H.R. 3838—STREAMLINING PROCUREMENT FOR EFFECTIVE EXECUTION AND DELIVERY AND NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2026

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 211—Modification to Authority to Award Prizes for Advanced Technology Achievements

This section would amend the authority to operate prize competitions to enable the Secretary of Defense to delegate the authority and increases the potential value of the prize challenges.

Section 212—Extension of Authority for Assignment to Defense Advanced Research Projects Agency of Private Sector Personnel with Critical Research and Development Expertise

This section would extend the authority for the Defense Advanced Research Projects Agency to temporarily assign employees of nontraditional defense contractors to the Agency by five years.

Section 213—Review and Alignment of Standards, Guidance, and Policies Relating to Digital Engineering

This section would require the Secretaries of the military departments, in coordination with the Under Secretary of Defense for Research and Engineering (USD(R&E)), Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the Director, Operational Test and Evaluation (DOT&E), to conduct a review of the reference architectures, standards, and best practices for the use of digital engineering tools at all stages of program design, development, and testing.

This section would also require the Secretaries of the military departments to develop and implement a standard reference architecture for each covered military service to guide the use of digital engineering for program development.

Finally, this section would also require the USD(R&E), USD(A&S), and DOT&E to identify and develop recommendations regarding areas in which further standardization of reference architectures for digital engineering across the covered armed services may be feasible.

Section 214—Application of Software Innovation and Data Management Plans to Modernize Test and Evaluation Infrastructure

This section would require the Director, Test Resource Management Center, in coordination with the Director, Defense Innovation Unit, the Director, Operational Test and Evaluation, and the military services, to develop and maintain a digital test and evaluation environment for developmental and operational testing. The section would also require program managers to submit data management plans prior to executing a test and evaluation event. Finally, this section would establish a pilot program to determine how commercial software could accelerate and improve testing for priority mission areas.

SUBTITLE C—PLANS, REPORTS, AND OTHER MATTERS

Section 221—Feasibility Study on Incorporating Militarily-Relevant Applications of Emerging Biotechnology into Wargaming Exercises

This section would require the Chairman of the Joint Chiefs of Staff to conduct a feasibility study on incorporating military-relevant applications of emerging biotechnology to wargaming exercises.

TITLE VIII—ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE A—ACQUISITION POLICY AND MANAGEMENT

Section 803—Establishing Biobased Product Merit Guidance

This section would require the Under Secretary of Defense for Research and Engineering, in coordination with the Secretaries of the military departments, to develop and make publicly available guidance for private entities to prove biobased products meet Department of Defense requirements.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

LEGISLATIVE PROVISIONS

SUBTITLE A—OFFICE OF THE SECRETARY OF DEFENSE AND RELATED MATTERS

Section 901—Modification to Authorities of the Under Secretary of Defense for Research and Engineering

This section would expand the authorities of the Under Secretary of Research and Engineering.

Section 902—Additional Authorities for the Office of Strategic Capital

This section would allow the Office of Strategic Capital to charge fees on their transactions.

SUBTITLE B—OTHER DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT MATTERS

Section 912—Authority to Establish Regional Outreach Centers for the Defense Innovation Unit

The section provides statutory authority for the Defense Innovation Unit regional outreach centers which include domestic or international locations. The Director of the Defense Innovation Unit shall provide a briefing to Committee on Armed Services, not later than January 1, 2026, detailing plans to stand up at least two additional OnRamp Hubs in fiscal year 2026, including planned locations for such Hubs and the necessary personnel and resourcing to stand up those locations. The briefing shall also include relevant criteria, personnel, resourcing, and potential locations for overseas locations.

TITLE XV—CYBERSPACE-RELATED MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE A—CYBER OPERATIONS

Section 1501—Accountability of the Authorization to Operate Processes

This section would add additional reporting requirements to the Authority to Operate (ATO) process and streamline timelines for approving an ATO.

Section 1502—Assessment of Cyber Operational Support to Geographic Combatant Commands

This section would require the commanders of the unified combatant commands, other than the Commander of the United States Cyber Command, to submit, on an annual basis, a report to the congressional defense committees on the sufficiency of support provided by the Commander of the United States Cyber Command.

SUBTITLE B—CYBERSECURITY

Section 1511—Annual Report on Weapon Systems Data Accessibility and Security

This section would require the Secretaries of the Army, Navy, and Air Force to report on an annual basis those weapon systems which lack onboard, real-time cybersecurity capabilities.

Section 1512—Incorporation of Artificial Intelligence Considerations into Annual Cybersecurity Training

This section would require the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, to revise the mandatory annual cybersecurity training to include content related to unique challenges related to Artificial Intelligence.

SUBTITLE C—INFORMATION TECHNOLOGY AND DATA MANAGEMENT

Section 1521—Biological Data for Artificial Intelligence

This section would require the Secretary of Defense to develop and implement requirements that ensure qualified Department of Defense biological data resources are collected and stored for advanced computational methods.

SUBTITLE D—ARTIFICIAL INTELLIGENCE

Section 1531—Artificial Intelligence and Machine Learning Security in the Department of Defense

This section would create a requirement for a software bill of materials for artificial intelligence.

Section 1532—Pilot Program for Data-Enabled Fleet Maintenance

This section would require the Secretaries of the Army, Navy, and Air Force to establish pilot programs to use commercially available artificial intelligence technologies to improve the maintenance of ground vehicles in each military service's inventory.

Section 1533—Generative Artificial Intelligence for National Defense

This section would authorize the Department to create up to 12 generative artificial intelligence lines of effort.

TITLE XVIII—STREAMLINING PROCUREMENT FOR EFFECTIVE EXECUTION AND DELIVERY

LEGISLATIVE PROVISIONS

SUBTITLE D—MATTERS RELATING TO COMMERCIAL INNOVATION

Section 1833—Requirements for Modular Open System Approach and Modifications to Rights in Technical Data

This section would amend chapter 327 of title 10, United States Code, to streamline and simplify the requirements for a modular open system approach to the design and development of a major weapon system. This section would also make conforming amendments to section 3771 of title 10, United States Code, related to intellectual property and data rights in modular system interfaces.

Section 1834—Bridging Operational Objectives and Support for Transition Program

This section would require the Director of the Defense Innovation Unit (DIU) to establish a program to support the transition of technologies into established capability development and procurement activities of the military services. The Bridging Operational Objectives and Support for Transition (BOOST) program would directly support program managers and program executive officers (PEOs) by matching identified technologies with program requirements and serving as an on-ramp to integration of the needed technology into programs of record. The committee also intends that the BOOST program would create an active feedback

loop between the program manager or PEO and the innovator, which would inform and guide prototyping efforts in the context of an existing requirement in an established program.

This section would require the Secretary of Defense, in coordination with the Under Secretary of Defense for Acquisition and Sustainment and the Director of DIU, to provide the congressional defense committees a report on the effectiveness of the BOOST program in accelerating technology adoption or integration. The report would be due not later than two years after the date of the enactment of this Act and would require the Secretary to recommend whether to terminate or continue the BOOST program beyond December 31, 2030.

BILL LANGUAGE

Subtitle B—Program Requirements, Restrictions, and Limitations

SEC. 211 [Log 82844]. MODIFICATION TO AUTHORITY TO AWARD PRIZES FOR ADVANCED TECHNOLOGY ACHIEVEMENTS.

(a) SECRETARIAL AUTHORITY.—Subsection (a) of section 4025 of title 10, United States Code, is amended by striking '', acting through the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, and the service acquisition executive for each military department,''.

(b) MAXIMUM AMOUNT OF AWARD PRIZES.—Subsection (c) of such section is amended to read as follows:

''(c) LIMITATION.—No prize competition may result in the award of a prize with a fair market value of more than $20,000,000 without the approval of the Secretary of Defense.''.

(c) CONGRESSIONAL NOTIFICATION THRESHOLD.—Subsection (g)(1) of such section is amended by striking ''$10,000,000'' and inserting ''the amount specified in subsection (c)''.

SEC. 212 [Log 82842]. EXTENSION OF AUTHORITY FOR ASSIGNMENT TO DEFENSE ADVANCED RESEARCH PROJECTS AGENCY OF PRIVATE SECTOR PERSONNEL WITH CRITICAL RESEARCH AND DEVELOPMENT EXPERTISE.

(a) EXTENSION.—Subsection (e) of section 232 of the Carl Levin and Howard P. ''Buck'' McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291; 10 U.S.C. note prec. 4091) is amended by striking ''September 30, 2025'' and inserting ''September 30, 2030''.

(b) TECHNICAL AMENDMENT.—Subsection (f)(2) of such section is amended by striking ''section 2302'' and inserting ''section 3014''.

SEC. 213 [Log 82148]. REVIEW AND ALIGNMENT OF STANDARDS, GUIDANCE, AND POLICIES RELATING TO DIGITAL ENGINEERING.

(a) REVIEW REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, each Secretary of a military department, in coordination with the officials specified in subsection (c), shall complete a comprehensive review of the standards, guidance, and policies relating to digital engineering within the covered Armed Forces under the jurisdiction of that Secretary.

(2) ELEMENTS.—Each review under paragraph (1) shall include, with respect to the covered Armed Forces under the jurisdiction of the Secretary concerned, the following:

(A) A review of the reference architectures, standards, and best practices for the use of digital engineering tools (including digital twins and digital threads) as in effect at the time of the review, including standards for the use of such tools at all stages of program design, development, and testing.

(B) Identification of the current standards guiding the use of such digital engineering

tools, at all stages of program design, development, and testing.

(C) Assessment of—

(i) the extent to which the use of such standards and related governance structures is consistent across the covered Armed Forces under the jurisdiction of the Secretary concerned; and

(ii) the level of interoperability of such standards across such Armed Forces.

(D) Identification of best practices for digital engineering within each such Armed Force.

(E) Recommendations for improvements to the use of digital engineering tools in each such Armed Force.

(b) DEVELOPMENT OF STANDARD REFERENCE ARCHITECTURE.—

(1) IN GENERAL.—Not later than 180 days after the date on which the Secretary of a military department completes the review required under subsection (a), the Secretary shall develop and implement a standard reference architecture to guide the use of, and best practices for, digital engineering for program design, development, and testing within each covered Armed Force under the jurisdiction of

that Secretary. Each reference architecture shall include—

(A) a framework and clear requirements for developing and deploying digital engineering tools across program lifecycles; and

(B) defined standards for data management and modeling.

(2) PERIODIC REVIEW.—Not less frequently than once every three years following implementation of the standard reference architecture required under paragraph (1), each Secretary of a military department shall—

(A) conduct periodic reviews of the reference architecture to ensure it effectively addresses advancements in technology and evolving operational needs; and

(B) if necessary, modify the reference architecture to address such advancements and needs.

