I

117TH CONGRESS
1ST SESSION

H. R. 4985

To implement certain recommendations of the National Security Commission on Artificial Intelligence.

IN THE HOUSE OF REPRESENTATIVES

AUGUST 6, 2021

Mr. VELA introduced the following bill; which was referred to the Committee on Armed Services, and in addition to the Committees on Intelligence (Permanent Select), Foreign Affairs, Transportation and Infrastructure, and Oversight and Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To implement certain recommendations of the National Security Commission on Artificial Intelligence.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Digital Defense Leadership Act''.

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

Sec. 1. Short title; table of contents.
Sec. 2. National strategy relating to the global information domain.
Sec. 3. Artificial intelligence readiness goals.

Sec. 4. Role of intelligence community in steering committee on emerging technology.
Sec. 5. Resourcing plan for digital ecosystem.
Sec. 6. Integrating digital skill sets and computational thinking into military junior leader education.
Sec. 7. Integration of material on emerging technologies into professional military education.
Sec. 8. Short course on emerging technologies for senior personnel of the Department of Defense.
Sec. 9. Emerging technology-coded billets within the Department of Defense.
Sec. 10. Agile contracting mechanism for software acquisition.
Sec. 11. Enhanced role of Under Secretary of Defense for Research and Engineering on the Joint Requirements Oversight Council.
Sec. 12. Artificial Intelligence Development and Prototyping Fund.
Sec. 13. Enhanced authority to enter into cooperative research and development agreements with international partners.
Sec. 14. Role of Director of Science and Technology as Chief Technology Officer for the intelligence community.
Sec. 15. Establishment of Artificial Intelligence Critical Applications Fund.
Sec. 16. Artificial intelligence technology roadmap and funding plan for the intelligence community.
Sec. 17. Digital expertise recruiting offices.
Sec. 18. Occupational series relating to artificial intelligence and digital career fields.
Sec. 19. Military career fields for software development, data science, and artificial intelligence.

SEC. 2. NATIONAL STRATEGY RELATING TO THE GLOBAL INFORMATION DOMAIN.

(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this section, the President shall transmit to Congress a national strategy relating to the global information domain to—

(1) address such domain as a component of the national security of the United States; and

(2) ensure the United States leads in the development of technologies and tactics applicable to such domain.

(b) ELEMENTS.—The strategy required under subsection (a) shall, at a minimum—

(1) prioritize the global information domain as an area for international competition with respect to foreign adversaries;

(2) detail how such adversaries, as well as nonstate actors, are attempting to influence and control such domain to shape global opinion and achieve strategic advantage;

(3) account for the critical role of artificial intelligence-enabled malign information in the activities of such adversaries and nonstate actors referred to in paragraph (2);

(4) identify and prioritize actions to defend, counter, and compete in such domain, including recommendations with respect to—

(A) changing the priorities of the national security agencies of the United States; and

(B) establishing new national security agencies to prioritize such actions; and

(5) provide recommendations, including any suggestions for legislation, with respect to updating—

(A) critical infrastructure designations; and

(B) sector-specific plans to account for emerging technologies, including artificial intelligence.

(c) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given such 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) ARTIFICIAL INTELLIGENCE-ENABLED MALIGN INFORMATION.—The term ''artificial intelligence-enabled malign information'' refers to a broad range of applications in which artificial intelligence is used to generate, spread, or target disinformation, or otherwise control or manipulate the flow and substance of information in the global information domain.

(3) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(4) FOREIGN ADVERSARY.—The term ''foreign adversary'' means a foreign government engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the

United States or security and safety of United States persons.

(5) GLOBAL INFORMATION DOMAIN.—The term ''global information domain'' means a sphere of strategic competition in which foreign adversaries and nonstate actors create, obtain, fuse, analyze, distort, transfer, exchange, or disseminate information, overtly or covertly, to influence public opinion for national security, geopolitical, or economic purposes.

SEC. 3. ARTIFICIAL INTELLIGENCE READINESS GOALS.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall—

(1) review the potential applications of artificial intelligence and digital technology to the platforms, processes, and operations of the Department of Defense; and

(2) establish performance objectives and accompanying metrics for the incorporation of artificial intelligence and digital readiness into such platforms, processes, and operations.

