# H.R. 8070—SERVICEMEMBER QUALITY OF LIFE IMPROVEMENT AND NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2025

# SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

# SUMMARY OF BILL LANGUAGE

# Table Of Contents



---

## DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

# TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

## LEGISLATIVE PROVISIONS

### SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

#### Section 212—Modification to Defense Laboratory Education Partnerships

This section would modify educational partnership agreements to allow for defense laboratories to enter into direct financing agreements.

#### Section 213—Modification to Personnel Management Authority to Attract Experts in Science and Engineering

This section would improve the ability of the Defense Innovation Unit to attract and more rapidly hire new types of staff.

#### Section 216—Agility Prime Transition Working Group

This section would establish a working group to assist in the transition of hybrid and electric vertical take-off and landing technologies developed under the Air Force's Agility Prime program.

#### Section 217—Measures to Advance Quantum Information Science within the Department of Defense

This section would require the Secretary of Defense to develop a strategic plan to guide the development and maturation of quantum information sciences technologies within the Department of Defense and military services. In addition, this section would require the Secretary to establish a center of excellence for quantum computing at an existing military service laboratory.

#### Section 218—Authority to Temporarily Detail Employees of the Office of Strategic Capital to Certain Private-Sector Organizations

This section would allow the Office of Strategic Capital to administer and manage a program for the Department of Defense to place military and civilian personnel in temporary assignments with the private sector in industries related to the work of the Office of Strategic Capital.

#### Section 219—Pilot Program on Establishment of a Test and Evaluation Cell within the Defense Innovation Unit

This section would set up a pilot program within the Defense Innovation Unit to conduct test and evaluation.

### SUBTITLE C—PLANS, REPORTS, AND OTHER MATTERS

#### Section 221—Plan for Establishment of Secure Computing and Data Storage Environment for Testing of Artificial Intelligence Trained on Biological Data

This section would require the Under Secretary of Defense for Research and Engineering, in coordination with the Chief Digital and Artificial Intelligence Officer, to submit an implementation plan, not later than 1 year after the date of the enactment of this Act, on the feasibility of establishing a secure computing and data storage environment to facilitate the testing of artificial intelligence models trained on biological data and the development and testing of products generated by such models.

#### Section 222—Study and Report on Foreign Capital Disclosure Requirements of Certain Department of Defense Organizations

This section would require the Secretary of Defense to conduct a study and report to Congress on the foreign capital disclosure requirements of innovation organizations within the Department.

#### Section 223—Biotechnology Roadmap

This section would require that not later than 1 year after the date of the enactment of this Act, and not less frequently than once every 2 years thereafter, the Secretary of Defense would be required to develop a biotechnology roadmap to guide efforts of the Department of Defense relating to biotechnology.

## TITLE XV—CYBERSPACE-RELATED MATTERS

### LEGISLATIVE PROVISIONS

### SUBTITLE A—CYBER OPERATIONS

#### Section 1501—Authority to Accept Voluntary and Uncompensated Services from Cybersecurity Experts

This section would provide the legal authority for the military services to accept voluntary and uncompensated services from civilian cybersecurity experts to train servicemembers on technical matters. It would solidify the legal basis for the United States Marine Corps Cyber Auxiliary program, as well as enable the other military services to establish their own Cyber Auxiliary programs. This section builds on committee report language titled "Cyber Auxiliary Utilization," which accompanied the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263).

## SUBTITLE B—CYBERSECURITY

### Section 1511—Protective Measures for Mobile Devices within the Department of Defense

This section would require the Secretary of Defense to perform a detailed evaluation of products and services specifically aimed to improve the cybersecurity of mobile devices within the Department of Defense.

## SUBTITLE C—INFORMATION TECHNOLOGY AND DATA MANAGEMENT

### Section 1521—Usability of Antiquated Data Formats for Modern Operations

This section would require the Secretary of Defense and the Secretaries of the military departments to develop both a strategy and roadmap to optimize and improve the Department of Defense's reliance on antiquated data formats.

### Section 1522—Modernization of the Department of Defense's Authorization to Operate Processes

This section would require the Department of Defense to take actions directed at improving and streamlining the processes regarding the "Authority to Operate" for information technology.

## SUBTITLE D—REPORTS AND OTHER MATTERS

### Section 1531—Access to National Suicide Prevention and Mental Health Crisis Hotline System

This section would require the Department of Defense Chief Information Officer to implement access to the national suicide prevention and mental health crisis hotline from all Department facilities and report to Congress when complete.

### Section 1532—Oversight and Reporting on the Mission Partner Environment and Associated Activities within the Department of Defense

This section would establish an improved oversight mechanism for the Department of Defense activities related to the Mission Partner Environment (MPE). Until 2030, the Department would have to brief the congressional defense committees twice annually on MPE developments.

# BILL LANGUAGE

**SEC. 212 [Log 80324]. MODIFICATION TO DEFENSE LABORATORY EDUCATION PARTNERSHIPS.**

Section 2194(b) of title 10, United States Code, is amended—

(1) in paragraph (6), by striking ''and'' at the end;

(2) in paragraph (7), by striking the period at the end and inserting ''; and''; and

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

''(8) entering into contracts or cooperative agreements with, or making grants to, the institution to provide financial assistance for activities conducted under such partnership agreement.''.

**SEC. 213 [Log 80169]. MODIFICATION TO PERSONNEL MANAGEMENT AUTHORITY TO ATTRACT EXPERTS IN SCIENCE AND ENGINEERING.**

Section 4092(b) of title 10, United States Code, is amended—

(1) in paragraph (1)(E), by striking ''5 scientific and engineering positions in the Unit'' and inserting ''35 scientific and engineering positions in the Unit, of which not more than 5 such positions may be positions of administration or management of the Unit''; and

(2) in paragraph (2)(A)—

(A) in the matter preceding clause (i), by striking ''subparagraphs (B) and (H)'' and inserting ''subparagraphs (B), (E), and (H)''; and

(B) by amending clauses (i) and (ii) to read as follows:

''(i) to any of the 5 positions designated by the Director of the Defense Advanced Research Projects Agency, any of the 5 positions designated by the Director of the Space Development Agency, and any of the 5 positions designated by the Director of the Defense Innovation Unit for purposes of this clause, at rates not in excess

of a rate equal to 150 percent of the maximum rate of basic pay authorized for positions at Level I of the Executive Schedule under section 5312 of title 5; and

''(ii) to any other position designated by the Director of the Defense Advanced Research Projects Agency, the Director of the Space Development Agency, and the Director of the Defense Innovation Unit for purposes of this clause, at rates not in excess of the maximum amount of total annual compensation payable at the salary set in accordance with section 104 of title 3;''.

**SEC. 216 [Log 80193]. AGILITY PRIME TRANSITION WORKING GROUP.**

(a) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Air Force, in coordination with the Under Secretary of Defense for Acquisition and Sustainment and the Under Secretary of Defense for Research and Engineering, shall establish a working group to be known as the ''Agility Prime Transition Working Group'' (referred to in this section as the ''Working Group'').

(b) DUTIES.—The duties of the Working Group shall include the following:

(1) To develop and implement a strategy to transition capabilities developed under the Agility Prime program of the Air Force to program executive offices of the covered Armed Forces, as appropriate.

