 540 days after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall, in coordination with the Secretary of Defense, the Secretary of Homeland Security, the Director of the Office of Personnel Management, and the heads of other appropriate agencies, use a consultative process with other Federal agencies, academia, and industry to identify multiple career pathways for cybersecurity work roles that can be used in the private and public sectors.

(2) REQUIREMENTS.—The Director shall ensure that the multiple cybersecurity career pathways identified under paragraph (1) indicate the knowledge, skills, and abilities, including relevant education, training, internships, apprenticeships, certifications, and other experiences, that—

(A) align with employers' cybersecurity skill needs, including proficiency level requirements, for its workforce; and

(B) prepare an individual to be successful in entering or advancing in a cybersecurity career.

Coordination.

(3) EXCHANGE PROGRAM.—Consistent with requirements under chapter 37 of title 5, United States Code, the Director of the National Institute of Standards and Technology, in coordination with the Director of the Office of Personnel Management, may establish a voluntary program for the exchange of employees engaged in one of the cybersecurity work roles identified in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework, between the National Institute of Standards and Technology and private sector institutions, including nonpublic or commercial businesses, research institutions, or institutions of higher education, as the Director of the National Institute of Standards and Technology considers feasible.

Deadline. Coordination. 15 USC 7451 note.

(d) PROFICIENCY TO PERFORM CYBERSECURITY TASKS.—Not later than 540 days after the date of the enactment of this Act, the

Director of the National Institute of Standards and Technology shall, in coordination with the Secretary of Defense, the Secretary of Homeland Security, and the heads of other appropriate agencies—

(1) in carrying out subsection (a) of such section, assess the scope and sufficiency of efforts to measure an individual's capability to perform specific tasks found in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181) at all proficiency levels; and Assessment.

(2) submit to Congress a report—

(A) on the findings of the Director with respect to the assessment carried out under paragraph (1); and

(B) with recommendations for effective methods for measuring the cybersecurity proficiency of learners. Recommendations.

(e) CYBERSECURITY METRICS.—Such section is further amended by adding at the end the following:

"(e) CYBERSECURITY METRICS.—In carrying out subsection (a), the Director of the Office of Management and Budget may seek input from the Director of the National Institute of Standards and Technology, in coordination with the Department of Homeland Security, the Department of Defense, the Office of Personnel Management, and such agencies as the Director of the National Institute of Standards and Technology considers relevant, to develop quantifiable metrics for evaluating Federally funded cybersecurity workforce programs and initiatives based on the outcomes of such programs and initiatives.".

(f) REGIONAL ALLIANCES AND MULTISTAKEHOLDER PARTNERSHIPS.—Such section is further amended by adding at the end the following:

"(f) REGIONAL ALLIANCES AND MULTISTAKEHOLDER PARTNERSHIPS.—

"(1) IN GENERAL.—Pursuant to section 2(b)(4) of the National Institute of Standards and Technology Act (15 U.S.C. 272(b)(4)), the Director shall establish cooperative agreements between the National Initiative for Cybersecurity Education (NICE) of the Institute and regional alliances or partnerships for cybersecurity education and workforce. Contracts.

"(2) AGREEMENTS.—The cooperative agreements established under paragraph (1) shall advance the goals of the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework, by facilitating local and regional partnerships to— Contracts.

"(A) identify the workforce needs of the local economy and classify such workforce in accordance with such framework;

"(B) identify the education, training, apprenticeship, and other opportunities available in the local economy; and

"(C) support opportunities to meet the needs of the local economy.

"(3) FINANCIAL ASSISTANCE.—

"(A) FINANCIAL ASSISTANCE AUTHORIZED.—The Director may award financial assistance to a regional alliance or partnership with whom the Director enters into a cooperative agreement under paragraph (1) in order to assist the regional alliance or partnership in carrying out the terms of the cooperative agreement.

"(B) AMOUNT OF ASSISTANCE.—The aggregate amount of financial assistance awarded under subparagraph (A) per cooperative agreement shall not exceed $200,000.

"(C) MATCHING REQUIREMENT.—The Director may not award financial assistance to a regional alliance or partnership under subparagraph (A) unless the regional alliance or partnership agrees that, with respect to the costs to be incurred by the regional alliance or partnership in carrying out the cooperative agreement for which the assistance was awarded, the regional alliance or partnership will make available (directly or through donations from public or private entities) non-Federal contributions, including in-kind contributions, in an amount equal to 50 percent of Federal funds provided under the award.