(b) SKILLS GAPS.—As a part of the review required by subsection (a), the Secretary shall direct the military departments and other relevant organizations and elements of the Department of Defense to—

(1) conduct a comprehensive review of skill gaps in the fields of software development, software engineering, knowledge management, data science, and artificial intelligence;

(2) assess the number and qualifications of civilian personnel needed for both management and specialist tracks in such fields;

(3) assess the number of military personnel (including officers and enlisted members of the Armed Forces) needed for both management and specialist tracks in such fields; and

(4) establish recruiting, training, and talent management goals to achieve and maintain the staffing levels needed to fill identified gaps and meet the Department's needs for skilled personnel.

(c) REPORT TO CONGRESS.—Not later than 120 days after the completion of the review required by subsection (a), the Secretary of Defense shall submit to Congress a report on the findings of the review and any actions taken or proposed to be taken by the Secretary to address such findings.

SEC. 4. ROLE OF INTELLIGENCE COMMUNITY IN STEERING COMMITTEE ON EMERGING TECHNOLOGY.

Section 236 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283), is amended—

(1) in subsection (b)—

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

(B) by inserting after paragraph (7) the following new paragraph:

''(8) One or more representatives of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), which shall include, at a minimum, the Principal Deputy Director of National Intelligence.'';

(2) by redesignating subsection (c) as subsection (d); and

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

''(c) CHAIRPERSONS.—The Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence shall serve as Co-Chairpersons of the Steering Committee.''.

SEC. 5. RESOURCING PLAN FOR DIGITAL ECOSYSTEM.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall develop a plan for the development of a modern digital ecosystem that uses state-of-the-art tools and modern processes to enable the development, testing, fielding, and continuous updating of artificial intelligence-powered applications at speed and scale from headquarters to the tactical edge.

(b) CONTENTS OF PLAN.—At a minimum, the plan required by subsection (a) shall include—

(1) an open architecture and an evolving reference design and guidance for needed technical investments in the proposed ecosystem that address issues including common interfaces, authentication, applications, platforms, software, hardware, and data infrastructure; and

(2) a governance structure, together with associated policies and guidance, to drive the implementation of the reference throughout the Department on a federated basis.

SEC. 6. INTEGRATING DIGITAL SKILL SETS AND COMPUTATIONAL THINKING INTO MILITARY JUNIOR LEADER EDUCATION.

(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Chiefs of the Armed

Forces shall expand the curriculum for military junior leader education to include the following:

(1) Problem definition and curation.

(2) A conceptual understanding of the artificial intelligence lifecycle.

(3) Data collection and management.

(4) Probabilistic reasoning and data visualization.

(5) Data-informed decision making.

(b) RESOURCES.—In carrying out subsection (a), the Chiefs shall use existing artificial intelligence-enabled systems and tools to the extent possible.

SEC. 7. INTEGRATION OF MATERIAL ON EMERGING TECHNOLOGIES INTO PROFESSIONAL MILITARY EDUCATION.

Not later than one year after the date of the enactment of this Act, the Secretary of Defense, in consultation with the Joint Chiefs of Staff, shall ensure that the curriculum for professional military education for each Armed Force under the jurisdiction of the Secretary of a military department includes periodic courses on militarily significant emerging technologies that expand the knowledge base, vocabulary, and skills necessary to intelligently analyze and use emerging technologies in the tactical, oper-

ational, and strategic levels of warfighting and warfighting support.

SEC. 8. SHORT COURSE ON EMERGING TECHNOLOGIES FOR SENIOR PERSONNEL OF THE DEPARTMENT OF DEFENSE.

(a) ESTABLISHMENT.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall establish a short course on emerging technologies for covered personnel. The short course shall be taught on an iterative, two-year cycle and shall address how the most recent and relevant technologies may be applied to military and business outcomes in the Department of Defense.

(b) OBJECTIVES.—In assessing participation in the short course under subsection (a), the Secretary shall ensure that—

(1) in the first year that the course is offered, at least 20 percent of covered personnel pass the short course; and

(2) in each subsequent year, an additional 10 percent of covered personnel pass the such course, until 80 percent of covered personnel have passed.