(3) APPROVAL AND CERTIFICATION REQUIRED.—Before a reference architecture may be implemented under this subsection, the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the Under Secretary of Defense

for Research and Engineering and the Director of Operational Test and Evaluation, shall—

(A) review and approve the reference architecture; and

(B) submit certification of such approval to the head of the covered Armed Force involved.

(4) RECOMMENDATIONS FOR FURTHER STANDARDIZATION.—Based on the reviews conducted under paragraph (3), the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the Under Secretary of Defense for Research and Engineering and the Director of Operational Test and Evaluation, shall—

(A) identify and develop recommendations regarding areas in which further standardization of reference architectures across the covered Armed Forces may be feasible; and

(B) submit such recommendations to the Secretaries of the military departments.

(c) OFFICIALS SPECIFIED.—The officials specified in this subsection are the following—

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

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

(3) The Director of Operational Test and Evaluation.

(d) DEFINITIONS.—In this section:

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

(2) The term ''reference architecture'' means an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions, as described in the guidance of the Office of the Assistant Secretary of Defense titled ''Reference Architecture Description'', dated June 2010, or any successor to such guidance.

SEC. 214 [Log 82149]. APPLICATION OF SOFTWARE INNOVATION AND DATA MANAGEMENT PLANS TO MODERNIZE TEST AND EVALUATION INFRASTRUCTURE.

(a) ESTABLISHMENT OF DIGITAL TEST AND EVALUATION ENVIRONMENT.—

(1) PROGRAM.—The Director of the Test Resource Management Center, in coordination with the officials specified in paragraph (4), shall establish and maintain a digital test and evaluation environment for developmental and operational testing of warfighting capabilities.

(2) REQUIREMENTS.—The digital test and evaluation environment required under paragraph (1) shall—

(A) incorporate commercially-derived data management, analysis, and operations software tools to enable rapid test and evaluation;

(B) enable real-time and iterative data collection, management, analysis, and feedback loops across the life cycle of tested systems;

(C) provide secure environments for testing systems with operational security sensitivities; and

(D) use a modular open system approach (as defined in section 4401 of title 10, United

States Code) to ensure the environment can be accessed by multiple vendors and is interoperable with multiple data sources, data formats, and digital tools.

(3) USE OF SOFTWARE ACQUISITION PATHWAY.—In procuring software and covered hardware (as defined in section 3603 of title 10, United States Code) for the digital test and evaluation environment required under paragraph (1), the Director of the Test Resource Management center shall use a software acquisition pathway described in section 3603 of title 10, United States Code.

(4) OFFICIALS SPECIFIED.—The officials specified in this paragraph are—

(A) the Director of the Defense Innovation Unit;

(B) the Director of Operational Test and Evaluation; and

(C) each chief of a covered Armed Force.

(b) DATA MANAGEMENT PLANS.—

(1) IN GENERAL.—Before a covered Armed Force may conduct a test and evaluation event, an appropriate official from the Armed Force shall submit to the Director of Operational Test and Evaluation and the Director of the Test Resource Manage-

ment Center a data management plan for the event. Such data management plan may be included as part of the Test and Evaluation Master plan submitted for the event pursuant to Department of Defense Directive 5000.100.

(2) PLAN REQUIREMENTS.—The Director of Operational Test and Evaluation and the Director of the Test Resource Management Center shall jointly develop standard requirements for the data management plans required under paragraph (1). Each such data management plan shall include, with respect to the test and evaluation event covered by the plan—

(A) identification of relevant data to be collected during the event;

(B) methodologies for analyzing data after testing is complete; and

(C) any other information the Directors determine appropriate.

(c) PILOT PROGRAM TO ACCELERATE TEST.—

(1) IN GENERAL.—The Director of the Defense Innovation Unit and the Director of the Test Resource Management Center, in coordination with the Director of Operational Test and Evaluation, shall jointly carry out a pilot program to determine how

commercial software can be used to accelerate and improve testing for priority mission areas—

(A) to accelerate continuous integration and continuous testing of warfighting capabilities by applying industry best practices and tooling for scalability, advanced analysis, and data sharing on identified priority use cases; and

(B) to enable continuous and iterative testing throughout capability design, development, engineering, and fielding.

(2) REPORTS REQUIRED.—The Director of the Defense Innovation Unit and the Director of the Test Resource Management Center, in coordination with the Director of Operational Test and Evaluation, shall—

(A) not later than 120 days after the date of the enactment of this Act, submit to the congressional defense committees an interim report that includes an implementation plan for the pilot program under paragraph (1); and

(B) following submittal of the report under subparagraph (A), but not later than 270 days after the date of the enactment of this Act, submit to the committees a report on the progress

of the pilot program, which shall include a description of—

(i) the metrics used to measure the performance of commercial software under the program;

(ii) the initial findings of the program; and

(iii) based on such findings, any identified roadblocks or limitations to using commercial software and digital tools for accelerated testing.

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

(d) COVERED ARMED FORCE DEFINED.—In this section, the term ''covered Armed Force'' means the Army, Navy, Air Force, Marine Corps, and Space Force.

Subtitle C—Plans, Reports, and Other Matters

SEC. 221 [Log 82517]. FEASIBILITY STUDY ON INCORPORATING MILITARILY-RELEVANT APPLICATIONS OF EMERGING BIOTECHNOLOGY INTO WARGAMING EXERCISES.

(a) IN GENERAL.—The Chairman of the Joint Chiefs of Staff shall conduct a review to determine the feasibility and advisability modifying the design of wargaming exercises to ensure that such exercises incorporate militarily-relevant applications of emerging biotechnology.

(b) ELEMENTS.—In conducting the review required under subsection (a), the Chairman of the Joint Chiefs of Staff shall take into account—

(1) biotechnology-enabled enhancements that improve the cognitive and physical performance of warfighters;

(2) biotechnology-enabled chemicals and materials intended to provide a strategic advantage on the battlefield;

(3) adversaries' use of biotechnology for military purposes beyond traditional biological weapons; and

(4) any other militarily-relevant applications of biotechnology determined appropriate by the Chairman.

(c) CONSULTATION.—In conducting the review under subsection (a), the Chairman of the Joint Chiefs of Staff shall consult with—

(1) the commanders of the combatant commands; and

(2) other stakeholders within and outside the Department of Defense, as necessary, to identify recent militarily-relevant advancements in the field of biotechnology that could potentially be incorporated into exercises.

(d) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Chairman of the Joint Chiefs of Staff shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the results of the review conducted under subsection (a). The report shall include—

(1) a detailed summary of any recommended modifications to wargaming exercises; and

(2) if applicable, a plan for regularly updating the design of such exercises to keep pace with advances in biotechnology.

(e) WARGAMING EXERCISE DEFINED.—In this section, the term ''wargaming exercise'' means a military exercise conducted to test or improve tactical expertise, and includes the Globally Integrated Wargames.

SEC. 803 [Log 82190]. ESTABLISHING BIOBASED PRODUCT MERIT GUIDANCE.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Under Secretary of Defense for Research and Engineering, in coordination with the Secretaries of the military departments, shall develop and make public available guidance for private entities on how such entities can effectively prove that a biobased product of such entity provides capabilities meeting the requirements of the Department of Defense.

(b) ANALYSIS.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct an analysis of the process of the Department of Defense for developing requirements to determine if such processes intentionally or unintentionally exclude biobased products.

(2) REPORT.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the congressional defense committees a report on the findings of the analysis conducted under paragraph (1) and, if Comptroller General determines through such analysis that the processes described in such paragraph exclude biobased products, containing recommendations of the Comptroller General to reduce such exclusion.

(c) BIOBASED PRODUCT DEFINED.—In this section, the term ''biobased product'' means a product manufactured, produced, or developed through the application living organisms to alter living or non-living materials.

Subtitle A—Office of the Secretary of Defense and Related Matters

SEC. 901 [Log 82127]. MODIFICATION TO AUTHORITIES OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING.

Section 133a(b) of title 10, United States Code, is amended—

(1) in paragraph (2), by striking ''and'' at the end;

(2) in paragraph (3), by striking the period at the end and inserting a semicolon; and

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

''(4) having the authority to direct the Secretaries of the military departments and the heads of other elements of the Department with regard to matters for which the Under Secretary has responsibility; and

''(5) conducting developmental prototyping, designing and executing experiments of prototypes in the field to demonstrate operational relevance to address joint force capability gaps, and encouraging and supporting the rapid transition of technology from the research and development phase into operational use within the Department.''.

SEC. 902 [Log 82511]. ADDITIONAL AUTHORITIES FOR THE OFFICE OF STRATEGIC CAPITAL.

Section 149(e) of title 10, United States Code, is amended—

(1) in paragraph (3)(A)(ii)(VI), by striking ''Secretary'' and inserting ''Director'';

(2) by amending clause (ii) of paragraph (5)(A) to read as follows:

''(ii) The Department of Defense Credit Program Account shall be credited with amounts appropriated pursuant to the authorization of appropriations and fees and payments received under paragraph (6).'';

(3) by redesignating paragraphs (6) through (9) as paragraphs (7) through (10), respectively; and

(4) by inserting after paragraph (5) the following new paragraph:

''(6)(A) The Director may charge and collect fees and collect payments to reimburse costs incurred by the Office in connection with an application for, or as a condition of an eligible entity receiving or restructuring, capital assistance under this subsection. The Director may set the fees at a level that the Director considers appropriate. Fees and

payments received under this paragraph shall be credited to the Department of Defense Credit Program Account to remain available until expended for costs and expenditures as provided under clauses (ii) through (iv) of paragraph (5)(B).

''(B)(i) Except as provided in clause (ii), no fees or payments may be received pursuant to the authority provided under subparagraph (A) as of the date specified in paragraph (10).

''(ii) With respect to loan and loan guarantees for which an obligation was incurred prior to the expiration date in paragraph (10), the Director may continue to charge and collect fees and cost reimbursements in connection with such loan and loan guarantee assets until fully collected.''.

SEC. 912 [Log 82411]. AUTHORITY TO ESTABLISH REGIONAL OUTREACH CENTERS FOR THE DEFENSE INNOVATION UNIT.

Section 4127 of title 10, United States Code, is amended—

(1) by redesignating subsection (f) as subsection (g); and

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

''(f) REGIONAL OUTREACH CENTERS.—

''(1) IN GENERAL.—The Director may establish and maintain regional offices of the Unit at locations within and outside the United States for purposes of conducting outreach to and streamlining interactions between the Unit and the private sector, academia, and other mission partners.