"(4) APPLICATION.—

"(A) IN GENERAL.—A regional alliance or partnership seeking to enter into a cooperative agreement under paragraph (1) and receive financial assistance under paragraph (3) shall submit to the Director an application therefore at such time, in such manner, and containing such information as the Director may require.

"(B) REQUIREMENTS.—Each application submitted under subparagraph (A) shall include the following:

"(i)(I) A plan to establish (or identification of, if it already exists) a multistakeholder workforce partnership that includes—

"(aa) at least one institution of higher education or nonprofit training organization; and

"(bb) at least one local employer or owner or operator of critical infrastructure.

"(II) Participation from academic institutions in the Federal Cyber Scholarships for Service Program, the National Centers of Academic Excellence in Cybersecurity Program, or advanced technological education programs, as well as elementary and secondary schools, training and certification providers, State and local governments, economic development organizations, or other community organizations is encouraged.

"(ii) A description of how the workforce partnership would identify the workforce needs of the local economy.

"(iii) A description of how the multistakeholder workforce partnership would leverage the programs and objectives of the National Initiative for Cybersecurity Education, such as the Cybersecurity Workforce Framework and the strategic plan of such initiative.

"(iv) A description of how employers in the community will be recruited to support internships, externships, apprenticeships, or cooperative education programs in conjunction with providers of education and training. Inclusion of programs that seek to include veterans, Indian Tribes, and underrepresented groups, including women, minorities, persons from rural and underserved areas, and persons with disabilities is encouraged.

"(v) A definition of the metrics to be used in determining the success of the efforts of the regional alliance or partnership under the agreement.

"(C) PRIORITY CONSIDERATION.—In awarding financial assistance under paragraph (3)(A), the Director shall give priority consideration to a regional alliance or partnership that includes an institution of higher education that is designated as a National Center of Academic Excellence in Cybersecurity or which received an award under the Federal Cyber Scholarship for Service program located in the State or region of the regional alliance or partnership.

"(5) AUDITS.—Each cooperative agreement for which financial assistance is awarded under paragraph (3) shall be subject to audit requirements under part 200 of title 2, Code of Federal Regulations (relating to uniform administrative requirements, cost principles, and audit requirements for Federal awards), or successor regulation.

"(6) REPORTS.—

"(A) IN GENERAL.—Upon completion of a cooperative agreement under paragraph (1), the regional alliance or partnership that participated in the agreement shall submit to the Director a report on the activities of the regional alliance or partnership under the agreement, which may include training and education outcomes.

"(B) CONTENTS.—Each report submitted under subparagraph (A) by a regional alliance or partnership shall include the following:

Assessment.

"(i) An assessment of efforts made by the regional alliance or partnership to carry out paragraph (2).

"(ii) The metrics used by the regional alliance or partnership to measure the success of the efforts of the regional alliance or partnership under the cooperative agreement.".

(g) TRANSFER OF SECTION.—

15 USC 7451, 7443.

(1) TRANSFER.—Such section is transferred to the end of title III of such Act and redesignated as section 303.

(2) REPEAL.—Title IV of such Act is repealed.

(3) CLERICAL.—The table of contents in section 1(b) of such Act is amended—

(A) by striking the items relating to title IV and section 401; and

(B) by inserting after the item relating to section 302 the following:

"Sec. 303. National cybersecurity awareness and education program.".

(4) CONFORMING AMENDMENTS.—

(A) Section 302(3) of the Federal Cybersecurity Workforce Assessment Act of 2015 (Public Law 114–113; 5 U.S.C. 301 note) is amended by striking "under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451)" and inserting "under section 303 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274)".

(B) Section 2(c)(3) of the NIST Small Business Cybersecurity Act (Public Law 115–236; 15 U.S.C. 272 note) is amended by striking "under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451)" and

inserting "under section 303 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274)".

(C) Section 302(f) of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442(f)) is amended by striking "under section 401" and inserting "under section 303".

SEC. 9402. DEVELOPMENT OF STANDARDS AND GUIDELINES FOR IMPROVING CYBERSECURITY WORKFORCE OF FEDERAL AGENCIES.