(c) COVERED PERSONNEL DEFINED.—In this section, the term ''covered personnel'' means—

(1) officers in—

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

(B) a grade above O-6; and

(2) civilian employees of the Department of Defense in the Senior Executive Service.

SEC. 9. EMERGING TECHNOLOGY-CODED BILLETS WITHIN THE DEPARTMENT OF DEFENSE.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall ensure that each Armed Force under the jurisdiction of the Secretary of a military department—

(1) develop a process to qualify officers on emerging technology; and

(2) establishes billets for officers qualified under such process; and

(b) QUALIFICATION PROCESS.—The process under subsection (a)(1) shall be modeled on a streamlined version of the joint qualification process and may include credit for serving in the following:

(1) Fellowships focused on emerging technology.

(2) Talent exchanges focused on emerging technology.

(3) Federal occupations focused on emerging technology.

(4) Educational courses focused on emerging technologies.

(c) APPROPRIATE BILLETS.—Billets under subsection (a)(2) may include the following duties:

(1) Acquisition of emerging technologies.

(2) Integrating technology into field units.

(3) Developing organizational and operational concepts.

(4) Developing training and educational plans.

(5) Operational and tactical leadership.

SEC. 10. AGILE CONTRACTING MECHANISM FOR SOFTWARE ACQUISITION.

(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall establish an agile contracting mechanism to support any software acquisition pathway developed pursuant to section 800 of the National Defense Authorization Act for Fiscal Year 2020 (10 U.S.C. 2223a note).

(b) CHARACTERISTICS.—The agile contracting mechanism established pursuant to subsection (a) shall authorize processes pursuant to which—

(1) a contract is awarded on the basis of statements of qualifications and past performance data

submitted by offerors, supplemented by discussions with two or more offerors determined to be the most highly qualified offerors, without regard to price;

(2) the contract terms identify the persons to be engaged for the work, and substitutions shall not be made during the base contract period without the advance written consent of the contracting officer;

(3) the contractor reviews existing software in consultation with the user community and utilizes user feedback to define and prioritize software requirements, and to design and implement new software and software upgrades, as appropriate;

(4) an independent cost estimate is developed in parallel with engineering of the software; and

(5) performance metrics based on the value of the software to be acquired are established to address issues such as development, delivery, and deployment rates of software and software updates, and assessment and estimation of the size and complexity of the life cycle of such software.

SEC. 11. ENHANCED ROLE OF UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING ON THE JOINT REQUIREMENTS OVERSIGHT COUNCIL.

Section 181 of title 10, United States Code, is amended—

(1) in subsection (b)—

(A) in the matter preceding paragraph (1), by inserting ''the Secretary of Defense and'' before ''the Chairman of the Joint Chiefs of Staff'';

(B) by redesignating paragraphs (2) through (6) as paragraphs (3) through (7);

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

''(2) leveraging awareness of global technology trends, threats, and adversary capabilities to address gaps in joint military capabilities and validate the technical feasibility of requirements developed by the armed forces;'';

(D) in paragraph (4)(B), as so redesignated, by inserting ''the Secretary of Defense and'' before ''the Chairman of the Joint Chiefs of Staff''; and

(E) in paragraph (5), as so redesignated, by inserting ''the Secretary of Defense and'' be-

fore ''the Chairman of the Joint Chiefs of Staff'';

(2) in subsection (c)—

(A) in paragraph (1)—

(i) in subparagraph (A), by striking ''Chairman of the Joint Chiefs of Staff for making recommendations about'' and inserting ''Council for'';

(ii) by redesignating subparagraphs (B) through (F) as subparagraphs (C) through (G), respectively; and

(iii) by inserting after subparagraph (A) the following new subparagraph:

''(B) The Under Secretary of Defense for Research and Engineering, who is the Co-Chair of the Council and is the chief science advisor to the Council.'';

(B) in paragraph (2), by striking ''(B), (C), (D), and (E)'' and inserting ''(C), (D), (E), and (F)''; and

(C) by amending paragraph (3) to read as follows:

''(3) In making any recommendation to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff pursuant to this section, the Co-

Chairs of the Council shall provide any dissenting view of members of the Council with respect to such recommendation.''; and

(3) in subsection (d)(1)—

(A) by striking subparagraph (D); and

(B) by redesignating subparagraphs (E) through (H) as paragraphs (D) through (G), respectively.