(2) To provide a forum for members of the Working Group to coordinate activities relating to hybrid and electric vertical takeoff and landing capabilities developed under the Agility Prime program, including—

(A) research, development, testing, and evaluation activities;

(B) demonstration activities; and

(C) activities to transition such capabilities from the research and development phase into operational use within the covered Armed Forces, as appropriate.

(3) To identify programs, projects, activities, and requirements of the covered Armed Forces that may be supported by technologies and capabilities developed under the Agility Prime program, including hybrid and electric vertical takeoff and landing aircraft, advanced air mobility platforms, autonomous flight capabilities, test and evaluation software, and related technologies.

(4) To identify requirements of the combatant commands and the covered Armed Forces relating to distributed and contested logistics, mobility and sustainment, intelligence, surveillance, and reconnaissance, strike, and other operational use cases that align with previous, ongoing, or planned efforts under the Agility Prime program.

(5) To assess whether previous, ongoing, or planned efforts under the Agility Prime program and other vertical take off and landing aircraft capability development efforts align with other current, planned, or future acquisition programs of the covered Armed Forces.

(6) Identify any changes to doctrine, organization, training, materiel, leadership, personnel, facilities, and policy (commonly known as ''DOTMLPF–P'') required to successfully integrate hybrid and electric vertical takeoff and landing aircraft platforms into future force design.

(7) To assess how the authorities and resources of the Department of Defense may be used to support the advanced air mobility and hybrid and electric vertical takeoff and landing aircraft industries, including support in the form of loans, loan guarantees, private investment matching programs, and other financial mechanisms.

(8) To assist the Secretary of the Air Force in preparing the briefing and reports required under subsection (g).

(c) MEMBERSHIP.—The Working Group shall be composed of the following members or their designees:

(1) The Secretary of the Air Force.

(2) Each Secretary of a military department.

(3) The Chairman of the Joint Chiefs of Staff.

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

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

(6) The Director of the Defense Innovation Unit.

(7) The Director of the Office of Strategic Capital.

(8) A representative from the United States Special Operations Command.

(9) A representative from the United States Transportation Command.

(10) Representatives of such other organizations and elements of the Department of Defense as the Chairperson of the Working Group determines appropriate.

(d) CHAIRPERSON.—The Secretary of the Air Force, or the designee of the Secretary, shall serve as the Chairperson of the Working Group.

(e) MEETINGS.—The Working Group shall meet not less frequently than twice each year at the call of the Chairperson.

(f) TERMINATION.—The working group shall terminate on September 30, 2027.

(g) BRIEFINGS AND REPORTS.—

(1) INITIAL BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Air Force shall provide to the congressional defense committees a briefing on the sta-

tus of the Working Group, which shall include information on the organization, activities, plans, actions, and milestones of the Working Group as of the date of the briefing.

(2) ANNUAL REPORT.—Not later than September 30, 2025, and not later than September 30 of each year thereafter through 2027, the Secretary of the Air Force shall submit to the congressional defense committees a report on the efforts of the Working Group. Each report shall include, with respect to the year covered by the report, information on—

(A) any funding under the categories of research, development, test, and evaluation, procurement, or operation and maintenance that is expected to be used for further development or procurement of hybrid and electric vertical takeoff and landing capabilities in the fiscal year of the report and the in the following fiscal year;

(B) any planned transitions of hybrid and electric vertical takeoff and landing technologies to—

(i) acqusition programs of the covered Armed Forces; or

(ii) research, development, test, and evaluation programs of the covered Armed Forces.

(C) any actions taken by the Working Group;

(D) any milestones achieved by the Working Group; and

(E) such other matters as the Secretary determines appropriate.

(h) DEFINITIONS.—In this section:

(1) The term ''Agility Prime program'' means the program of the Air Force under which the Air Force is developing hybrid and electric vertical take-off and landing capabilities in collaboration with partners in commercial industry and other sectors.

(2) The term ''covered Armed Forces'' means the Army, Navy, Air Force, Marine Corps, and Space Force.

**SEC. 217 [Log 80365]. MEASURES TO ADVANCE QUANTUM INFORMATION SCIENCE WITHIN THE DEPARTMENT OF DEFENSE.**

(a) STRATEGIC PLAN.—

(1) IN GENERAL.—The Secretary of Defense shall develop a strategic plan to guide the research, development, test, and evaluation, procurement, and implementation of quantum information science (referred to in this section as ''QIS'') technologies within the Department of Defense, including the covered Armed Forces, over the period of five years following the date of the enactment of this Act.

(2) ELEMENTS.—The plan required under paragraph (1) shall include the following:

(A) Identification of—

(i) QIS technologies that have the potential to solve operational challenges faced by the Department of Defense; and

(ii) the technology readiness levels of those QIS technologies.

(B) Plans to transition technologies identified under subparagraph (A) from the research, development, and prototyping phases into operational use within the Department.

(C) Plans for allocating the resources of the Department to ensure such resources are

focused on QIS technologies with the potential to solve operational challenges as identified under subparagraph (A).

(D) Plans for the continuous evaluation, development, and implementation of QIS technology solutions within the Department.

(E) Plans for the development, review, performance evaluation, and adoption of a fault-tolerant, utility-scale quantum computer and the transition of that capability to appropriate organizations and elements of the Department of Defense and such other departments and agencies of the Federal Government as the Secretary determines appropriate.

(3) REPORT.—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 includes—

(A) the strategic plan developed under paragraph (1); and

(B) an assessment of whether the budgets proposed for QIS-related activities of the Department of Defense and each of the covered Armed Forces appropriately balance the use of research, development, test, and evaluation

funds designated as budget activity 1 (basic research), budget activity 2 (applied research), and budget activity 3 (advanced technology development) (as those budget activity classifications are set forth in volume 2B, chapter 5 of the Department of Defense Financial Management Regulation (DOD 7000.14–R)) to achieve the objectives of the strategic plan over near-, mid-, and long-term timeframes.

(b) QUANTUM COMPUTING CENTER OF EXCELLENCE.—

(1) IN GENERAL.—The Secretary of Defense shall establish a Quantum Computing Center of Excellence (referred to in this subsection as the ''Center'') at a research laboratory of a covered Armed Force with requisite experience in quantum computing, integrated photonics and photon qubits, superconducting and hybrid systems, and trapped ions.

(2) ACTIVITIES.—The Center shall carry out the following activities:

(A) Accelerate the transition of advanced quantum and quantum hybrid computing technology from the research and development phase into operational use.

(B) Facilitate quantum computing workforce development.

(C) Conduct outreach to enhance government, industry, and academia's understanding of—

(i) national security-related use cases for quantum computing and quantum hybrid technology; and

(ii) operational challenges faced by the Department of Defense that may be addressed using such technology.

(D) Conduct prototyping of quantum computing and quantum hybrid applications.

(E) Undertake efforts to advance the technology readiness levels of quantum computing technologies.

(F) Carry out such other activities relating to quantum computing as the Secretary determines appropriate.

(3) PARTNER ORGANIZATIONS.—For purposes of carrying out the activities of the Center under this subsection, the research laboratory selected under paragraph (1) may partner with one or more of the following:

(A) Other research laboratories of the covered Armed Forces.