(a) IN GENERAL.—Section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)) is amended—

(1) in paragraph (3), by striking "; and" and inserting a semicolon;

(2) in paragraph (4), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(5) identify and develop standards and guidelines for improving the cybersecurity workforce for an agency as part of the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181), or successor framework.".

Deadline.
15 USC 278g–3 note.

(b) PUBLICATION OF STANDARDS AND GUIDELINES ON CYBERSECURITY AWARENESS.—Not later than three years after the date of the enactment of this Act and pursuant to section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), the Director of the National Institute of Standards and Technology shall publish standards and guidelines for improving cybersecurity awareness of employees and contractors of Federal agencies.

SEC. 9403. MODIFICATIONS TO FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

Section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442) is amended—

(1) in subsection (b)—

(A) in paragraph (2), by striking "information technology" and inserting "information technology and cybersecurity";

(B) by amending paragraph (3) to read as follows:

"(3) prioritize the placement of scholarship recipients fulfilling the post-award employment obligation under this section to ensure that—

"(A) not less than 70 percent of such recipients are placed in an executive agency (as defined in section 105 of title 5, United States Code);

"(B) not more than 10 percent of such recipients are placed as educators in the field of cybersecurity at qualified institutions of higher education that provide scholarships under this section; and

"(C) not more than 20 percent of such recipients are placed in positions described in paragraphs (2) through (5) of subsection (d); and"; and

(C) in paragraph (4), in the matter preceding subparagraph (A), by inserting ", including by seeking to provide awards in coordination with other relevant agencies for summer cybersecurity camp or other experiences, including teacher training, in each of the 50 States," after "cybersecurity education";

(2) in subsection (d)—

(A) in paragraph (4), by striking "or" at the end;

(B) in paragraph (5), by striking the period at the end and inserting "; or"; and

(C) by adding at the end the following:

"(6) as provided by subsection (b)(3)(B), a qualified institution of higher education."; and

(3) in subsection (m)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking "cyber" and inserting "cybersecurity"; and

(B) in paragraph (2), by striking "cyber" and inserting "cybersecurity".

SEC. 9404. ADDITIONAL MODIFICATIONS TO FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

Section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442) is further amended—

(1) in subsection (f)—

(A) in paragraph (4), by striking "and" after the semicolon; and

(B) by striking paragraph (5) and inserting the following:

"(5) enter into an agreement accepting and acknowledging the post award employment obligations, pursuant to section (d); Contracts.

"(6) accept and acknowledge the conditions of support under section (g); and

"(7) accept all terms and conditions of a scholarship under this section.";

(2) in subsection (g)—

(A) in paragraph (1), by inserting "the Office of Personnel Management (in coordination with the National Science Foundation) and" before "the qualified institution";

(B) in paragraph (2)—

(i) in subparagraph (D), by striking "or" after the semicolon; and

(ii) by striking subparagraph (E) and inserting the following:

"(E) fails to maintain or fulfill any of the post-graduation or post-award obligations or requirements of the individual; or

"(F) fails to fulfill the requirements of paragraph (1).";

(3) in subsection (h)(2), by inserting "and the Director of the Office of Personnel Management" after "Foundation";

(4) in subsection (k)(1)(A), by striking "and the Director" and all that follows through "owed" and inserting ", the Director of the National Science Foundation, and the Director of the Office of Personnel Management of the amounts owed"; and

(5) in subsection (m)(2), by striking "once every 3 years" and all that follows through "workforce" and inserting "once every two years, to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Science, Space, and Technology and the Committee on Oversight and Reform of the House of Representatives a report, including— Time period.

"(A) the results of the evaluation under paragraph (1);

"(B) the disparity in any reporting between scholarship recipients and their respective institutions of higher education; and

"(C) any recent statistics regarding the size, composition, and educational requirements of the Federal cyber workforce.".

SEC. 9405. CYBERSECURITY IN PROGRAMS OF THE NATIONAL SCIENCE FOUNDATION.

(a) COMPUTER SCIENCE AND CYBERSECURITY EDUCATION RESEARCH.—Section 310 of the American Innovation and Competitiveness Act (42 U.S.C. 1862s–7) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by inserting "and cybersecurity" after "computer science"; and

(B) in paragraph (2)—

(i) in subparagraph (C), by striking " and" after the semicolon;

(ii) in subparagraph (D), by striking the period at the end and inserting "; and"; and

(iii) by adding at the end the following:

"(E) tools and models for the integration of cybersecurity and other interdisciplinary efforts into computer science education and computational thinking at secondary and postsecondary levels of education."; and

(2) in subsection (c), by inserting ", cybersecurity," after "computing".