SEC. 12. ARTIFICIAL INTELLIGENCE DEVELOPMENT AND PROTOTYPING FUND.

(a) IN GENERAL.—The Secretary of Defense shall establish a fund to be known as the ''Artificial Intelligence Development and Prototyping Fund'' to support operational prototyping and speed the transition of artificial intelligence-enabled applications into both service-specific and joint mission capabilities, with priority given to joint mission capabilities for combatant commanders. The Fund shall be managed by the Under Secretary of Defense for Research and Engineering, in consultation with the Director of the Joint Artificial Intelligence Center, the head of the Joint Staff, and the Chief of each Armed Force.

(b) TRANSFER AUTHORITY.—Amounts available in the Fund may be transferred to the Secretary of a military department for the purpose of carrying out a development or prototyping program selected by the Under Secretary

of Defense for Research and Engineering for the purposes described in subsection (a). Any amount so transferred shall be credited to the account to which it is transferred. The transfer authority provided in this subsection is in addition to any other transfer authority available to the Department of Defense.

(c) NOTICE TO CONGRESS.—The Under Secretary of Defense for Research and Development shall notify the congressional defense committees (as defined in section 101(a)(16) of title 10, United States Code) of all transfers under subsection (b). Each notification shall specify the amount transferred, the purpose of the transfer, and the total projected cost and estimated cost to complete the acquisition program to which the funds were transferred.

SEC. 13. ENHANCED AUTHORITY TO ENTER INTO COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENTS WITH INTERNATIONAL PARTNERS.

(a) AUTHORITY OF SECRETARY OF DEFENSE.—Section 2350a of title 10, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (2), by adding at the end the following:

''(F) Any business, academic institution, research institution, or other nongovernmental entity organized pursuant to the laws of a country referred

to in subparagraphs (C), (D), and (E), subject to the consent of the country involved.'';

(B) in paragraph (3), by striking ''a country referred to in subparagraph (E) of paragraph (2),'' and inserting ''a country referred to in subparagraph (E) of paragraph (2) or a non-governmental entity referred to in subparagraph (F) of such paragraph,''; and

(C) by adding at the end the following:

''(4) The Secretary may delegate the authority to enter memoranda of understanding pursuant to this section to the secretary of a military department, the Director of the Joint Artificial Intelligence Center, and the Director of the Defense Advanced Research Projects Agency, subject to such terms and conditions as may be necessary to ensure that any agreements entered are consistent with the foreign policy and defense policy of the United States.'';

(2) in subsection (b)(1), by striking ''will improve, through the application of emerging technology,'' and inserting ''is likely to improve, through the application or enhancement of emerging technology,''; and

(3) in subsection (c)(3), by inserting at the end the following: ''If a foreign partner is expected to

contribute significantly to the development of a new or novel capability, full consideration shall be given to nonmonetary contributions, including the value of research and development capabilities and the strategic partnerships.''.

(b) AUTHORITY OF THE PRESIDENT.—Section 2767 of title 22, United States Code, is amended—

(1) in subsection (c), by adding at the end the following: ''If a foreign partner is expected to contribute significantly to the development of a new or novel capability, full consideration shall be given to non-monetary contributions, including the value of research and development capabilities and the strategic partnerships.'';

(2) in subsection (f)(4), by inserting ''(and a description of any nonmonetary contributions made by such participants)'' before the semicolon; and

(3) in subsection (j)—

(A) by amending the subsection heading to read as follows: ''COOPERATIVE PROJECT AGREEMENTS WITH FRIENDLY FOREIGN COUNTRIES NOT MEMBERS OF NATO AND WITH NONGOVERNMENTAL ORGANIZATIONS IN NATO AND IN FRIENDLY NON-NATO COUNTRIES''; and

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

''(2) The President may enter into a cooperative project agreement with any business, academic institution, research institution, or other nongovernmental entity organized pursuant to the laws of a NATO member or a friendly foreign country that is not a member of NATO, subject to the consent of the country involved.''.

SEC. 14. ROLE OF DIRECTOR OF SCIENCE AND TECHNOLOGY AS CHIEF TECHNOLOGY OFFICER FOR THE INTELLIGENCE COMMUNITY.