(B) The Defense Innovation Unit.

(C) Federally funded research and development centers.

(D) University affiliated research centers.

(E) Private sector entities with expertise in quantum computing.

(F) Such other organizations as the Secretary of Defense determines appropriate.

(4) CONTRACT AUTHORITY.—Subject to availability of appropriations, Secretary of Defense may make grants and enter into contracts or other agreements, on a competitive basis, to support the activities of the Center.

(5) TERMINATION.—The Center shall terminate on the date that is 10 years after the date of the enactment of this Act.

(c) DEFINITIONS.—In this section:

(1) The term ''covered Armed Force'' means the Army, Navy, Air Force, Marine Corps, or Space Force.

(2) The term ''quantum computing'' means computing algorithms and applications that use

quantum mechanics through quantum processing units, including—

(A) quantum-classical hybrid applications which are applications that use both quantum computing and classical computing hardware systems;

(B) annealing and gate systems; and

(C) all qubit modalities (including superconducting, trapped-ion, neutral atom, and photonics).

(3) The term ''quantum information science'' means the use of the laws of quantum physics for the storage, transmission, manipulation, computing, or measurement of information.

**SEC. 218 [Log 80483]. AUTHORITY TO TEMPORARILY DETAIL EMPLOYEES OF THE OFFICE OF STRATEGIC CAPITAL TO CERTAIN PRIVATE-SECTOR ORGANIZATIONS.**

(a) AUTHORIZATION.—Using the authority provided under section 1599g of title 10, United States Code, the Secretary of Defense, acting through the Director of the Office of Strategic capital, may carry out a program under which the Director arranges for the temporary assignment of an employee of the Office to a qualifying private-sector organization.

(b) OBJECTIVES.—The objectives of the program under subsection (a) shall be—

(1) to enable the Office of Strategic Capital and other organizations and elements of the Department of Defense to rapidly acquire industry-specific context and technical competence across high priority technology and industrial focus areas through immersion in highly relevant emerging technology and business ecosystems across the United States; and

(2) to enhance, among personnel of the Department—

(A) understanding of, connectivity with, and access to knowledge about critical and emerging defense industrial base capabilities; and

(B) understanding of the strategic role that venture capital and private equity operations have in shaping future sustainment and modernization requirements for the defense industrial base.

(c) MATCHING AND TRACKING CAPABILITIES.—In carrying out program under subsection (a), the Director of the Office of Strategic Capital shall—

(1) use an information technology system to optimize the identification, assessment, and placement of participants within the program, which shall include the use of such system to match private-sector organizations with employees of the Office participating in the program in a manner that aligns the priorities, needs, and expertise of such employees, organizations, and the Office; and

(2) establish a database or other capability that—

(A) enables the Office to identify and track current and former participants in the program;

(B) documents the nature of the experience such participants had while in the program; and

(C) is suitable for further development and expansion to other organizations of Department

of Defense in the event the Secretary of Defense determines such expansion is appropriate.

(d) QUALIFYING PRIVATE-SECTOR ORGANIZATION DEFINED.—In this section, the term ''qualifying private-sector organization'' means a private-sector organization within the defense industrial base that has functions and expertise relevant to the responsibilities of the Office of Strategic Capital, which may include organization such as a venture capital firm, private equity firm, emerging technology company, or other such organizations as determined appropriated by the Director.

**SEC. 219 [Log 80248]. PILOT PROGRAM ON ESTABLISHMENT OF A TEST AND EVALUATION CELL WITHIN THE DEFENSE INNOVATION UNIT.**

(a) PILOT PROGRAM.—The Director of the Defense Innovation Unit shall carry out a pilot program under which the Director—

(1) develops an alternative testing and evaluation pathway to accelerate the testing and evaluation of technologies that have the potential to provide warfighting capabilities to the Department of Defense in the near-term and mid-term timeframes; and

(2) establishes a cell of dedicated personnel within the Unit to manage and implement the alternative testing and evaluation pathway developed under paragraph (1).

(b) ACTIVITIES.—In carrying out the pilot program under subsection (a), the Director of the Defense Innovation Unit shall—

(1) conduct continuous and iterative test and evaluation of technologies that have the potential to provide warfighting capabilities to the Department of Defense in the near-term and mid-term timeframes, including—

(A) commercial dual use technologies;

(B) technologies that are not integrated into an established program of record;

(C) technologies that have not been fully fielded;

(D) software-based technologies; and

(E) such other technologies as the Director determines appropriate;

(2) use tools and technologies to emulate operationally relevant threat scenarios and conditions; and

(3) integrate the development of concepts of operations and concepts of employment with testing and evaluation activities conducted under the program to ensure early alignment between capability development and future concepts of operations and concepts of employment.

(c) CONSULTATION.—The Director of the Defense Innovation Unit shall carry out the pilot program under subsection (a), in consultation with—

(1) service-level innovation organizations;

(2) research laboratories of the Armed Forces;

(3) the combatant commands;

(4) the Joint Staff;

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

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

(7) the Director of Operational Test and Evaluation;

(8) the Director of the Test Resource Management Center;

(9) industry partners; and

(10) Federal, State, local, and international partners with test and evaluation infrastructure.

(d) ANNUAL BRIEFINGS.—Not later than 180 days after the date of the enactment of this Act, and on an annual basis thereafter through the termination date specified in subsection (e), the Director of the Defense Innovation Unit shall provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the status of the pilot program under subsection (a).

(e) TERMINATION.—The pilot program under subsection (a) shall terminate on December 31, 2028.

# Subtitle C—Plans, Reports, and Other Matters

**SEC. 221 [Log 80620]. PLAN FOR ESTABLISHMENT OF SECURE COMPUTING AND DATA STORAGE ENVIRONMENT FOR TESTING OF ARTIFICIAL INTELLIGENCE TRAINED ON BIOLOGICAL DATA.**

(a) PLAN REQUIRED.—The Under Secretary of Defense for Research and Engineering, in coordination with the Chief Digital and Artificial Intelligence Officer, shall develop a plan for the establishment of a secure computing and data storage environment to facilitate—

(1) the testing of artificial intelligence models trained on biological data; and

(2) the development and testing of products generated by such models.

(b) ELEMENTS.—The plan under subsection (a) shall provide as follows:

(1) DESIGNATION.—The secure computing and data storage environment described in subsection (a) shall be known as the ''AIxBio sandbox''.

(2) COMPUTING AND DATA STORAGE INFRASTRUCTURE.—The AIxBio sandbox shall consist of a secure computing and data storage infrastructure to be used for the testing and development activities described in subsection (a). To the extent feasible,

such infrastructure shall be assembled from the existing computing and data storage infrastructure organizations and elements of the Department of Defense with relevant capabilities, such as the Test Resource Management Center and the AI Accelerator of the Department of the Air Force.

(3) RESPONSIBLE OFFICIAL.—The Under Secretary of Defense for Research and Engineering shall be responsible for—

(A) managing and overseeing the activities of the sandbox;

(B) coordinating the efforts of the organizations of the Department involved in the activities of the sandbox;

(C) selecting projects for development and testing using the sandbox in accordance with paragraph (4); and

(D) arranging partnerships in accordance paragraph (5).