''(2) SELECTION CRITERIA AND OTHER GUIDANCE.—In the event the Director exercises the authority to establish and maintain regional offices under paragraph (1), the Director shall—

''(A) develop a strategy and criteria for the selection of locations for such offices;

''(B) issue any rules, regulations, policies, or guidance necessary for the operation of such offices; and

''(C) make the information described in subparagraphs (A) and (B) available on a publicly accessible website of the Department of Defense.''.

Subtitle A—Cyber Operations

SEC. 1501 [Log 82320]. ACCOUNTABILITY OF THE AUTHORIZATION TO OPERATE PROCESSES.

Section 1522 of the National Defense Authorization Act for Fiscal Year 2025 (Public Law 118-159; 10 U.S.C. 2223 note) is amended—

(1) in subsection (b)(2)—

(A) in subparagraph (C), by striking ''and'' at the end;

(B) in subparagraph (D), by striking the period at the end and inserting a semicolon; and

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

''(E) defines Department of Defense-wide, mandatory timelines for activities performed by authorizing officials with respect to an Authorization to Operate for cloud-hosted platforms, services, and applications; and

''(F) establishes processes and policies, developed in coordination with the Chief Information Officers of the military departments, for the boards established in subsections (c) and (d).'';

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

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

''(c) ESTABLISHMENT OF AUTHORITY-TO-OPERATE EXPEDITED APPEALS BOARD FOR THE DEPARTMENT OF DEFENSE.—

''(1) IN GENERAL.—Not later than 180 days after enactment of this Act, the Secretary of Defense shall establish a board, to be known as the 'Authority-to-Operate Expedited Appeals Board'.

''(2) RESPONSIBILITIES.—

''(A) IN GENERAL.—The board established under paragraph (1) shall decide whether to grant each Authorization to Operate for which a relevant stakeholder in the Authorization to Operate submission process submits a request in accordance with subparagraph (B) not later than 90 days after the date on which such relevant stakeholder submits such request.

''(B) SUBMISSION.—A relevant stakeholder in the Authorization to Operate submission process seeking a decision from the board established under paragraph (1) with respect to

an Authorization to Operate may submit a request for such decision to such board if—

''(i) a request for such Authorization to Operate was appropriately submitted to the authorizing official for such Authorization to Operate not less than 180 days prior to the submission to the board; and

''(ii) as of the date of such submission, such authorizing official has not made a final decision with respect such Authorization to Operate.

''(C) AUTHORIZING OFFICIAL AUTHORITY.—Upon the submission of a request for an Authorization to Operate in accordance with subparagraph (B), the authorizing official for an Authorization to Operate shall cease to have authority to grant or deny such Authorization to Operate.

''(3) SUBMISSION FOR CONSIDERATION.—The Secretary of Defense shall ensure that each relevant stakeholder in the Authorization to Operate submission process may submit to the board established under paragraph (1) a request for a decision under paragraph (2).

''(4) BOARD REQUIREMENTS.—

''(A) MEMBERSHIP.—The board established under paragraph (1) shall be composed of the following members:

''(i) The Chief Information Officer of the Department of Defense.

''(ii) The Commander of the United States Cyber Command.

''(iii) The Director of the Defense Information Systems Agency.

''(iv) Any other official determined appropriate by the chair of such board.

''(B) CHAIR.—The chair of the board established under paragraph (1) shall be the Chief Information Officer of the Department of Defense.

''(C) FREQUENCY.—The board established under paragraph (1) shall meet not less than frequently than quarterly.

''(5) EXISTING FORUM.—

''(A) IN GENERAL.—The Secretary of Defense may designate a body in the Department of Defense to carry the responsibilities described in paragraph (2) if—

''(i) the body so designated is in existence as of the date of the enactment of this subsection: and

''(ii) the responsibilities of such body relate to managing risks for information technologies.

''(B) EFFECTS.—If the Secretary of Defense designates a body under subparagraph (A)—

''(i) paragraph (1) shall not apply with respect to the Secretary; and

''(ii) such body shall be deemed to be a board established in such military department under paragraph (1) for the purposes of paragraphs (2) and (3).

''(C) DISSOLUTION.—If the body designated by the Secretary of Defense under this paragraph ceases to exist or becomes permanently unable to carry out the responsibilities described in paragraph (2), the Secretary may designate another body in the Department of Defense to carry out such responsibilities or establish a board in accordance with paragraph (1), except that the Secretary shall establish such board not later than 180 days after the

date on which the body designated by the Secretary under this paragraph ceases to exist or becomes permanently unable to carry out such responsibilities.

''(d) ESTABLISHMENT OF AUTHORITY-TO-OPERATE EXPEDITED APPEALS BOARD FOR THE MILITARY DEPARTMENTS.—

''(1) IN GENERAL.—Not later than 180 days after enactment of this Act, each Secretary of a military department shall establish in such military department a board.

''(2) RESPONSIBILITIES.—

''(A) IN GENERAL.—Each board established in a military department under paragraph (1) shall decide whether to grant each Authorization to Operate for which a relevant stakeholder in the Authorization to Operate submission process submits a request in accordance with subparagraph (B) not later than 90 days after the date on which such relevant stakeholder submits such request.

''(B) SUBMISSION.—A relevant stakeholder in the Authorization to Operate submission process seeking a decision from a board established in a military department under para-

graph (1) with respect to an Authorization to Operate may submit a request for such decision to such board if—

''(i) a request for such Authorization to Operate was appropriately submitted to the authorizing official for such Authorization to Operate not less than 180 days prior to the submission to the board;

''(ii) the Authorization to Operate is for an information system of such military department; and

''(iii) as of the date of such submission, the authorizing official for such Authorization to Operate has not made a final decision with respect such Authorization to Operate.

''(C) AUTHORIZING OFFICIAL AUTHORITY.—Upon the submission of a request for an Authorization to Operate in accordance with subparagraph (B), the authorizing official for an Authorization to Operate shall cease to have authority to grant or deny such Authorization to Operate.

''(3) SUBMISSION CAPABILITY.—The Secretary concerned for a military department shall ensure

that each relevant stakeholder in the Authorization to Operate submission process may submit to the board established in such military department under paragraph (1) a request for a decision under paragraph (2).

''(4) BOARD REQUIREMENTS.—

''(A) MEMBERSHIP.—A board established in a military department under paragraph (1) shall be composed of the following members:

''(i) The Chief Information Officer of such military department.

''(ii) The service acquisition executive of such military department.

''(iii) The commanders of the relevant service cyber components.

''(iv) Any other official determined appropriate by the chair of such board.

''(B) CHAIR.—The chair of a board established in a military department under paragraph (1) shall be the Chief Information Officer of such military department.

''(C) FREQUENCY.—Each board established under paragraph (1) shall meet not less than frequently than quarterly.

''(5) EXISTING FORUM.—

''(A) IN GENERAL.—The Secretary of a military department may designate an body in such military department to carry the responsibilities of described in paragraph (2) if—

''(i) the body so designated is in existence as of the date of the enactment of this subsection: and

''(ii) the responsibilities of such body relate to managing risks for information technologies.

''(B) EFFECTS.—If the Secretary of a military department designates a body under subparagraph (A)—

''(i) paragraph (1) shall not apply with respect to such Secretary; and

''(ii) such body shall be deemed to be a board established in such military department under paragraph (1) for the purposes of paragraphs (2) and (3).

''(C) DISSOLUTION.—If the body designated by the Secretary of a military department under this paragraph ceases to exist or becomes permanently unable to carry out the responsibilities described in paragraph (2), the Secretary may designate another body in such

military department to carry out such responsibilities or established a board in accordance in with paragraph (1), except that the Secretary shall establish such board not later than 180 days after the date on which the body designated by the Secretary under this paragraph ceases to exist or becomes permanently unable to carry out such responsibilities.''; and

(4) by inserting after subsection (e), as so redesignated, the following new subsection:

''(f) BIANNUAL REPORT.—

''(1) IN GENERAL.—Not later than six months after the date of the enactment of this subsection, and every six months thereafter under October 1, 2031, the Secretary of Defense shall submit to the congressional defense committees a report on activities under this section in the six-month period ending on the date of the submission of such report.

''(2) CONTENTS.—Each report required under paragraph (1) shall include, for the period covered by such report—

''(A) the number of new Authorizations to Operate;

''(B) the number of Authorizations to Operate evaluated;

"(C) the number of requests for Authorizations to Operate that were denied;

"(D) the number of requests for Authorizations to Operate submitted to the board established under subsection (c);

"(E) the number of requests for Authorizations to Operate resolved by the board established under subsection (c);

"(F) the number of requests for Authorizations to Operate submitted to a board established under subsection (d);

"(G) the number of requests for Authorizations to Operate resolved by a board established under subsection (d);

"(H) the average length of time required for a capability to receive an Authorization to Operate in accordance with the organization's implementation of the risk management framework publish by the National Institution of Standards and Technology in NIST Special Publication 800-37, or any amendatory or superseding document thereto;

"(I) the number of Authorizations to Operate issued pursuit to the policy of required by subsection (b);

"(J) the number of requested reciprocal Authorizations to Operate denied due to insufficiency of supporting evidence; and

"(K) a narrative summary identifying deficiencies in Bodies of Evidence packages that prevented an authorizing official from adopting the security analysis and artifacts, as appropriate, of a cloud-hosted platform, service, or application that has already been authorized by another authorizing official in the Department of Defense in accordance with the policy required by subsection (b).".

SEC. 1502 [Log 82332]. ASSESSMENT OF CYBER OPERATIONAL SUPPORT TO GEOGRAPHIC COMBATANT COMMANDS.

(a) REPORTS.—Not later than one year after the date of the enactment of this Act, each commander of a unified combatant command, other than the Commander of the United States Cyber Command, shall submit to the congressional defense committees a report assessing the sufficiency of support provided by the Commander of United States Cyber Command in carrying out the mission of such unified combatant command.

(b) ELEMENTS.—Each report submitted by a commander of a unified combatant command under subsection (a) shall include an evaluation of—

(1) the ability of the United States Cyber Command and the service cyber components to provide to such combatant command capabilities that align with the operational requirements of such commander, including capabilities to support such commander acting with respect to targets on the joint integrated prioritized target list of such commander; and

(2) such other matters as determined appropriate by such commander.

Subtitle B—Cybersecurity

SEC. 1511. [Log 82318] ANNUAL REPORT ON WEAPON SYSTEMS DATA ACCESSIBILITY AND SECURITY.

(a) IN GENERAL.—Not later than April 30, 2026, and annually thereafter until September 30, 2030, the Secretary of Defense, in coordination with the Secretary of the Army, Secretary of the Navy, and Secretary of the Air Force, shall submit to the congressional defense committees a report analyzing the weapons platforms of the Department of Defense that lack onboard, real-time cybersecurity capabilities.