(b) SCIENTIFIC AND TECHNICAL EDUCATION.—Section 3(j)(9) of the Scientific and Advanced-Technology Act of 1992 (42 U.S.C. 1862i(j)(9)) is amended by inserting "and cybersecurity" after "computer science".

(c) LOW-INCOME SCHOLARSHIP PROGRAM.—Section 414(d) of the American Competitiveness and Workforce Improvement Act of 1998 (42 U.S.C. 1869c) is amended—

(1) in paragraph (1), by striking "or computer science" and inserting "computer science, or cybersecurity"; and

(2) in paragraph (2)(A)(iii), by inserting "cybersecurity," after "computer science,".

42 USC 1862s–6 note.

(d) PRESIDENTIAL AWARDS FOR TEACHING EXCELLENCE.—The Director of the National Science Foundation shall ensure that educators and mentors in fields relating to cybersecurity can be considered for—

(1) Presidential Awards for Excellence in Mathematics and Science Teaching made under section 117 of the National Science Foundation Authorization Act of 1988 (42 U.S.C. 1881b); and

(2) Presidential Awards for Excellence in STEM Mentoring administered under section 307 of the American Innovation and Competitiveness Act (42 U.S.C. 1862s–6).

51 USC 40901 note prec.

SEC. 9406. CYBERSECURITY IN STEM PROGRAMS OF THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION.

In carrying out any STEM education program of the National Aeronautics and Space Administration (referred to in this section as "NASA"), including a program of the Office of STEM Engagement, the Administrator of NASA shall, to the maximum extent

practicable, encourage the inclusion of cybersecurity education opportunities in such program.

SEC. 9407. NATIONAL CYBERSECURITY CHALLENGES.

(a) IN GENERAL.—Title II of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7431 et seq.) is amended by adding at the end the following:

"SEC. 205. NATIONAL CYBERSECURITY CHALLENGES. 15 USC 7432.

"(a) ESTABLISHMENT OF NATIONAL CYBERSECURITY CHALLENGES.—

"(1) IN GENERAL.—To achieve high-priority breakthroughs in cybersecurity by 2028, the Secretary of Commerce shall establish the following national cybersecurity challenges:

"(A) ECONOMICS OF A CYBER ATTACK.—Building more resilient systems that measurably and exponentially raise adversary costs of carrying out common cyber attacks.

"(B) CYBER TRAINING.—

"(i) Empowering the people of the United States with an appropriate and measurably sufficient level of digital literacy to make safe and secure decisions online.

"(ii) Developing a cybersecurity workforce with measurable skills to protect and maintain information systems.

"(C) EMERGING TECHNOLOGY.—Advancing cybersecurity efforts in response to emerging technology, such as artificial intelligence, quantum science, next generation communications, autonomy, data science, and computational technologies.

"(D) REIMAGINING DIGITAL IDENTITY.—Maintaining a high sense of usability while improving the privacy, security, and safety of online activity of individuals in the United States.

"(E) FEDERAL AGENCY RESILIENCE.—Reducing cybersecurity risks to Federal networks and systems, and improving the response of Federal agencies to cybersecurity incidents on such networks and systems.

"(2) COORDINATION.—In establishing the challenges under paragraph (1), the Secretary shall coordinate with the Secretary of Homeland Security on the challenges under subparagraphs (B) and (E) of such paragraph.

"(b) PURSUIT OF NATIONAL CYBERSECURITY CHALLENGES.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary, acting through the Under Secretary of Commerce for Standards and Technology, shall commence efforts to pursue the national cybersecurity challenges established under subsection (a). Deadline.

"(2) COMPETITIONS.—The efforts required by paragraph (1) shall include carrying out programs to award prizes, including cash and noncash prizes, competitively pursuant to the authorities and processes established under section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719) or any other applicable provision of law.

"(3) ADDITIONAL AUTHORITIES.—In carrying out paragraph (1), the Secretary may enter into and perform such other transactions as the Secretary considers necessary and on such terms as the Secretary considers appropriate.