(4) SELECTION OF PROJECTS.—The Under Secretary of Defense for Research and Engineering shall—

(A) identify projects funded, in whole or in part, by the Department of Defense that—

(i) have demonstrated a proof-of-concept or another similar indicator of early success or feasibility; and

(ii) involve the development of a model, technology, or product at the intersection of artificial intelligence and biotechnology that has potential defense applications, such as a project using artificial intelligence and biological data—

(I) to direct and produce medical countermeasures;

(II) to predict and produce new or enhanced biological materials for military purposes; or

(III) to analyze how biology could fulfill different components of the supply chain, including by improving the domestic supply chain through the use of biomanufacturing; and

(B) from projects identified under subparagraph (A), select projects for further development and testing using the AIxBio sandbox.

(5) PARTNERSHIPS.—

(A) IN GENERAL.—The Under Secretary of Defense for Research and Engineering shall es-

tablish mechanisms through which organizations and entities involved in projects of the AIxBio sandbox may work with Department of Defense laboratories and Department-funded laboratories of academic institutions to carry out activities in support of such projects, including biological testing and experimentation and testing and experimentation to validate artificial intelligence models in development.

(B) STREAMLINED PROCESSES.—In carrying out subparagraph (A), the Under Secretary shall establish streamlined processes to facilitate efficient collaboration between laboratories, organizations of the Department of Defense, and private entities for purposes of developing products for national security purposes and carrying out activities in support of projects under AIxBio sandbox, including testing and experimentation.

(6) OTHER ELEMENTS.—The plan shall address—

(A) the manner in which existing computing and data storage infrastructure of the Department of Defense shall be made available

for the AIxBio sandbox in accordance with paragraph (2);

(B) the development of any mechanisms needed to facilitate collaboration among individuals and organizations involved in projects under the AIxBio sandbox, including any necessary agreements concerning intellectual property, funding, and the transfer of materials or other resources;

(C) the process for selecting projects for development and testing using the sandbox in accordance with paragraph (4); and

(D) the process for determining the amount of funding needed for projects under the sandbox, including the length of time each project is expected to receive such funding.

(c) REPORT AND BRIEFING.—Not later than one year after the date of the enactment of this Act, the Under Secretary of Defense for Research and Engineering shall—

(1) submit to the Committees on Armed Services of the Senate and the House of Representatives a report that includes the plan developed under subsection (a); and

(2) provide to the Committees a briefing on the plan.

**SEC. 222 [Log 80326]. STUDY AND REPORT ON FOREIGN CAPITAL DISCLOSURE REQUIREMENTS OF CERTAIN DEPARTMENT OF DEFENSE ORGANIZATIONS.**

(a) STUDY REQUIRED.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Defense shall seek to enter into a contract or other agreement with a federally funded research and development center to conduct an independent study on the foreign capital disclosure requirements of organizations of the Department of Defense that routinely engage with commercial entities backed by private equity or venture capital funds.

(b) ELEMENTS.—The study under subsection (a) shall include the following:

(1) A comparative analysis of current foreign capital disclosure requirements used by organizations within the Department of Defense that engage with commercial entities backed by private equity or venture capital funds, including the Defense Innovation Unit, National Security Innovation Capital, and other such organizations within the Department.

(2) An assessment of any business intelligence, due diligence information, classified information, and other information sources available to such organiza-

tions to assist the organizations in formulating and executing foreign capital disclosure requirements.

(3) An assessment of the extent to which such foreign capital disclosure requirements are shared with commercial entities.

(4) An assessment of best practices for foreign capital disclosure requirements across the Department of Defense, including best practices for flexibly implementing such requirements based upon real or perceived risks.

(5) An assessment of the feasibility of harmonizing the best practices as described in paragraph (4) across the Department of Defense in a responsive manner.

(6) An analysis of foreign capital disclosure requirements that are used elsewhere within the Federal Government and in the Governments of international allies and partners of the United States.

(7) An assessment of such other factors as may be relevant to inform the implementation of coordinated, effective foreign capital disclosure requirements across the Department of Defense and the Governments of international allies and partners of the United States.

(c) REPORT.—

(1) IN GENERAL.—Not later than 270 days 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 study conducted under subsection (a).

(2) FORM OF REPORT.—The report required under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

**SEC. 223 [Log 80354]. BIOTECHNOLOGY ROADMAP.**

(a) ROADMAP REQUIRED.—The Secretary of Defense shall develop a biotechnology roadmap to guide the efforts of the Department of Defense relating to biotechnology.

(b) ELEMENTS.—In the roadmap required by subsection (a), the Secretary of Defense shall—

(1) clearly articulate the strategic objectives of the Department of Defense relating to biotechnology;

(2) for each strategic objective, establish specific goals and milestones for the achievement of such objective, including timelines for meeting such goals and milestones;

(3) in the case of each updated version of the roadmap following submittal of the initial roadmap under subsection (d)(1), include—

(A) a review of the goals and milestones established under paragraph (2) to ensure such goals and milestones continue to align with strategic objectives under paragraph (1); and

(B) a description of any goals and milestones that changed as a result of such review;

(4) separately identify each biotechnology effort covered by the strategy, including any programs, projects, or other activities associated with such effort within the Office of the Secretary of Defense,

the Armed Forces, and other organizations of the Department, and for each such effort provide—

(A) a description of the effort;

(B) an estimate of the funding dedicated to the effort;

(C) a timeline for carrying out the effort; and

(D) an explanation of how the effort aligns with the strategic objectives under paragraph (1);

(5) identify and describe the role of each organization of the Department with responsibilities relating to biotechnology under the strategy;

(6) establish metrics to measure the progress of the Department in meeting the objectives, goals, and milestones under the strategy;

(7) based on such metrics, assess the progress of the Department in meeting such objectives, goals, and milestones;

(8) based on the results of such assessment, make any necessary adjustments to the planning and execution of the roadmap to ensure the Department makes continuous progress toward achieving the objectives under paragraph (1);

(9) assess the overall risk to the security of the United States of the biotechnology efforts covered by the strategy;

(10) analyze any requirements of the Federal Government that hinder the ability of the Department to advance and use biotechnology;

(11) provide for the development and support of the biotechnology workforce of the Department, including personnel with responsibilities relating directly to biotechnology and personnel who indirectly support the biotechnology efforts of the Department such as personnel involved program management, acquisition, investment, and legal matters;

(12) with respect to the biotechnology workforce described in paragraph (11)—

(A) identify the total number of biotechnology positions required to support the objectives of the roadmap—

(i) as of the date of the road map; and

(ii) over the periods of five and 10 years following such date;

(B) indicate the number of such positions that have been filled as of the date of the roadmap;

(C) describe the positions included in the biotechnology workforce, including a description of—

(i) the role of each position in supporting the objectives under paragraph (1); and

(ii) the qualifications required for each position, including any qualifications relating to seniority level, education, training, and security clearances;

(D) identify any challenges affecting the ability of the Department to develop the biotechnology workforce and propose solutions to those challenges;

(E) assess whether the codes used to define positions and roles within the workforce of the Department adequately cover the range of positions and personnel that comprise the biotechnology workforce, such as personnel in research, engineering, and testing;