Section 103E(c) of the National Security Act of 1947 (50 U.S.C. 3030(c)) is amended—

(1) by redesignating paragraphs (2) through (5) as paragraphs (5) through (8), respectively; and

(2) by inserting after paragraph (1) the following new paragraphs:

''(2) serve as the Chief Technology Officer for the intelligence community;

''(3) establish policies for the intelligence community on research and engineering, technology development, technology transition, prototyping activities, experimentation, and developmental testing, and oversee the implementation of such policies;

''(4) establish common technical standards and policies necessary to rapidly scale artificial intelligence-enabled applications across the intelligence community;''.

SEC. 15. ESTABLISHMENT OF ARTIFICIAL INTELLIGENCE CRITICAL APPLICATIONS FUND.

(a) ESTABLISHMENT.—The Director of National Intelligence shall establish in the Treasury a fund, to be known as the ''Artificial Intelligence Critical Applications Fund'', for the purposes of supporting the development and acquisition of applications enabled by artificial intelligence for use by the intelligence community.

(b) MANAGEMENT.—The Director of Science and Technology appointed under section 103E of the National Security Act of 1947 (50 U.S.C. 3030), in consultation with the Director of National Intelligence Science and Technology Committee specified in such section, shall be responsible for the management of the Artificial Intelligence Critical Applications Fund.

(c) AUTHORITY TO TRANSFER AMOUNTS.—

(1) TRANSFER AUTHORITY.—The Director of National Intelligence may transfer amounts from the Artificial Intelligence Critical Applications Fund to the head of any element of the intelligence community, to be merged with amounts otherwise available

under the account to which transferred, for the purpose of carrying out a program selected by the Director of Science and Technology for the purposes described in subsection (a). Any amount so transferred shall be credited to the account to which it was transferred.

(2) ADDITIONAL TRANSFER AUTHORITY.—The transfer authority in paragraph (1) is in addition to any other transfer authority provided to the Director of National Intelligence or the head of any element of the intelligence community.

(d) CONGRESSIONAL NOTIFICATION.—Upon making a transfer pursuant to subsection (c), the Director of National Intelligence shall submit to the appropriate congressional committees a notification of the transfer. Each notification shall include an identification of the following:

(1) The amount transferred.

(2) The purpose of the transfer.

(3) The total projected cost and estimated cost to complete the program for which the transferred amounts will be used.

(e) DEFINITIONS.—In this section:

(1) The term ''appropriate congressional committees'' means—

(A) the congressional intelligence committees; and

(B) the Committees on Appropriations of the House of Representatives and the Senate.

(2) The term ''artificial intelligence'' has the meaning given such term in section 238 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note).

(3) The terms ''congressional intelligence committees'' and ''intelligence community'' have the meaning given those term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 16. ARTIFICIAL INTELLIGENCE TECHNOLOGY ROADMAP AND FUNDING PLAN FOR THE INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Secretary of Defense, shall develop a technology annex to the National Intelligence Strategy and a 10-year plan to provide long-term, predictable funding of up to $1,000,000,000 to implement the steps identified in such annex.

(b) CONTENTS OF TECHNOLOGY ANNEX.—The technology annex under subsection (a) shall provide a technology roadmap for the adoption of artificial intelligence-

enabled applications to solve operational intelligence requirements, including—

(1) a description of challenges faced in the efforts of the intelligence community to analyze the global environment and monitor technological advancements, adversarial capability development, and emerging threats;

(2) identification of technical capabilities, including artificial intelligence capabilities, needed to enable steps to address each challenge;

(3) a prioritized, time-phased plan for developing or acquiring such technical capabilities, that takes into account research and development timelines, a strategy for public private partnerships, and a strategy for connecting researchers to end users for early prototyping, experimentation, and iteration;

(4) any additional or revised acquisition policies and workforce training requirements that may be needed to enable personnel of the intelligence community to identify, procure, integrate, and operate the technologies identified in the annex;

(5) identification of infrastructure requirements for developing and deploying technical capabilities, including—

(A) data, compute, storage, and network needs;

(B) a resourced and prioritized plan for establishing such infrastructure; and

(C) an analysis of the testing, evaluation, verification, and validation requirements to support prototyping and experimentation and a resourced plan to implement them, including standards, testbeds, and red-teams for testing artificial intelligence systems against digital ''denial and deception'' attacks;

(6) consideration of human factor elements associated with priority technical capabilities, including innovative human-centric approaches to user interface, human-machine teaming, and workflow integration;

(7) consideration of interoperability with allies and partners of the United States, including areas for sharing of data, tools, and intelligence products; and

(8) flexibility to adapt and iterate annex implementation at the speed of technological advancement.