(b) ELEMENTS.—Each annual report submitted under subsection (a) shall include, for each weapons platform analyzed in such report, the following:

(1) An explanation of why onboard, real-time cybersecurity capabilities have not yet been integrated into such weapons platform.

(2) An estimate of the cost to implement onboard, real-time cybersecurity capabilities into such weapons platform to enable monitoring and detection of cyber intrusions.

(3) A timeline, correlated with the cost estimate required under paragraph (2), to implement onboard, real-time cybersecurity capabilities across the

entire inventory of the Department of Defense of such weapons platform.

(c) ONBOARD, REAL-TIME CYBERSECURITY CAPABILITIES DEFINED.—In this section, ''onboard, real-time cybersecurity capabilities'' means technologies integrated into a weapons platform that mitigate cyber risks to operation, including serial bus monitoring capabilities or runtime application self-protection capabilities.

SEC. 1512. [Log 82581] INCORPORATION OF ARTIFICIAL INTELLIGENCE CONSIDERATIONS INTO ANNUAL CYBERSECURITY TRAINING.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, shall revise the mandatory annual training on cybersecurity for members of the Armed Forces and civilian employees of the Department of Defense to include content related to the unique cybersecurity challenges posed by the use of artificial intelligence.

(b) BRIEFINGS.—Not later than 90 days after the date of the enactment of this Act, and every 90 days thereafter until the training described in subsection (a) has been revised as required by such subsection, the Chief Information Officer of the Department of Defense shall provide to the Committees on Armed Services of the House of Representatives and Senate a briefing on the progress of such revision.

Subtitle C—Information Technology and Data Management

SEC. 1521. [Log 82364] BIOLOGICAL DATA FOR ARTIFICIAL INTELLIGENCE.

(a) AI ACCESSIBILITY TO QUALIFIED BIOLOGICAL DATA RESOURCES.—

(1) IN GENERAL.—Not later than one year after the enactment of this Act, the Secretary of Defense shall develop and implement requirements that ensure qualified biological data resources created by research entirely funded by the Department of Defense are collected and stored in a manner that facilitates the use of such qualified biological data resources for advanced computational methods, including artificial intelligence.

(2) RULES OF REQUIREMENTS.—The requirements implemented under subsection (a) shall include the following:

(A) A definition of the term ''qualified biological data resource'' for the purposes of such requirements, which shall be based on one or more of the following criteria:

(i) The type of biological data generated.

(ii) The size of collection of such biological data.

(iii) The amount of Federal funds awarded to the research that created such qualified biological data resource.

(iv) The level of sensitivity of the biological data generated.

(v) Any other factor determined appropriate by the Secretary of Defense.

(B) Guidance on the metrics and metadata included under such requirements to indicate data quality, including usability, interoperability, and completeness.

(C) Requirements for tiered levels of cybersecurity safeguards and access controls for the storage of biological data.

(D) Exceptions to such requirements, including for biological data that may implicate national security.

(E) Requirements for the protection of the privacy of individuals.

(b) CONSULTATION.—In developing and implementing the requirement under subsection (a), the Secretary shall consult with the Secretaries of the Armed Forces, the heads of the research laboratories of each of

the Armed Services, and private sector and academia recipients of funding for research from the Department of Defense to ensure that such requirements are not overly burdensome.

(c) REPORT.—Not later than one year after the date of the enactment of this Act, and annually thereafter, the Secretary shall submit to Congress a report describing the progress made in developing and implementing the requirements under subsection (a), including—

(1) the quantity of the biological data generated and stored in accordance with such requirement and accessible through application programming interfaces;

(2) user engagement with biological data in accordance with such requirements.

Subtitle D—Artificial Intelligence

SEC. 1531 [Log 82326]. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING SECURITY IN THE DEPARTMENT OF DEFENSE.

(a) CYBERSECURITY POLICY FOR ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING USE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Defense shall develop and implement a Department-wide policy for the cybersecurity and governance of artificial intelligence and machine learning, as well as the models for artificial intelligence and machine learning used in national defense applications.

(2) POLICY ELEMENTS.—The policy required under paragraph (1) shall address the following:

(A) Protection against security threats specific to artificial intelligence and machine learning, including model serialization attacks, model tampering, data leakage, adversarial prompt injection, model extraction, model jailbreaks, and supply chain attacks.

(B) Use of cybersecurity measures throughout the life cycle of systems using artificial intelligence or machine learning.

(C) Adoption of industry-recognized frameworks to guide the development and implementation of artificial intelligence and machine learning security best practices.

(D) Standards for governance, testing, auditing, and monitoring of systems using artificial intelligence and machine learning to ensure the integrity and resilience of such systems.

(E) Training requirements for the workforce of the Department of Defense to ensure personnel are prepared to identify and mitigate vulnerabilities that are specific to artificial intelligence and machine learning.

(3) REVIEW AND REPORT.—

(A) REVIEW.—The Secretary of Defense shall conduct a comprehensive review to identify and assess the effectiveness of the artificial intelligence and machine learning cybersecurity and governance practices of the Department of Defense.

(B) REPORT.—

(i) IN GENERAL.—Not later than August 31, 2026, the Secretary of Defense shall submit to the Committees on Armed Services of the House of Representatives

and the Senate a report on the findings of the review conducted under subparagraph (A).

(ii) CONTENTS.—The report required under clause (i) shall include—

(I) an assessment of the current security practices for artificial intelligence and machine learning across the Department of Defense;

(II) an assessment of the cybersecurity risks posed by the use of authorized and unauthorized artificial intelligence software, including models developed by companies headquartered in or operating from foreign countries of concern, by the Department;

(III) an identification of gaps in the existing security measures of the Department related to threats specific to the use of artificial intelligence and machine learning;

(IV) an analysis of the potential of security management, access, and runtime capabilities for artificial intelligence in the commercial sector for

use by the Department to defend system using artificial intelligence from threats, minimize data exposure resulting from the use of such systems, and maintain the trustworthiness of applications of the Department that use artificial intelligence;

(V) an evaluation of the alignment of the policies of the Department with industry frameworks;

(VI) recommend actions to enhance the security, integrity, and governance of artificial intelligence and machine learning models used by the Department; and

(VII) an identification of any additional authorities, resources, or legislative actions required for the Department to effectively implement artificial intelligence and machine learning model security policy required by paragraph (1).

(b) BILL OF MATERIALS FOR ARTIFICIAL INTELLIGENCE.—

(1) IN GENERAL.—Any policy, regulation, guidance, or requirement issued by the Department of Defense relating to the use, submission, or maintenance of a software bill of materials shall also apply to an artificial intelligence software bill of materials, to the extent practicable, for all artificial intelligence systems, models, and software used, developed, or procured by the Department.

(2) IMPLEMENTATION AND OVERSIGHT.—Not later than 180 days after the date of enactment of this Act, the Secretary of Defense, acting through the Chief Digital and Artificial Intelligence Officer of the Department of Defense and Chief Information Officer of the Department of Defense, shall revise the regulations, guidance, and policies of the Department of Defense to comply with paragraph (1), including guidance and standards for artificial intelligence software bill of materials, in accordance with the best practices for software bill of materials.

(3) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of the Department of Defense shall submit to the Committees on Armed Services of the House of Representatives and the Senate a report on—

(A) the status of the implementation of requirements for artificial intelligence software bill of materials under this subsection, including challenges, recommendations, and potential legislative or regulatory modifications needed to enhance the effectiveness of such implementation;

(B) the feasibility and necessity to update Department of Defense Instruction 5000.87, Operation of the Software Acquisition Pathway (October 2, 2020) and the software acquisition pathway established under section 3603 of title 10, United States Code, with requirements for artificial intelligence software bill of materials and more detailed software bill of materials in the procurement of software, hardware, artificial intelligence technologies, and cryptographic technologies; and

(C) the estimated costs for the implementation of the policies for artificial intelligence software bill of materials and more detailed software bill of materials required under this subsection and described in subparagraph (B), including for any new systems or investments required to support greater implementation and

adoption by the Department of Defense of artificial intelligence.

(c) DEFINITIONS.—In this section:

(1) The terms ''artificial intelligence'' and ''machine learning'' have the meanings given such terms, respectively, in section 5001 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

(2) The term ''artificial intelligence software bill of materials'' means the records kept in the normal course of business that identify each component, library, and dependency comprising an artificial intelligence software application.

(3) The term ''software bill of materials'' means the records kept in the normal course of business that identify each component, library, and dependency comprising a software application.

SEC. 1532 [Log 82351]. PILOT PROGRAM FOR DATA-ENABLED FLEET MAINTENANCE.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary concerned for a covered armed force, in consultation with the Chief Digital and Artificial Intelligence Officer of the Department of Defense, shall establish in such covered armed force a pilot program under which the covered armed force shall use commercially available artificial intelligence technologies to improve the maintenance of ground vehicles performed by such covered armed force.

(b) OBJECTIVES.—Under the pilot program established under subsection (a), the Secretary concerned shall—

(1) assess the feasibility and effectiveness of artificial intelligence-driven approaches in improving maintenance regimes for ground vehicles;

(2) assess the cost savings resulting from the use of artificial intelligence technology for the maintenance of ground vehicles; and

(3) identify and mitigate potential challenges and risks associated with the integration of artificial intelligence technology for modernized maintenance of ground vehicles, including cybersecurity concerns.

(c) REPORT.—Not later than one year after the date of the enactment of this Act, each Secretary concerned

for a covered armed force shall submit to Committees on Armed Services of the House of Representatives and the Senate a report on the activities performed under the pilot program established under subsection (a) in such covered armed force.

(d) TERMINATION.—The authority to carry out a pilot program under subsection (a) shall terminate on January 1, 2029.

(e) DEFINITIONS.—In this section:

(1) The term ''covered armed force'' means the Army, Navy, or Air Force.

(2) The term ''Secretary concerned'' has the meaning given such term in section 101(a) of title 10, United States Code.

SEC. 1533 [Log 82895]. GENERATIVE ARTIFICIAL INTELLIGENCE FOR NATIONAL DEFENSE.

(a) IN GENERAL.—Subject to the availability of appropriations, the Secretary of Defense shall carry out not less than two and not more than 12 generative artificial intelligence efforts to enhance the national security of the United States and the capabilities of the Department of Defense and to accelerate the adoption to generative artificial intelligence capabilities at the Department of Defense.

(b) DESIGNATION OF RESPONSIBLE ORGANIZATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall designate an organization in the Department of Defense which shall be responsible for managing and coordinating the efforts under subsection (a).

(c) SCOPE.—In managing the efforts under subsection (a), the head of the organization designated under subsection (b), in coordination with the Chairman of the Joint Chiefs of Staff and the commanders of the combatant commands, shall evaluate how generative artificial intelligence can enhance the efficiency and improve the mission effectiveness of the Department of Defense with respect to the following:

(1) Damage assessment from battlefield imagery and video.