(F) identify mechanisms to enable the Department to access outside expertise relating to biotechnology, including mechanisms to assemble a pool of outside experts who have been prequalified (including by obtaining any nec-

essary security clearances) to provide advice and assistance to the Department on matters relating to biotechnology on an as-needed basis;

(G) assess whether personnel occupying existing positions in the Department could be used to meet biotechnology workforce needs with additional training and, if so, the nature and scope of the training required;

(13) address collaboration between the Department and international partners to advance research on biotechnology, which shall include—

(A) a description of any international partnerships under which the United States is collaborating with partners to conduct biotechnology research and development for defense purposes;

(B) a description of any new international partnerships that may be entered into, or existing partnerships that may be modified, to provide for such collaboration; and

(C) identification of any challenges affecting the ability of the Department engage in such collaboration with international partners, including—

(i) any limitations on co-investments within international partnerships;

(ii) any United States export controls or other technology protections that hinder information sharing within such partnerships; and

(iii) any other challenges that may prevent the full utilization of such partnerships for such collaboration.

(c) CONSULTATION.—In preparing the roadmap required under subsection (a), the Secretary of Defense shall consult with—

(1) the Under Secretary of Defense for Research and Engineering

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

(3) the Secretaries of the military departments; and

(4) such other officials of the Department of Defense as the Secretary determines appropriate.

(d) SUBMITTAL TO CONGRESS; UPDATES.—

(1) INITIAL SUBMISSION.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall submit to the congres-

sional defense committees the roadmap developed under subsection (a).

(2) ANNUAL UPDATES.—Not less frequently than once every two years following the submittal of the initial roadmap under paragraph (1), the Secretary shall—

(A) review and update the roadmap; and

(B) submit an updated version of the roadmap to the congressional defense committees.

(3) FORM.—Each version of the roadmap required to be submitted under this subsection may be submitted in classified form, but if so submitted, shall include an unclassified executive summary.

(e) PUBLIC AVAILABILITY.—On annual basis, the Secretary shall make an unclassified version of the most recent roadmap submitted under subsection (d) available on a publicly accessible website of the Department of Defense.

(f) BIOTECHNOLOGY DEFINED.—In this section, the term ''biotechnology'' means the application of science and technology to living organisms and to parts, products and models of such organisms to alter living or non-living materials for the production of knowledge, goods, or services.

# Subtitle A—Cyber Operations

**SEC. 1501[Log 80272]. AUTHORITY TO ACCEPT VOLUNTARY AND UNCOMPENSATED SERVICES FROM CYBERSECURITY EXPERTS.**

Section 167b(d) of title 10, United States Code, is amended by adding at the end the following new paragraph:

''(4) The Commander of the United States Cyber Command may accept voluntary and uncompensated services from cybersecurity experts, notwithstanding the provisions of section 1342 of title 31, and may delegate such authority to the chiefs of the armed forces.''.

# Subtitle B—Cybersecurity

**SEC. 1511[Log 80271]. PROTECTIVE MEASURES FOR MOBILE DEVICES WITHIN THE DEPARTMENT OF DEFENSE.**

(a) IN GENERAL.—The Secretary of Defense shall carry out a detailed evaluation of the cybersecurity products and services for mobile devices to identify products and services that may improve the cybersecurity of mobile devices used by the Department of Defense, including mitigating the risk to the Department of Defense from cyber attacks against mobile devices.

(b) CYBERSECURITY TECHNOLOGIES.—In carrying out the evaluation required under subsection (a), the Secretary of Defense shall evaluate each of the following technologies:

(1) Anonymizing-enabling technologies, including dynamic selector rotation, un-linkable payment structures, and anonymous onboarding.

(2) Network-enabled full content inspection.

(3) Mobile-device case hardware solutions.

(4) On-device virtual private networks.

(5) Protected Domain Name Server infrastructure.

(6) Extended coverage for mobile device endpoint detection.

(7) Any other emerging or established technologies determined appropriate by the Secretary.

(c) ELEMENTS.—In carrying out the evaluation required under subsection (a), for each technology described in subsection (b), the Secretary of Defense shall—

(1) assess the efficacy and value of the cybersecurity provided by the technology for mobile devices;

(2) assess the feasibility of scaling the technology across the entirety or components of the Department of Defense, including the timeline for deploying the technology across the entirety or components of the Department of Defense; and

(3) evaluate the ability of the Department of Defense to integrate the technology with the existing cybersecurity architecture of the Department of Defense.

(d) REPORT.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report of the findings of the evaluation carried out under subsection (a), including a determination whether the Department of Defense or any component thereof should procure or incorporate any of the technologies evaluated pursuant to subsection (b).

# Subtitle C—Information Technology and Data Management

**SEC. 1521[Log 80275]. USABILITY OF ANTIQUATED DATA FORMATS FOR MODERN OPERATIONS.**

(a) STRATEGY AND ROADMAP.—

(1) IN GENERAL.—Not later than 270 days after the date of enactment of this act, the Secretary of Defense, in coordination with the Secretaries of the military departments, shall develop—

(A) a strategy—

(i) for the Department of Defense, including each of the military departments, to implement and use modern data formats as the primary method of electronic communication for command and control activities and for weapon systems, including sensors associated with such weapon systems; and

(ii) which accounts for specific needs of each military department with respect to such implementation and use of modern data formats; and

(B) an associated five-year roadmap for such implementation.

(2) ELEMENTS.—The strategy and roadmap required under paragraph (1) shall include the following elements:

(A) The activities of the Chief Digital and Artificial Intelligence Officer of the Department of Defense to increase and synchronize the use of modern data formats and modern data sharing standards across the Department of Defense, including the Armed Forces in the Department of Defense.

(B) The activities of the military departments to increase the use of modern data formats and modern data sharing standards for command and control systems, weapon systems, and sensors associated with such weapon systems.

(C) An identification of barriers to the use of modern data formats and modern data sharing standards within weapon systems and sensors associated with such weapon systems across the Department of Defense, including the Armed Forces in the Department of Defense.

(D) An identification of barriers to the use of modern data formats and modern data shar-

ing standards within command and control systems across the Department of Defense, including the Armed Forces in the Department of Defense.

(E) An identification of limitations on combined joint all-domain command and control capabilities resulting from the use of antiquated data formats, including—

(i) the Extensible Markup Language file format;

(ii) the JavaScript Object Notation data format;

(iii) the Binary JavaScript Object Notation data format; and

(iv) the Protocol Buffers data format.

(3) SUBMISSION TO CONGRESS.—Upon completion of the strategy and roadmap required under this subsection, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives such strategy.

(b) PILOT PROGRAMS.—

(1) ESTABLISHMENT.—Not later than 60 days after the date of enactment of this Act—

(A) the Secretary of Defense shall establish a pilot program under which the Department of Defense, other than the military departments, shall use modern data formats to improve the usability and functionality of information stored or produced in antiquated data formats, including by converting such information to modern data formats; and

(B) each Secretary of a military department shall establish a pilot program under which such military department shall use modern data formats as described in subparagraph (A).