(c) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the mean-

ing given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 17. DIGITAL EXPERTISE RECRUITING OFFICES.

(a) DIGITAL EXPERTISE RECRUITING FOR THE DEPARTMENT OF DEFENSE.—

(1) ESTABLISHMENT.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall designate a chief digital recruiting officer within the office of the Under Secretary of Defense for Personnel and Readiness to oversee a digital recruiting office to carry out the responsibilities set forth in paragraph (2).

(2) DUTIES.—The chief digital recruiting officer shall be responsible for—

(A) identifying needs within the Department of Defense for specific types of digital expertise;

(B) recruiting technologists in partnership with the heads of elements of the Department, including by attending conferences and career fairs, and actively recruiting on university campuses and from the private sector;

(C) integrating Federal scholarship for service programs into civilian recruiting;

(D) offering recruitment and referral bonuses; and

(E) partnering with human resource teams in the elements of the Department to use direct-hire authorities to accelerate hiring.

(3) RESOURCES.—The Secretary of Defense shall ensure that the chief digital recruiting officer is provided with personnel and resources sufficient to maintain an office and to carry out the duties set forth in paragraph (2).

(b) DIGITAL EXPERTISE RECRUITING FOR THE INTELLIGENCE COMMUNITY.—

(1) ESTABLISHMENT.—Not later than 270 days after the date of the enactment of this Act, the Director of National Intelligence shall designate a chief digital recruiting officer to oversee a digital recruiting office to carry out the responsibilities set forth in paragraph (2).

(2) DUTIES.—The chief digital recruiting officer shall be responsible for—

(A) identifying needs within the intelligence community for specific types of digital expertise;

(B) recruiting technologists, in partnership with the heads of the elements of the intel-

ligence community, including by attending conferences and career fairs, and actively recruiting on university campuses and from the private sector;

(C) integrating Federal scholarship for service programs into intelligence community recruiting;

(D) offering recruitment and referral bonuses; and

(E) partnering with human resource teams in the elements of the intelligence community to use direct-hire authorities to accelerate hiring.

(3) RESOURCES.—The Director of National Intelligence shall ensure that the chief digital recruiting officer is provided with personnel and resources sufficient to maintain an office and to carry out the duties set forth in paragraph (2).

(4) INTELLIGENCE COMMUNITY DEFINED.—In this subsection, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 18. OCCUPATIONAL SERIES RELATING TO ARTIFICIAL INTELLIGENCE AND DIGITAL CAREER FIELDS.

(a) DIGITAL CAREER FIELDS.—Not later than 270 days after the date of the enactment of this Act, the Director of the Office of Personnel Management shall exercise the authority of the Director under section 5105 of title 5, United States Code, to establish one or more new occupational series and associated policies covering Federal Government positions in the fields of software development, software engineering, data science, and knowledge management.

(b) ARTIFICIAL INTELLIGENCE FIELDS.—Not later than 270 days after the date of the enactment of this Act, the Director of the Office of Personnel Management shall exercise the authority of the Director under section 5105 of title 5, United States Code, to establish a new occupational series and associated policies covering Federal Government positions in the field of artificial intelligence.

SEC. 19. MILITARY CAREER FIELDS FOR SOFTWARE DEVELOPMENT, DATA SCIENCE, AND ARTIFICIAL INTELLIGENCE.

Section 230 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 10 U.S.C. 501 note prec.) is amended by adding at the end the following new subsection:

''(d) CAREER FIELDS.—Not later than 270 days after the date of the enactment of the Digital Defense Leadership Act, each Chief of an Armed Force shall establish new military career fields—

''(1) for software development, data science, and artificial intelligence for members and officers under the jurisdiction of such Chief; and

''(2) that are designated competitive categories for promotion under subchapter VI of chapter 36 of title 10, United States Code.''.

○