(2) Human and machine teaming interfaces.

(3) Cybersecurity.

(4) Mission analysis.

(5) Order of battle.

(6) Mission planning.

(7) Intelligence collection and analysis.

(8) Any other areas the Chairman of the Joint Chiefs of Staff or the commanders of the combatant commands determine appropriate in addressing existing or anticipated mission requirements of the Department of Defense.

SEC. 1833.[Log 82219] REQUIREMENTS FOR MODULAR OPEN SYSTEM APPROACH AND MODIFICATIONS TO RIGHTS IN TECHNICAL DATA.

(a) REQUIREMENTS FOR MODULAR OPEN SYSTEM APPROACH.—Section 4401 of title 10, United States Code, is amended to read as follows:

"§ 4401. Requirement for modular open system approach

''(a) REQUIREMENT.—The Secretary of Defense shall ensure that a covered system to be procured is designed and developed, to the maximum extent practicable, with a modular open system approach.

''(b) ASSESSMENT TO INFORM STRATEGY.—Before designing or developing a covered system, the Secretary of Defense shall conduct an assessment to identify the open systems objectives to be achieved by the design and development of the covered system. Such assessment shall identify and document how such approach would—

''(1) support the objectives of the defense acquisition system established pursuant to section 3102 of this title;

''(2) align with the preference for the acquisition of commercial products in section 3453 of this title to retain, to the maximum extent practicable, the commercial viability of subsystems and components of the covered system;

''(3) reduce the complexity and increase the speed by which new technology can be integrated into a covered system to enhance miliary effectiveness and responsiveness to emerging threats;

''(4) enable the use of iterative development cycles and discontinue or terminate the development of capabilities—

''(A) that no longer align with approved capability requirements (as defined in section 181 of this title) or priorities; or

''(B) that are experiencing significant cost growth, performance deficiencies, or delays in schedule;

''(5) promote a robust and responsive defense industrial base, and foster competition amongst offerors of subsystems and components of the covered system through the life cycle of the covered system, especially at the module level;

''(6) reduce schedule delays and development timelines;

''(7) increase and enable interoperability of a covered system with the joint force as changes to force design evolve; and

''(8) enable effective life-cycle management and product support of a covered system—

''(A) in accordance with the requirements of section 4322 [*log 82283*] of this title; and

''(B) to ensure that the covered system will meet applicable operational readiness requirements (as defined in such section 4322) and materiel readiness objectives (established under section 118(c) of this title) in the most cost-effective manner practicable.

''(c) ARCHITECTURE REQUIREMENTS.—(1) In developing an architecture for the procurement of a covered system using a modular open system approach, the Secretary shall ensure that the architecture—

''(A) adequately designates and defines modules, module interfaces, key interfaces, and openness characteristics of the covered system necessary to achieve the open systems objectives described in subsection (b);

''(B) to the extent practicable, is based on—

''(i) widely accepted, consensus-based standards that are available at no cost or under fair and reasonable license terms; or

''(ii) if such standards are not available or suitable, incremental standards that define relationships between module interfaces and key interfaces; and

''(C) is designed and developed to accelerate the procurement and integration of commercial products as modules, module interfaces, and key interfaces.

''(2) The Secretary shall consider input from private entities as early as possible to inform decisions regarding the level in the architecture at which a modular open system approach will be implemented for a covered system.

''(3) The architecture described in this subsection shall be included in any draft and final solicitations for procurement of a covered system.

''(d) OPENNESS CHARACTERISTICS.—Consistent with the requirements of subchapter I of chapter 275 of this title, the Secretary shall include in the solicitation for the covered system a description of the desired openness characteristics of the covered system necessary to achieve the open systems objectives described in subsection (b), including the following:

''(1) The open systems objectives identified as result of the assessment required by subsection (b).

''(2) A description of the application of specifications or standards for module interfaces to achieve such objectives.

''(3) A description of the minimum technical data package elements necessary to achieve such objectives.

''(4) The desired license rights in module interfaces or key interfaces based on such objectives, including desired license rights to enable the replacement of a module or module interface with an alternative or new module or module interface.

''(e) APPLICABILITY TO COMMERCIAL PRODUCTS.—In applying the requirements of this section to a covered system that includes a commercial product, the Secretary of Defense shall—

''(1) implement modular open system approaches in accordance with such approaches used in the ordinary course of business for such commercial product on the commercial marketplace;

''(2) for a commercial product that is commercial technical data or commercial software, procure such commercial product under license terms similar to such terms that are customarily provided to the public, unless the Secretary has specifically negotiated different license terms;

''(3) when applicable, obtain the delivery of commercial software development kits with license rights necessary to support the desired openness characteristics for the covered system; and

''(4) to the maximum extent practical, conduct negotiations for desired license rights in accordance

with the preference for specially negotiated licenses in section 3774(c) of this title.

''(f) DEFINITIONS.—In this section:

''(1) The term 'covered system' means a system acquired or developed under—

''(A) an acquisition program of the Department of Defense; or

''(B) a research and development program of the Department to address a capability requirement or joint capability requirement (as defined in section 181 of this title).

''(2) The term 'incremental standard' means a specification for a module interface or key interface that includes—

''(A) software-defined syntax and properties that specifically govern how values are validly passed and received between subsystems and components in machine-readable format;

''(B) a machine-readable definition of the relationship between the module interface or key interface and existing common standards or interfaces available in Department databases; and

''(C) documentation with functional descriptions of software-defined interfaces, con-

veying semantic meaning of elements of the module interface or key interface.

''(3) The term 'key interface' means a shared boundary between any system, subsystem of a covered system, or set of modules, defined by various physical, logical, functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software.

''(4) The term 'modular open system approach' means the application of a strategy that leverages an architecture that enables modules to be incrementally added, removed, or replaced throughout the life cycle of the covered system to achieve a set of objectives.

''(5) The term 'module' means a self-contained functional hardware or software unit—

''(A) that can be developed, tested, and deployed independently of a module interface or key interface; and

''(B) that can simultaneously interact with another self-contained functional hardware or software unit described in subparagraph (A) through a module interface or key interface.

''(6) The term 'module interface' means a shared boundary between modules, defined by phys-

ical, logical, and functional characteristics, such as electrical, mechanical, fluidic, optical, radio frequency, data, networking, or software.

''(7) The term 'software development kit' means a collection of software tools and programs such as libraries, application programming interfaces, integrated development environments, testing tools, or documentation used to create applications that are appropriate for a specific software platform.''.

(b) GUIDANCE.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall issue guidance to carry out the requirements of section 4401 of title 10, United States Code, as amended by this section.

(c) APPLICABILITY.—The requirements of section 4401 of title 10, United States Code, as amended by this section, shall apply with respect to a contract entered into on or after the date of the enactment of this Act.

(d) MODIFICATION TO RIGHTS IN TECHNICAL DATA.—

(1) RIGHTS IN TECHNICAL DATA.—Section 3771 of title 10, United States Code, is amended—

(A) in subsection (a)—

(i) in paragraph (2)(A), by striking ‘‘ or copyrights’’ and inserting ‘‘, copyrights, trade secrets,’’; and

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

‘‘(3) ENFORCEMENT OF CERTAIN RIGHTS.—Regulations prescribed under paragraph (1) may not affect or limit any right described in paragraph (2)(A) or the ability of a contractor or subcontractor to enforce such a right against a third party that has not otherwise obtained a license for such a right from the United States or from the contractor or subcontractor.’’; and

(B) in subsection (b)—

(i) in paragraph (2), by striking ‘‘paragraphs (3), (4), and (7),’’ and inserting ‘‘paragraphs (3) and (4),’’;

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

‘‘(3) INAPPLICABILITY OF PARAGRAPH (2).—Unless otherwise negotiated, paragraph (2) does not apply to technical data that—

‘‘(A) constitutes a correction or change to data furnished by the United States; or

''(B) is otherwise publicly available or has been released or disclosed by the contractor or subcontractor without restriction on further release or disclosure.'';

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

''(4) EXCEPTIONS TO PARAGRAPH (2).—(A) Notwithstanding paragraph (2), unless otherwise negotiated, the United States shall have government purpose rights, in perpetuity, in technical data that—

''(i) relates to form, fit, or function of an item or process; or

''(ii) is necessary for operation, maintenance, installation, or training (other than detailed manufacturing or process data) of an item or process.

''(B) Notwithstanding paragraph (2), the United States may release or disclose technical data to persons outside the Government, or permit the use of technical data by such persons, if such release, disclosure, or use—

''(i) is necessary for emergency repair and overhaul;

''(ii) is a release or disclosure of technical data (other than detailed manufacturing or process data) to, or use of such data by, a foreign government, where such release or disclosure is in the interest of the United States and is required for evaluation or informational purposes;

''(iii) is made subject to a prohibition that the person to whom the data are released or disclosed may not further release, disclose, or use such data; and

''(iv) the contractor or subcontractor asserting the restriction is notified of such release, disclosure, or use.'';

(iv) in paragraph (6)—

(I) in the paragraph heading, by striking ''INTERFACES'' and inserting ''MODULE INTERFACES OF AN ITEM'';

(II) by inserting '', in perpetuity,'' after ''government purpose rights''; and

(III) by striking ''an interface between an item or process and other items or processes'' and inserting ''a module interface of an item''; and

(v) in paragraph (7)—

(I) in the paragraph heading, by striking ''MODULAR SYSTEM INTERFACES'' and inserting ''KEY INTERFACES OF AN ITEM'';

(II) in subparagraph (A)—

(aa) by striking ''paragraphs (2) and (5)'' and inserting ''paragraph (5) and except as otherwise provided by subsection (e) of section 4401 of this title,'';

(bb) by inserting '', in perpetuity,'' after ''government purpose rights''; and

(cc) by striking ''modular system interface'' and inserting ''key interface of an item'';

(III) in subparagraph (B), by striking ''modular system interface'' and inserting ''a key interface''; and

(IV) in subparagraph (C), by striking ''modular system interface'' and inserting ''key interface of an item''.

(2) DEFINITIONS.—Section 3775(b) of title 10, United States Code, is amended to read as follows:

''(b) ADDITIONAL DEFINITIONS.—In this subchapter, the terms 'key interface', 'modular open system approach', 'module interface' have the meanings given, respectively, in section 4401 of this title.''.

(e) CONFORMING AMENDMENTS.—

(1) Section 3791(c)(1) of title 10, United States Code, is amended—

(A) in subparagraph (A), by striking ''section 4401(b) of this title'' and inserting ''section 4401 of this title''; and

(B) in subparagraph (D)(iv), by striking ''modular system interfaces (as defined in section 4401(b) of this title)'' and inserting ''module interfaces (as defined in section 4401(f) of this title)''.