(2) BRIEFING.—Not later than 180 days after the date of enactment, the Secretary of Defense and the Secretaries of the military departments shall each submit to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the progress of the pilot program established by such Secretary under this subsection, including specific examples of the use of modern data formats under such pilot program to improve the usability and functionality of information stored or produced in antiquated data formats.

(3) SUNSET.—Each pilot program established under this subsection shall terminate on the date that is three years after the date of the enactment of this Act.

(c) MILITARY DEPARTMENT DEFINED.—In this section, the term ''military department'' has the meaning given such term in section 101(a) of title 10, United States Code.

**SEC. 1522[Log 80172]. MODERNIZATION OF THE DEPARTMENT OF DEFENSE'S AUTHORIZATION TO OPERATE PROCESSES.**

(a) ACTIVE DIRECTORY OF AUTHORIZING OFFICIALS.—

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense and in coordination with the Chief Information Officers of the military departments, shall establish and regularly update a digital directory of all authorizing officials in the military departments.

(2) CONTENTS.—The directory established under paragraph (1) shall include—

(A) the most current contact information for such authorizing official; and

(B) a list of each training required to perform the duties and responsibilities of an authorizing official completed by such authorizing official.

(b) PRESUMPTION OF RECIPROCAL SOFTWARE ACCREDITING STANDARDS.—

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Chief Information Officers of the military depart-

ments shall jointly develop and implement a policy and guidance—

(A) requiring authorizing officials in the military departments to presume the cybersecurity of a cloud-based platform, service, or application that has already been accredited by another authorizing official in a military department for the same or similar purposes and the same classification level when determining whether to approve or deny a request for an Authorization to Operate for such cloud-based platform, service, or application; and

(B) requiring authorizing officials in the military departments to consult with the current or planned mission owners of a cloud-based platform, service, or application that will use such cloud-based platform, service, or application pursuant to an Authorization to Operate for such cloud-based platform, service, or application when such authorizing official is making a determination whether to approve or deny the request for such Authorization to Operate.

(2) CRITERIA.—The policy and guidance required under paragraph (1) shall—

(A) require each relevant authorizing official in a military department who is making a determination to approve or deny a request for an Authorization to Operate for a cloud-based platform, service, or application to ensure that documentation containing all of the relevant details of the cybersecurity, accreditation, performance, and operational capabilities of such cloud-based platform, service, or application is easily accessible and comprehensible to all relevant stakeholders with respect to such request; and

(B) require the development and implementation of a system for the digital sharing of the documentation described in subparagraph (A), including documenting the communication and acknowledgment of the uses of cloud-based platforms, services, and applications between mission owners and system owners of such cloud-based platforms, services, and applications.

(3) APPLICABILITY.—The policy and guidance developed under this subsection shall apply with respect to all cloud-based platforms, services, and applications capabilities operating across accredited

cloud environments of the military departments, to the extent practicable.

(c) DEFINITIONS.—In this section—

(1) the term ''Authorization to Operate'' has the meaning given such term in the Office of Management and Budget Circular A-130;

(2) the term ''authorizing official'' means an officer who is authorized to assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations and the United States;

(3) the term ''military departments'' has the meaning given such term in section 101(a) of title 10, United States Code;

(4) the term ''mission owner'' means the user of a cloud-based platform, service, or application; and

(5) the term ''system owner'' means the element of the Department of Defense responsible for acquiring a cloud-based platform, service, or application, but which is not a mission owner of such cloud-based platform, service, or application.

# Subtitle D—Reports and Other Matters

**SEC. 1531[Log 80319]. ACCESS TO NATIONAL SUICIDE PREVENTION AND MENTAL HEALTH CRISIS HOTLINE SYSTEM.**

(a) IN GENERAL.—The Chief Information Officer shall, as soon as practicable, implement at each facility of the Department access to the universal telephone number for the national suicide prevention and mental health crisis hotline system described in section 251(e)(4) of the Communications Act of 1934 (47 U.S.C. 251(e)(4)).

(b) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Chief Information Officer shall submit to the congressional defense committees a report describing the resources required to implement the access described in subsection (a) at each facility of the Department.

(2) CONTENTS.—The report required by paragraph (1) shall include—

(A) a timeline for the implementation of the access described in subsection (a), disaggregated by geographic location to the ex-

tent determined appropriate by the Chief Information Officer;

(B) a description of the actions required to implement such access at facilities of the Department located outside of the United States; and

(C) an analysis of the feasibility and cost of automatically conveying dispatchable location information with each call to the universal telephone number described in subsection (a) from a facility of the Department.

(c) DEFINITIONS.—In this section—

(1) the term ''Chief Information Officer'' means the Chief Information Officer of the Department;

(2) the term ''Department'' means the Department of the Defense; and

(3) the term ''dispatchable information'' means the street address of the calling party and additional information such as room number, floor number, or similar information necessary to adequately identify the location of the calling party.

**SEC. 1532[Log 80316]. OVERSIGHT AND REPORTING ON THE MISSION PARTNER ENVIRONMENT AND ASSOCIATED ACTIVITIES WITHIN THE DEPARTMENT OF DEFENSE.**

(a) BIANNUAL BRIEFINGS.—

(1) IN GENERAL.—Not later than October 1, 2025, and every six months thereafter until October 1, 2030, the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, the Chief Information Officer of the Department of Defense, the head of the Information Security Risk Management Committee of the Department of Defense, the director of the Mission Partner Capability Office, the Executive Agent for the Mission Partner Environment, and a senior military service representative for each of the Armed Forces shall provide to the congressional defense committees a briefing on the Mission Partner Environment and related activities within the Department of Defense, including the modernization of the Mission Partner Environment.

(2) COMBATANT COMMANDS.—A senior representative from each unified combatant command shall attend and participate in each briefing required by paragraph (1).

(b) ELEMENTS.—Each briefing required by subsection (a) shall include the following:

(1) A description of all efforts of the Department of Defense for the Mission Partner Environment.

(2) A description of the overall progress on implementation and modernization of Mission Partner Environment across the entirety of the Department of Defense as of the date of the briefing and, for each such briefing after the first such briefing, the progress made on such implementation and modernization since the preceding briefing under such subsection.

(3) An explanation of any changes in policy necessary to execute on Mission Partner Environment, including changes made during the period covered by the briefing and changes that are planned as of the time of the briefing.

(4) An explanation of any changes to the governance of the Mission Partner Environment within the Department of Defense, including changes made during the period covered by the briefing and changes that are planned as of the time of the briefing.

(5) A detailed programmatic table of the funding for the combined joint all-domain command and control efforts of the Office of the Secretary of De-

fense and the military departments, as set forth in the budget of the President most recently submitted to Congress under section 1105 of title 31, United States Code.

(c) DEFINITIONS.—In this section—

(1) the terms ''Defense Agency'' and ''military departments'' have the meanings given such terms, respectively, in section 101(a) of title 10, United States Code;

(2) the term ''Mission Partner Environment'' means the operating framework enabling command and control, information sharing, and the exchange of data between the Department of Defense and partners and allies of the United States participating in a military or other operation for the purposes of planning and executing such operation through the use of common standards governance and procedures, including activities the Office of the Secretary of Defense, military departments, unified combatant commands (as defined in section 161 of title 10, United States Code), and Defense Agencies relating to the operation, modernization, implementation, or oversight of, or resourcing of networks or applications designed for such framework; and

(3) the term ''unified combatant command'' has the meaning given such term in section 161 of title 10, United States Code.

# DIRECTIVE REPORT LANGUAGE

# Table Of Contents



---

## DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

## TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

### RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, DEFENSE-WIDE

#### Items of Special Interest

##### Biobased Products

The committee is aware of the potential for domestic biomanufacturing to diversify critical supply chains and increase domestic resilience to overseas supply chain disruptions. The committee is likewise aware of requirements contained within the Federal Acquisition Regulations (FAR) that require maximum use of biobased products when competitive on cost, schedule, and performance. The

committee is concerned, however, that implementation of those requirements may be unclear when considered in concert with military equipment exemptions, and that acquisition personnel in the Department of Defense may not be fully cognizant of the FAR requirements. Therefore, the committee directs the Under Secretary of Defense for Acquisition and Sustainment to provide a briefing to the House Committee on Armed Services not later than March 1, 2025, describing:

(1) the Department's assessment of the need to clarify the Defense Supplement to the Federal Acquisition Regulation on the exemption of "military equipment" in section 52.223-2 of the Federal Acquisition Regulation (FAR), "Affirmative Procurement of Biobased Products Under Service and Construction Contracts", including the potential use of specified listings of products that are not considered military equipment;

(2) the current state of Department-wide and military service-specific guidance and required training on the above, along with plans on how the Department plans to incorporate section 52.223-2 of the FAR into guidance and training that may not currently address the section; and

(3) whether current Department of Defense purchasing systems, such as FedMall in the Defense Logistics Agency, indicate which products are U.S. Department of Agriculture's (USDA) Certified biobased product, or otherwise contain clear indications for customers using those systems that a product meets the USDA definition of a biobased product.

Compact Fusion Energy Sources

The committee notes with interest the announcement by the Defense Innovation Unit on May 17, 2022, regarding accelerated ground and flight testing for compact fusion energy sources for on-orbit power. The committee believes that compact fusion power technologies, if matured to an appropriate level, could provide significant advantages to the Department of Defense.

The committee likewise notes ongoing progress made by the Department of Defense Strategic Capabilities Office on Project Pele, an effort to design, build, and demonstrate a prototype mobile nuclear fission reactor. In particular, the committee is monitoring with interest the work done by Project Pele to demonstrate the ability of mobile nuclear power generation technologies to comply fully with all relevant regulations and statutory requirements, satisfy stakeholder concerns, and operate safely in real-world conditions. The committee believes that such pathfinder efforts could ultimately prove beneficial for eventual adoption and deployment compact fusion capabilities.

Therefore, the committee directs the Under Secretary of Defense for Research and Engineering to provide a briefing to the House Committee on Armed Services not later than March 1, 2025, that includes:

(1) an assessment of the technology readiness levels of fusion power technologies currently in development, including compact and modular approaches;

(2) an assessment of the potential for compact modular fusion power technologies to address needs and challenges described in the National Defense Strategy and other relevant strategic guidance documents;

(3) an assessment of fusion power technologies under development by adversaries or strategic competitors of the United States; and

(4) an identification of key supporting activities for and pacing challenges to the adoption of compact fusion power technologies responsive to Department of Defense needs.

### Display Technology

The committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services no later than June 1, 2025, on display technology. The briefing should include:

(1) an overview of the Department's strategy for the research, development, adoption, procurement, and sustainment of display technology, as well as its key national security use cases;

(2) an assessment of the state, resilience, and security of the global display supply chain, including a description of the degree to which foreign sources of supply and foreign supply chains involve dependence on production in countries unfriendly to the United States;

(3) opportunities for technological and industrial cooperation with U.S. allies and partners to ensure a reliable and trusted supply of leading-edge microdisplays for the Department; and

(4) a discussion of options available to the United States for addressing national security vulnerabilities identified in the report.

### Expenditure Benchmarks Policies on Grants Aligned with Academic Institutions' Fiscal Calendar

The committee applauds the Department’s efforts to ensure taxpayer dollars are properly administered through the application of expenditure benchmarks; however, the committee notes that research grants awarded to academic and research institutions do not operate under the same construct as contractual agreements. Research grantees are unable to begin expenditures until the funding reaches the Principal Investigator, which can be several months after the fiscal year appropriations are provided, yet the Department’s guidelines expect the funding recipient to have spent 40 to 50 percent of the grant by the time they receive the funding. Logistical delays are common and often require carrying over funds from the previous year to achieve the multi-year science objectives.

A research recipient typically invoices on actual rates, while the contractor can invoice on other benchmarks. In addition, where research instrumentation and equipment need to be purchased, long lead-times are required, and funds are not billed until the equipment is received. For research outside of the lab, fieldwork or offsite schedules are often moved and dependent on external factors. Finally,

academic institutions begin recruiting and hiring graduate and postdoctoral students in preparation for research efforts commencing in the summer as students are encumbered for the academic year, not the fiscal year, further delaying expenditure rates.

These expenditure challenges could deter researchers from participating in research sponsored by the Department. They could instead seek opportunities via other federal agency funding, which could undermine the Department's science, technology, engineering, and mathematics efforts and result in a reduced future scientific workforce interested in working on national security priorities. The committee urges the Department to implement expenditure benchmarks policies that take into account delays in allocations to the grantees and are more aligned with the fiscal policies and calendars of academic institutions.

The committee directs the Under Secretary of Defense (Comptroller), in coordination with the Under Secretary of Defense for Research and Engineering, to submit a report to the House Committee on Armed Services by December 1, 2024, on the steps taken to implement revised expenditure benchmarks related to research grants.

## Utility Scale Quantum Computing

The committee recognizes the importance of the Defense Advanced Research Projects Agency's (DARPA) Underexplored Systems for Utility-Scale Quantum Computing (US2QC) program and the significant progress made in demonstrating the technical feasibility of fault-tolerant utility-scale operations faster than conventional predictions. The committee is encouraged by DARPA's multi-phase, multi-year approach to exploring new ways to scale qubit count for larger, more complex systems for defense, scientific, and civilian applications. As the technological achievements associated with US2QC are demonstrated, it is critical that the Department maintains an accelerated pace of development to ensure the United States preserves its global lead in quantum computing. Given the significant capital investments required for fault-tolerant, utility-scale systems, it is imperative that the Department begins planning for project transition, supporting infrastructure and follow-on US2QC programs and funding. Therefore, the committee directs the Under Secretary of Defense for Research and Engineering to provide a briefing to the House Committee on Armed Services not later than December 1, 2024, on the status of the US2QC program and planned transition activities. The briefing shall include:

(1) a summary of the technical milestones and achievements of the US2QC program;

(2) a detailed assessment of the timeline associated with fielding fault-tolerant utility-scale quantum computers compared to previous estimates;

(3) an analysis of potential US2QC transition partners across the military services, National Laboratories, and within the Office of the Secretary of Defense, to include the timelines associated with those transitions; and

(4) an assessment of funding required to maintain the research, development, and demonstration of fault-tolerant, utility-scale quantum computers.