(2) Section 4402 of title 10, United States Code, is repealed.

(3) Section 4403 of title 10, United States Code, is repealed.

(4) Section 4425 of title 10, United States Code, is amended to read as follows:

''§ 4425. Definitions

''In this subchapter:

''(1) The term 'major system platform' means the highest level structure of a major weapon system that is not physically mounted or installed onto a higher level structure and on which a major system component can be physically mounted or installed.

''(2) The term 'weapon system component'—

''(A) means a high level subsystem or assembly, including hardware, software, or an integrated assembly of both, that can be mounted or installed on a major system platform through a key system interface (as defined in section 4401(f) of this title); and

''(B) includes a subsystem or assembly that is likely to have additional capability requirements, is likely to change because of evolving technology or threat, is needed for interoperability, facilitates incremental deployment of capabilities, or is expected to be replaced by another subsystem or assembly described in subparagraph (A).''.

(5) Section 804 of the National Defense Authorization Act for Fiscal Year 2021 (10 U.S.C. 4401 note) is repealed.

SEC. 1834.[Log 82204] BRIDGING OPERATIONAL OBJECTIVES AND SUPPORT FOR TRANSITION PROGRAM.

(a) BRIDGING OPERATIONAL OBJECTIVES AND SUPPORT FOR TRANSITION PROGRAM.—

(1) ESTABLISHMENT.—In meeting the responsibilities of the Defense Innovation Unit under section 4127(d) of title 10, United States Code, the Director of the Defense Innovation Unit shall establish a program (to be known as the ''Bridging Operational Objectives and Support for Transition program'') to accelerate the adoption or integration of commercial technologies into programs of record of the Department of Defense.

(2) PROGRAM EXECUTION.—Not later than 90 days after the date of the enactment of this subsection, the Director shall issue guidance on the BOOST program, including guidance to do the following:

(A) Enable a customer seeking a technology solution for a challenge or requirement in a program of record of the Department of Defense to request assistance under the BOOST program with identifying and adopting or integrating such a solution into such program.

(B) Establish requirements for the Defense Innovation Unit to—

(i) conduct a review of commercial technologies pursuant to a request described in subparagraph (A) with respect to a challenge or requirement of a program of record of the Department to identify commercial technology that may address such challenge or requirement;

(ii) provide to the customer that made such request the findings of such review, including any commercial technologies so identified; and

(iii) at the request of such customer after providing such findings to such customer, conduct development, experimentation, or integration activities in coordination with such customer to support or enable the adoption or integration of any commercial technology so identified into such program of record.

(C) Establish criteria for terminating assistance under the BOOST program for a customer or with respect to a commercial technology.

(3) SUPPORT TO OTHER PROGRAMS.—The Director shall ensure the BOOST program works with and in support of—

(A) the program established under section 4061(a) of title 10, United States Code;

(B) other organizations of the Department of Defense responsible for accelerating the adoption and integration of technology in systems or programs of the Department;

(C) the Small Business Innovation Research Program;

(D) the Small Business Technology Transfer Program; and

(E) the Joint Rapid Acquisition Cell (as described in the Department of Defense Directive 5000.71 titled ''Rapid Fulfillment of Combatant Commander Urgent Operational Needs'' (August 24, 2012)).

(4) FUNDING.—Subject to the availability of appropriations, amounts authorized to be appropriated the Defense Innovation Unit for research, development, test, and evaluation for a fiscal year may be used for such fiscal year to carry out the BOOST program.

(5) SUNSET.—The authorities and requirements under this subsection shall expire on December 31, 2030.

(b) REPORTING.—Not later than two years after the date of the enactment of this Act, the Secretary of Defense, in coordination with the Under Secretary of Defense for Acquisition and Sustainment and the Director, submit to the congressional defense committees a report on the effectiveness of the BOOST program in accelerating the adoption or integration of commercial technologies into programs of record of the Department of Defense, including—

(1) a summary description of customers and technologies adopted or integrated into such programs of record based on assistance provided under the BOOST program;

(2) recommendations of the Secretary to improve the BOOST program; and

(3) a recommendation whether to continue or terminate the BOOST program.

(c) DEFINITIONS.—In this section:

(1) The term ''BOOST program'' means the program established under subsection (a)(1).

(2) The term ''customer'' means a program manager or program executive officer of the Depart-

ment of Defense that has primary responsibility for fielding the system or systems acquired.

(3) The term ''Director'' means the Director of the Defense Innovation Unit.

(4) The term ''program executive officer'' has the meaning given such term in section 1737(a) of title 10, United States Code.

(5) The terms ''Small Business Innovation Research Program'' and ''Small Business Technology Transfer Program'' have the meanings given such terms, respectively, in section 9(e) of the Small Business Act (15 U.S.C. 638(e)).

DIRECTIVE REPORT LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, ARMY

Items of Special Interest

Army Research on Electromagnetic Pulse Weapon Threats

The committee understands the potential threat that electromagnetic pulse (EMP) weapons could pose to Department of Defense systems and domestic critical infrastructure. The committee is aware of efforts by the Army Research Laboratory and academia to study EMP effects and develop technologies and countermeasures to improve the ability to protect against such effects. The committee therefore directs the Secretary of the Army to provide a briefing to the House Committee on Armed Services not later than February 15, 2026, on how the Army Research Laboratory works with academic partners to advance the Department of the Army's understanding of EMP effects and countermeasures.

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, AIR FORCE

Items of Special Interest

Extended-Capability High-Energy Laser

The committee recognizes the potential for high energy lasers (HEL) deployed on long-endurance airborne platforms to contribute to the defense of the homeland and close gaps in current missile defense architectures. The committee also notes the need for further maturation of key technologies, particularly beam control capabilities suitable for laser sources above 500 kilowatts. Therefore, the committee directs the Secretary of the Air Force to provide a briefing to the House Committee on Armed Services, not later than December 1, 2025, describing HEL enabling technologies that have transitioned in the past five years or are planned to transition within the next five years to test on airborne platforms or representative surrogates, as well as options and associated resourcing requirements for transition effort acceleration.

Integration of Airborne Augmented Reality

The committee notes the potential for innovative technologies such as airborne augmented reality to modernize and improve pilot training, and believes that such technologies could also assist in mission scenario rehearsal and visualization for operational units. The committee is aware that the Air Force is

currently engaged in efforts to develop and mature augmented reality technologies, including through Small Business Innovation Research grants, and encourages the Air Force to continue resourcing these efforts. The committee directs the Secretary of the Air Force to provide a briefing to the House Committee on Armed Services not later than December 1, 2025, describing current Air Force efforts regarding airborne augmented reality systems, the technological maturity of such systems, and the potential impact of such systems on pilot training, including any opportunities for, and challenges to, their integration and validation.

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

Items of Special Interest

Advanced Radioisotope Power Systems

The committee recognizes the need for long-duration, resilient energy sources to support military operations in harsh and remote environments. The committee is aware that advanced radioisotope power systems, including both radioisotope thermal generators and radioisotope heater units, offer long-lasting, low-maintenance power and heating without frequent resupply.

The committee notes the potential for novel radioisotope production methods, such as compact fusion systems designed to generate high-energy neutrons, to enable on-demand edge production of radioisotopes and reduce reliance on centralized or foreign supply chains. The committee believes that this approach could broaden the range of viable isotopes beyond plutonium and strontium, including to isotopes with short half-lives and minimal shielding requirements, and that such developments could expand the operational utility of radioisotope power systems in expeditionary settings.

The committee therefore directs the Under Secretary of Defense for Research and Engineering to provide a briefing to the House Committee on Armed Services by December 1, 2025. The briefing should describe:

(1) current and potential radioisotope power systems suitable for military use;

(2) viable isotopes for such systems and their potential production methods, including fusion-based neutron generation;

(3) the feasibility of compact, forward-deployable production systems;

(4) relevant foreign developments; and

(5) the potential for such systems to fulfill relevant Department of Defense needs and requirements or enable novel capabilities.

Aluminum-Scandium Alloy Prototype Parts Development and Demonstration

The committee is aware of potential efforts to support domestic sourcing of scandium oxide. The committee notes the possibility that such domestic sourcing at a sufficient level of annual production could be sufficient to accelerate development

of a complete domestic supply chain for scandium products, including aluminum-scandium alloys, which have important applications for defense, aerospace, and space, and whose use has to date been supply-limited. The committee encourages the Department to utilize available tools and authorities, such as those provided to the Defense Logistics Agency and the Office of Strategic Capital, to evaluate and appropriately resource development and demonstration activities that would enable rapid exploitation of scandium alloys in relevant programs should expanded domestic sourcing become available. The committee directs the Deputy Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than March 1, 2026, containing an assessment of projected potential utilization of aluminum-scandium alloys and other scandium derivatives for defense programs.

Bioindustrial Manufacturing Innovation Institute

The committee is aware that the BioIndustrial Manufacturing and Design Ecosystem (BioMADE), the Department of Defense's Manufacturing Innovation Institute for bioindustrial manufacturing, involves nearly 300 members across 37 states, including industry leaders, academic institutions, and Government officials. The committee recognizes BioMADE's important responsibility to develop a network of open-access, precommercial bioindustrial facilities, and believes that this initiative is a critical enabler of a stronger U.S. bioindustrial manufacturing sector, a more robust biomanufacturing workforce, and a more advanced defense industrial base.

The committee believes that effective execution of BioMADE's mandate is critical to maintaining U.S. defense and strategic advantage. Therefore, in addition to the requirements of section 215 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263), the committee directs the Under Secretary of Defense for Research and Engineering to submit a report to the House Committee on Armed Services not later than February 1, 2026, describing BioMADE execution details. This report shall be unclassified but may include a classified annex. The report should include:

(1) an assessment of statutory barriers impeding the use of congressionally appropriated funds to build facilities;

(2) an explanation of BioMADE's role in achieving Department of Defense objectives, and of Department plans to utilize BioMADE;

(3) the average time required for BioMADE to execute contracts, from solicitation closure to award receipt;

(4) a list of current BioMADE awardees;

(5) details of all BioMADE grants made, planned, or in execution for the preceding fiscal year and the Future Years Defense Program, including amounts, purposes, execution timelines, and budget allocations over time;

(6) site selection decisions, criteria, processes, and timelines for facility construction;

(7) grant award selection decisions, criteria, processes, timelines, and communication mechanisms for members;

(8) membership structure and benefits, and their impact on access and payment for infrastructure usage;

(9) timeframes for integrating new members into the network; and

(10) mechanisms for interagency collaboration, particularly with regard to Department of Energy National Laboratories and precommercial infrastructure.