### OPERATIONAL TEST AND EVALUATION, DEFENSE

#### Items of Special Interest

##### Assessment of Department of Defense and Military Service Test and Evaluation Infrastructure Utilization and Optimization

The committee notes the critical role that the Department of Defense's test and evaluation (T&E) community plays in ensuring that new cutting edge technologies are mature and operationally effective to meet the needs of the joint force. The committee is concerned, however, that scheduling backlogs on Department of Defense T&E ranges could contribute to delays in transitioning technologies from research and development to fielded warfighting capabilities. The inability to effectively or efficiently test new warfighting technologies on a relevant timeline in operationally realistic scenarios is often cited as a "valley of death" in the Department's innovation process. The committee seeks to better understand the extent of this problem across the Department and military service test organizations and the impact that test range backlog and scheduling practices have on the Department's innovation ecosystem as a whole.

Accordingly, the committee directs the Comptroller General of the United States to review the extent to which the Department has data and information available to understand challenges, if any, related to test range availability and how, if at all, the Department uses available data to drive decision making and ensure timely testing. The committee is also interested in understanding the extent to which the Department has assessed alternative options such as using commercial test ranges or other partnerships to address any identified challenges.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services not later than April 1, 2025, on the question of available data and how it is used, with additional work to address the question of alternative options to follow at a mutually agreed upon time and in a mutually agreed upon format.

## TITLE XV—CYBERSPACE-RELATED MATTERS

### ITEMS OF SPECIAL INTEREST

#### Acquisition Planning for Data Use and Storage

The committee is aware of anecdotal reports concerning how the Department of Defense struggles with forecasting data use and cloud storage as part of the acquisition process. Claims have been made that costs are treated as unforeseen, and program managers are challenged in the planning for incurred

costs from cloud computing. To that end, the committee directs the Under Secretary of Defense for Acquisition & Sustainment, in coordination with the Department of Defense Chief Information Officer, provide a briefing to the House Committee on Armed Services not later than March 1, 2025, on the Department's efforts to enhance the planning and forecasting ability of program managers and acquisitions professionals in the use of cloud storage and computing.

### Clarification and Deconfliction of Responsibilities for Cybersecurity Functions within the Department of Defense

The committee believes that proper management of information technology and risk mitigation within any single portion of the Department of Defense is too vast to fall exclusively to any single senior official. This complexity in the operations, oversight, policy, and resourcing of information technology and cybersecurity necessitates a "team" approach. The committee recognizes the unique value provided by Chief Information Officers, acquisition personnel, and cyberspace operations organizations towards securing a network and technology landscape as vast as the one within the Department of Defense. From the perspective of statutory authorities, the Department is responsible for functions dictated across titles 10, 40, 44, and 50, United States Code. The committee is aware of anecdotal information suggesting that there have been occasions in which the various authorities are interpreted to be in conflict with each other, specifically as relates to cybersecurity responsibilities.

To better understand this situation, the committee directs the Secretary of Defense, in coordination with the Secretary of the Army, the Secretary of the Navy, and Secretary of the Air Force, to submit a report to the congressional defense committees not later than May 1, 2025, which details the collective efforts related to the cybersecurity program as required under title 44, United States Code. This report should also provide clarity to the primary and secondary officials within each organization charged with leading, executing, and implementing those statutory responsibilities. Additionally, the report should explain how senior officers charged in one portion of statute are made aware of decisions executed by other senior officers leveraging other parts of statute.

### Combined Joint All Domain and Control Applications

The committee applauds the Chief Digital and Artificial Intelligence (AI) Office's effort to advance Combined Joint All Domain and Control (CJADC2) applications and capabilities across combatant commands through rapid prototyping, experimentation, and production at scale. The committee recognizes U.S. Central Command (CENTCOM), U.S. Northern Command (NORTHCOM), U.S. European Command (EUCOM) and U.S. Indo-Pacific Command (INDOPACOM) for scaling successful efforts such as the CJADC2 Mission Application prototypes into enterprise-wise production capabilities. The scaled capability has become a central operating system for decision making spanning

directorates and warfighting functions to include intelligence, operations, and logistics.

Given its expansive use and criticality to mission success, the committee believes there are needs across all the combatant commands. Additionally, the committee recognizes the importance of timely and thorough data sharing between allies and partners. While there are positive efforts such as INDOPACOM's Mission Data Platform and CENTCOM's nascent initiative, there remains a significant gap at other combatant commands.

Therefore, the committee directs the Chief Digital and Artificial Intelligence Officer, in consultation with the combatant commands, to provide a briefing to the House Armed Services Committee no later than March 1, 2025, on plans to scale efforts such as the CJADC2 Mission Applications more broadly. The report shall contain at a minimum, the following:

(1) progress thus far in scaling the deployment;

(2) plans and timelines for potential expansion; and

(3) efforts to integrate with the Mission Partner Environment.

Department of Defense Information Network Approved Products List Efficacy

The committee recognizes that the Defense Information Systems Agency (DISA) maintains the Department of Defense Information Network Approved Products List (DODIN APL), which provides a consolidated list of products that have been certified as meeting cybersecurity and interoperation requirements as defined by the Unified Capabilities Requirement. According to DISA, the DODIN APL is the only listing of equipment by the Department to be fielded in Department of Defense networks, however, the committee is aware of reports that Department of Defense components are utilizing products not found on the DODIN APL, and potentially without the requisite waivers necessary to justify use of products not on the DODIN APL. If accurate, the committee is concerned by such claims when similar products and capabilities which have been certified on the DODIN APL are available. To that end, the committee directs the Department of Defense Chief Information Officer to provide a briefing to the House Committee on Armed Services no later than May 1, 2025, on its understanding of both the problem and efforts underway to address non-compliance within the Department of Defense for present instruction to use of DODIN APL products and services.

Security for the Joint Warfighter Cloud Capability Procurement

The committee recognizes the Department of Defense's progress with enterprise cloud capability through the Joint Warfighter Cloud Capability (JWCC) program. JWCC can provide scalable compute and storage for the Department and the military services, while also ensuring cost efficiencies for the taxpayer. While understanding that JWCC is a contract vehicle, the committee believes that the Department should consider how to complement the offerings with embedded cloud security applications. To that end, the committee directs the Department of Defense

Chief Information Officer to provide a briefing to the House Committee on Armed Services not later than February 1, 2025, on the Department's exploration of cloud-specific security solutions that could be considered as part of the JWCC effort.

### Transition Timelines from Joint Regional Security Stacks

The committee commends the Department of Defense's efforts towards Zero-Trust Architecture compliance by 2027. Pivoting towards Zero-Trust implementation requires concurrent efforts to pivot away from legacy programs and initiatives, one of the most significant being the Joint Regional Security Stacks. In section 1528 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81), the Department of Defense and specifically, the heads of each military department and component were directed to submit an implementation plan for Zero-Trust Architecture. The committee believes that such implementation efforts would benefit from greater clarity on the work necessary to move away from the current architectures in place. To that end, the committee directs the Department of Defense Chief Information Officer to provide a briefing to the House Committee on Armed Services no later than February 1, 2025, on the current and updated schedules from Department of Defense components migrating toward Zero-Trust Architecture.