Biotechnology Research Collaboration

The committee believes biotechnology to be a key emerging technology area for future U.S. military advantage. The committee is aware that, as a fundamentally multidisciplinary technology area, collaboration is fundamental for advancing the technology, encouraging innovation, maximizing investments, and reducing duplication.

However, the committee is concerned that the current complex process for biotechnology collaboration may stifle cooperation and result in a more siloed ecosystem. The committee has observed evidence that collaborations between research laboratories, regardless of whether they are intra- or inter-service, are difficult to initiate due to the long negotiation process for terms and issues, such as the ownership of any resulting intellectual property. The committee is concerned that these unnecessary barriers may slow biotechnology innovations that could enable important future military 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 December 1, 2025, on the Department of Defense's efforts and progress toward enhancing inter-service and inter-department cooperation on biotechnology research. The briefing should include:

(1) any past efforts to streamline inter-service and inter-department collaboration in biotechnology, as well as any lessons learned from those efforts;

(2) Department efforts to streamline, standardize, and update the existing memorandum of understanding process between relevant entities, especially between the military services' research laboratories;

(3) a description of any roadblocks, including statutory issues, preventing a more streamlined collaboration process related to biotechnology and how the Department might overcome those roadblocks, or a description of any statutory relief needed; and

(4) the predicted timelines for updating and streamlining such collaboration processes.

Defense Advanced Research Projects Agency Biotechnology Programs

The committee is aware of past programs undertaken by the Defense Advanced Research Projects Agency (DARPA) intended to explore and strengthen supply chains, such as LogX, Open Price Exploration for National Security, and

Resilient Supply-and-Demand Networks, which have developed novel technology tools to analyze and diagnose threats or vulnerabilities, provide projections and prognoses, and stress-test supply chains to assess resilience levels.

Building on these efforts, and in acknowledgment of the specific needs for biotechnology supply chain resilience, the committee supports further efforts by DARPA and elsewhere in the Department of Defense on supply chains, especially programs that could be relevant to emerging technologies such as biotechnology. In particular, the committee encourages additional efforts to develop better understanding of complex supply chains and promote biotechnology as a solution to supply chain challenges, such as the Environmental Microbes as a BioEngineering Resource program.

Therefore, the committee directs the Director of DARPA to provide a briefing to the House Committee on Armed Services, not later than July 1, 2026, on:

(1) efforts to expand programs focused on understanding complex supply chains and solving supply chain challenges, particularly those related to biotechnology;

(2) barriers to additional programs in understanding complex supply chains and solving such supply chain challenges for biotechnology; and

(3) efforts to promote biotechnology as a solution to supply chain challenges.

Defense Innovation Unit Geographic Expansion

The committee recognizes the ability of the Defense Innovation Unit (DIU) to further the United States' diplomatic and strategic interests around the world. However, the committee believes that limitations such as staffing headcount and constrained budgets mean that DIU must be strategic and deliberate in its partnerships and office locations, both domestically and internationally.

Therefore, the committee directs the Director of DIU to submit a report to the House Committee on Armed Services by March 15, 2026, detailing a comprehensive set of criteria for selecting future DIU international or domestic locations, partnerships, military embeds, or liaison officers. The criteria shall align with the National Defense Strategy and should include, but is not limited to, the following:

(1) alignment with the Administration and national security guidance;

(2) alignment with the Department of Defense's needs to ensure locations and partnerships support emerging operational requirements and long-term capability needs of the Department;

(3) proximity to innovation hubs such as universities, research institutions, private sector technology ecosystems with relevance to Department modernization priorities, Federal Government innovation organizations, or other DIU or defense innovation community of entity locations;

(4) assessment of existing Federal, State, and local innovation ecosystems to avoid duplication and ensure efficient use of available resources and presence across the United States;

(5) expected near- and long-term outcomes for defense innovation;

(6) workforce and talent pool availability;

(7) potential for public-private collaboration;

(8) geographic and strategic distribution;

(9) existing U.S. military presence;

(10) resource availability, including for establishment and sustainment cost, infrastructure, and workforce requirements; and

(11) any other relevant elements identified by the Director.

Fusion Energy and Domestic Energy Supply Chain

The committee is aware of near-term developments in fusion energy technology maturation that could result in commercialization and opportunities to scale or focus such technologies to support Department of Defense objectives and missions. The committee believes that, as fusion energy technologies mature, a strong and globally competitive domestic industrial base would be advantageous to U.S. national security. The committee is therefore concerned about the possibility that certain elements of the fusion energy supply chain may become dependent on foreign sources of materials or components, and that the rapid pace of technology development may outstrip the ability of the Department of Defense to analyze, monitor, and react to supply chain uncertainties. In particular, the committee notes that certain fusion technologies have achieved commercial readiness to a level sufficient for completion of Power Purchase Agreements with private sector customers, but that the Department of Defense has yet to sufficiently articulate objectives, requirements, and metrics for fusion technologies.

The committee therefore directs the Secretary of Defense to provide a report to the House Committee on Armed Services not later than January 30, 2026 containing:

(1) opportunities and objectives for Department adoption of fusion energy technologies of varying capabilities;

(2) obstacles to fusion energy adoption, including statutory, regulatory, and other matters;

(3) an analysis of key attributes and metrics necessary for adoption of fusion energy technologies;

(4) an overview of essential fusion supply chain components and critical materials, including an analysis of the current availability of these materials through domestic or trusted partner supply chains;

(5) an overview of Department stakeholders for fusion energy technology adoption; and

(6) an overview of the regulatory environment governing development, testing, adoption, and deployment of fusion energy technologies for national security purposes.

Integrated Hypersonic Propulsion

The committee supports the Defense Advanced Research Projects Agency's plans to begin development of a reusable hypersonic aircraft demonstrator in fiscal year 2027. The committee notes that development of an integrated hypersonic propulsion system capable of operating across the speed ranges necessary for reusable hypersonic flight is critical to the success of a potential program. Further, the committee recognizes recent technology breakthroughs related to propulsion system transitions from supersonic to hypersonic flight that may provide greater range and operational capability to reusable hypersonic aircraft. The committee believes that further investment in fiscal year 2026 in these technologies and associated risk reduction activities is necessary in preparation for the demonstrator program.

Therefore, the committee directs the Secretary of Defense, in coordination with 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, 2025, to include:

(1) the Department's reusable hypersonic propulsion strategy, including the acquisition strategy for a demonstrator;

(2) details of the technologies under development to increase the efficiency and reliability of a reusable hypersonic propulsion system and the projected impact of such technologies on the operational capability; and

(3) the transition plan of the reusable hypersonic aircraft from demonstrator to production.

Military Use of Hypersonic Aircraft

The committee remains concerned that the United States may lag in the development of hypersonic aircraft relative to countries of concern. The committee believes that hypersonic aircraft could provide expanded opportunities for responsive power projection at range and speed, and therefore believes that a comprehensive plan to develop, procure, utilize, and sustain hypersonic aircraft and their enabling technologies is essential in order to avoid technological disadvantage in future conflicts. The committee, therefore, encourages the Department of Defense to continue and expand its investment in hypersonic aircraft development to enable future technological advantage for the United States.

Accordingly, the committee directs the Secretary of Defense to provide a report to the House Committee on Armed Services not later than February 1, 2026, on plans for development of military-use hypersonic aircraft. The report shall include, but is not be limited to:

(1) a roadmap for the development, demonstration, and integration of hypersonic aircraft and enabling technology to support national security objectives;

(2) an evaluation of current Department of Defense and U.S. Government testing facilities and their ability to support the cadence and complexity of anticipated hypersonic weapon and aircraft development programs;

(3) an evaluation of commercial platforms, facilities, and capabilities that could be leveraged to address any Department of Defense testing shortfalls identified in (2); and

(4) an evaluation of associated workforce capacity challenges, if any, associated with hypersonic aircraft development and testing that could be addressed through partnerships with the hypersonic aircraft industrial base and academia.

OPERATIONAL TEST AND EVALUATION, DEFENSE

Items of Special Interest

Holloman High Speed Test Track

The committee is aware of the role of Holloman High Speed Test Track in the testing and evaluation of advanced weapon systems and warfighting capabilities. The committee believes the Holloman High Speed Test Track provides the Department of Defense with uniquely valuable capabilities to validate current and future weapon systems in dynamic and realistic test environments, and represents a national asset that must be preserved and modernized in order to maintain leadership in key technical areas. Given the importance of this infrastructure, the committee directs the Secretary of the Air Force to provide a briefing to the House Committee on Armed Services not later than December 1, 2025, on the Air Force's plan and timeline for construction of a new parallel test track at the Holloman High Speed Test Track.

Multi-Service Advanced Capability Hypersonic Test Bed

The committee supports the efforts of the Department of Defense to create a robust Multi-Service Advanced Capability Hypersonic Test Bed (MACH-TB) in order to rapidly accelerate the development of hypersonic capabilities. The committee is aware that since this effort's inception, multiple Department stakeholders have requested their technology be tested on MACH-TB flights. The committee understands that several strategic nuclear programs have emergent testing demands relevant to MACH-TB capabilities, and notes that hypersonic and strategic weapon systems may operate in a similar regime in terms of physics and data requirements due to their extreme speeds, altitudes, and thermal loadings. The committee believes that MACH-TB provides a cost-effective test platform to collect foundational data for the hypersonic and strategic communities, and applauds the Department's efforts to merge these common testing priorities effectively and efficiently and fulfill them within the MACH-TB program. The committee therefore believes that robust funding of this program is essential to national security and to many of our most vital programs. 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, 2026,

on the current flight test plan manifest for MACH-TB, including supported programs, and the potential for strategic nuclear programs and homeland missile defense programs to leverage MACH-TB capabilities.

TITLE XV—CYBERSPACE-RELATED MATTERS

ITEMS OF SPECIAL INTEREST

Artificial Intelligence Software for Contract Efficiencies

The committee is encouraged by work currently underway at Army Program Executive Office Enterprise Information Systems (PEO-EIS) to utilize commercially available artificial intelligence (AI)-enabled software to eliminate duplicative software licenses, identify best sources of supply, and enable bulk purchases through contract consolidation. The committee believes that efforts to better leverage AI-enabled software, such as that by PEO-EIS, enable improved effectiveness, speed and efficiency of contracting decisions and could help to reduce duplicative costs. The committee encourages the Army to support and resource broader adoption of software tools to improve contracting and procurement decision-making, including those using artificial intelligence and machine learning.

The committee directs the Secretary of the Army to provide a briefing to the House Committee on Armed Services not later than February 1, 2026, that describes:

(1) current commercially available tools for improved contract decision-making and visibility for users;

(2) projected resourcing and personnel requirements, cost savings, efficiencies, and any cybersecurity or other effects on the contracting enterprise; and

(3) any relevant timelines for testing and adoption of such technologies.

Cloud Computing, Data Storage Considerations, and Other Related Matters

Given the speed that cloud computing is evolving, the committee is interested to learn how the Department of Defense is positioned to move quickly and securely in capitalizing on these advancements. Risk mitigation measures, such as separation of data, zero trust architecture, and data recovery capabilities, are available to commercial and government customers. However, the speed by which the Department can seize on these capabilities is unclear to the committee. In furthering its oversight, the committee directs the Chief Information Officer of the Department of Defense provide a briefing to the House Committee on Armed Services, not later than May 31, 2026, that includes:

(1) an assessment of the benefits and costs associated with existing Department of Defense policy regarding data residency;

(2) existing policy related to data recovery from a cloud outage or malicious cyber attack;

(3) the benefits, costs, and risks associated with changes to Department of Defense policy around data residency and data recovery; and

(4) the Department's overall private cloud strategy, including the status of its implementation of its existing private cloud platform, and potential opportunities for additional private cloud platform implementation.

Containerized Computing within the Department of Defense

The committee is aware of efforts in the Department of Defense, specifically in the Department of the Air Force, to emphasize confidential computing, the technical capacity to ensure that data remains encrypted during processing. The committee understands that this technology can minimize the risks associated with unauthorized access or data breaches by maintaining encryption while the data is in use. Most notably, the committee is cognizant of the Department of the Air Force's Platform One efforts to support and encourage prioritization and utilization of confidential computing. By keeping software data protected throughout its lifecycle, confidential computing can strengthen the overall security of defense operations, ensuring that sensitive information is not exposed during processing. To better understand how other military services are considering confidential computing, the committee directs the Chief Information Officer of the Department of the Army, in coordination with the Chief Information Officer of the Department of the Navy and Chief Information Officer of the Department of the Air Force, to provide a briefing to the House Committee on Armed Services not later than March 1, 2026, on how their offices incorporate confidential computing into existing efforts.

Defense Travel System

The committee is concerned that, despite legislation seeking to address problems with the Defense Travel System (DTS), the Department of Defense is not postured to advance the state of a critically important business system. The present iteration of DTS remains anchored in outmoded technologies and processes which consume the time of uniformed and civilian personnel to an unnecessary degree. The committee continues to express the view that alternative and commercially available technologies can be quickly procured which address many of the inefficiencies of the current system. The committee directs the Under Secretary of Defense for Personnel and Readiness to submit a report to the House Committee on Armed Services not later than May 1, 2026, that includes:

(1) an evaluation of the costs and efforts of available technologies to replace the existing DTS architecture;

(2) estimated timelines and schedules of the effort; and

(3) an analysis of the procurement vehicles to be leveraged for the DTS replacement.

Enterprise-wide Artificial Intelligence Infrastructure

The committee asserts the view that the Department of Defense's use of Artificial Intelligence (AI) will only be successful with the establishment of enterprise-wide infrastructure, applications, and tools. Over the course of multiple years, Congress has mandated a range of efforts and initiatives designed to expand AI infrastructure, AI adoption, and AI expertise across the Department of Defense. Despite these requirements, the rate of adoption and adaptation has not matched the scale of the challenge. The committee directs the Chief Digital and Artificial Intelligence Officer of the Department of Defense to submit a report to the House Committee on Armed Services not later than March 1, 2026, which addresses the status of the following:

(1) enterprise-wide Data Repositories for AI (Section 232 of the National Defense Authorization Act for Fiscal Year 2022, as amended by Section 212 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023);

(2) the Digital Development Infrastructure Plan & Working Group (Section 1531(d)(2)(C) of the National Defense Authorization Act for Fiscal Year 2022, as amended by Sec. 212 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023);

(3) implementation Plan for the Talent Management of Digital Expertise and Software Professionals (Section 230(b) of the National Defense Authorization Act for Fiscal Year 2020); and

(4) Artificial Intelligence Education Strategy (Section 256 of the National Defense Authorization Act for Fiscal Year 2020).

Insider Threat Detection

The committee commends the Department of Defense on implementation of efforts to mitigate risk of insider threat through the use of innovative technologies. However, the committee believes there is an ability for the Department to further reduce risk with a more comprehensive use of insider threat detection technologies. The committee directs the Department of Defense Chief Information Officer, in coordination with the Under Secretary of Defense for Intelligence and Security, to submit a report to the House Committee on Armed Services not later than July 1, 2026, that provides an analysis of the Department's use and implementation of technologies to address requirements established in Section 1086 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92). This analysis shall address advancements in technology which could further mitigate risk of insider threat and an associated cost-benefit analysis.

Legacy Technologies and the Effect on the Department of Defense

The committee recognizes that technical debt is a known challenge for the agile acquisition of both software intensive systems and networking hardware infrastructure. The committee sought to address technical debt, specifically through section 1522 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81), by requiring the Department to address the issue; however,

insufficient progress has been made to date. The committee is concerned that the Department of Defense and the military services are either unwilling or incapable of tackling the matter with the attention necessary to identify outmoded and legacy systems, plan for modernization, or establish mitigations required to reduce risk from systems' failures. Moreover, technical debt costs the Department millions of dollars and exacerbates the Department's cyber risk.

Section 1522 of Public Law 117-81 required the Secretaries of the Army, Navy, and Air Force to initiate an effort to identify legacy applications, software, and information technology within their respective Departments and eliminate any such application, software, or information technology that is no longer required.

The committee is alarmed that despite the costs, risks, and congressional mandate, the military departments appear disinterested in the issue. The committee directs the Secretary of the Army, in coordination with the Secretary of the Navy and Secretary of the Air Force, to submit a report to the congressional defense committees, not later than January 31, 2026, that describes, in detail, all efforts taken since the enactment of Public Law 117-81 which align with the direction described under section 1522 of that law. Additionally, the report shall identify those systems, applications, and technologies still in use that have been determined to be end-of-life or end-of-service, as well as a plan to either mitigate the risk of that technology's failure or replace as necessary.

Modular Open Systems Architecture for Mounted Form Factor

The committee commends the Department for progress on implementation of Modular Open Systems Architecture (MOSA) and the United States Army for progress on the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Modular Open Suite of Standards Mounted Form Factor (CMFF) procurement. The committee looks forward to the Army's commitment to a long-term resourced program to realize CMFF benefits including reduced size, weight and power of systems, increased capability integration on armored and tactical vehicles and speed of development and technology refresh.

While the committee is encouraged by this progress and the anticipated award of CMFF Block 1, the committee is concerned that the long term CMFF program will experience significant delay without establishment of program security accreditation milestones and firm delivery and fielding dates. The key to achieving program milestone deliveries is a clear CMFF security accreditation strategy for all CMMF delivery blocks.

A prohibitively complicated and unpredictable accreditation process could negatively impact levels on industry engagement and investments and lead to lack of program achievement and accountability. The committee directs the Chief Information Officer of the Department of the Army to submit a report to the House Committee on Armed Services, not later than September 30, 2026, detailing the strategy for how MOSA systems, when applied to C5ISR requirements, are not

inhibited by the Department of Defense Type 1 encryption security accreditation process. This report shall include anticipated timelines for the accreditation process of CMFF systems as well as detail to whether Type 1 encryption will be accredited at the system, subsystem, or component level.

Multi-factor Authentication Across the Department of Defense

The committee is concerned that the Department of Defense is not keeping pace with its civilian agency counterparts when it comes to preventing phishing attacks that seek to compromise authentication. In January 2022, the Office of Management and Budget issued Memorandum 22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," which mandated that all civilian agency staff, contractors, and partners use only phishing-resistant multi-factor authentication (MFA).

While civilian agencies have made great progress since the issuance of Memorandum 22-09 in adopting phishing-resistant authentication, the committee is not aware of commensurate progress in the Department of Defense. While use of the common access card (CAC) is robust, there remains numerous use cases where CAC usage is infeasible: for instance, reservists at home or servicemembers utilizing mobile devices. The committee directs the Chief Information Security Officer of the Department of Defense to provide a briefing to the House Committee on Armed Services not later than July 31, 2026, that provides information on the Department's efforts around MFA.

Navy Efforts to Reduce Telecommunications Vulnerabilities

The committee is concerned about adversarial efforts to compromise Department of Defense mobile telecommunications through the penetration of commercial telecom and wireless companies, compromised call data records, personal device tracking, SIM swap attacks, and other nefarious means. The committee is also aware that the Department of the Navy has been conducting a pilot program to reduce vulnerabilities for telecommunications devices of Navy personnel that utilize the commercial international telecommunications infrastructure in the United States Territory of Guam. The committee has previously requested information regarding the Navy's efforts, but is unsatisfied with responses to date, especially given the increase in state-sponsored cybersecurity attacks. Furthermore, the committee understands and is concerned with the broader global threat to telecommunications devices of Department of Defense personnel. The committee directs the Secretary of the Navy to provide a briefing to the House Committee on Armed Services not later than April 1, 2026, on the following:

(1) preliminary observations and lessons learned from the Navy's Guam cybersecurity pilot program;

(2) the Navy's preliminary assessment of the effectiveness of the cybersecurity technologies employed; and

(3) the Navy's views on the utility of deploying these technologies to other locations and commands.

Strengthening Defense Industrial Base Cybersecurity Resilience

The committee notes that China and other sophisticated adversaries are targeting the U.S. defense industrial base (DIB) with increasing frequency in an effort to steal sensitive data and intellectual property, disrupt supply chains, and compromise critical infrastructure. The committee is encouraged by the success of the National Security Agency (NSA) Cybersecurity Collaboration Center (CCC) in supporting the DIB through services and offerings such as Protective Domain Name Services, attack surface management, and threat intelligence collaboration. The committee expects that the CCC will pursue the expansion of such efforts, due to their value and contributions in mitigating risk. The committee directs the Director of the NSA, in coordination with Chief Information Officer of the Department of Defense, to provide a briefing to the House Committee on Armed Services, not later than March 1, 2026, on the CCC's efforts, its future plans, and current and planned resourcing.

Website Management Across the Department of Defense

Since the appointment of the Defense Media Activity (DMA) as the lead agency for the consolidation of the Department of Defense's public website management, the committee is disappointed with the slow progress made by the Department of Defense in its cost rationalization for website management. The committee continues to support the compliance and modernization effort, titled "Web Enterprise Business (WEB) NextGen", which would support the Department of Defense's efforts to comply with the 21st Century Integrated Digital Experience Act (IDEA) (Public Law 115-336). The committee directs the Assistant to the Secretary of Defense for Public Affairs, in coordination with the Department of Defense Chief Information Officer, to provide a briefing to the House Committee on Armed Services not later than April 1, 2026, on the progress of WEB NextGen.