H.R. 8800—NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2027

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

Sec. 211—Budget Review and Certification for Certain Categories of Research and Development

This section would provide the Under Secretary of Defense for Research and Engineering (USD(R&E)) budget certification authority and require the USD(R&E) to promulgate standards on adequate levels of science and technology spending by elements of the Department of Defense.

Sec. 212—Modifications to Responsibilities of the Defense Innovation Unit

This section would amend section 4127 of title 10 United States Code to require the Defense Innovation Unit (DIU) to coordinate with the military service Portfolio Acquisition Executives (PAE) to: identify priority acquisition problems and capability gaps; identify platforms, capabilities, and solutions that could fill those gaps; and facilitate transition of technologies developed by DIU to the military service PAEs.

Sec. 213—Test and Evaluation Repository and Regional Test Hubs of the Test Resource Management Center

This section would require the Test Resource Management Center to establish and maintain a central repository of test and evaluation assets throughout the United States, to include: state, local, and Federal facilities; academic facilities; non-profit facilities; and for-profit facilities that could be used by the military services, the Department of Defense, and other partners to test and evaluate weapon systems and innovative technologies more efficiently. This section would also authorize the Director of the Test Resource Management Center to establish

regional test and evaluation hubs in various geographic regions in the United States.

Sec. 214—Weapon System Platform Modernization and Cyber Hardening

This section would amend section 228 of the National Defense Authorization Act for Fiscal Year 2026 (Public Law 119-60) to expand the demonstration of near real-time monitoring capabilities by requiring at least three additional weapon platforms for participation in the demonstration. This section would also extend reporting requirements, and authorize the demonstration through September 2028. It would also direct the Secretary of Defense to evaluate and pilot the integration of these monitoring capabilities into command and control, logistics, sustainment, and maintenance systems to improve operational value.

Sec. 215—Repeal of Requirement for Secretary of Defense to Act Through a Specified Official for NATO Innovation Program

This section would remove the requirement for the Secretary of Defense to act through the Under Secretary of Defense for Research and Engineering in carrying out section 222 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118-31), which authorizes the Secretary of Defense to provide funding support to the North Atlantic Treaty Organization's Defence Innovation Accelerator for the North Atlantic initiative.

Sec. 220—Realignment of the National Strategic Research Institute to the Department of the Air Force

This section would realign the National Strategic Research Institute University Affiliated Research Center, currently sponsored by U.S. Strategic Command, to the Department of the Air Force.

Sec. 221—Prize Competitions to Support the Research and Development of Biotechnology for the Department of Defense

This section would require the Secretary of Defense to carry out a program, pursuant to section 4025 title 10, United States Code, to award prizes to support research, development, and commercialization of biotechnology capabilities. Those prize competitions would address priority areas identified by the Secretary of Defense.

Sec. 222—Pilot Program to Recognize Outstanding Achievements in Technology and Prototype Development

This section would require the Director of the Defense Innovation Unit to carry out a pilot program to award cash prizes and other types of prizes to solve

operational problems leveraging co-investment from the military service portfolio acquisition executives.

Sec. 223—Pilot Program on Forward Deployable Biomanufacturing Capabilities

This section would authorize the Under Secretary of Defense for Research and Engineering, in coordination with the Secretary of the Army, to carry out a pilot program on forward deployable biomanufacturing.

SUBTITLE C—PLANS, REPORTS, AND OTHER MATTERS

Sec. 231—Policy to Guide the Development and Acquisition of Quantum Computing Systems for the Department of Defense

This section would require the Secretary of Defense to establish a policy to use the Defense Advanced Research Projects Agency Quantum Benchmarking Initiative to inform the development or acquisition of future Department of Defense quantum computing systems.

TITLE XV—CYBERSPACE-RELATED MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE A—CYBERSECURITY

Sec. 1501—Department of Defense AI Incident and Vulnerability Reporting Program

This section would amend title 10, United States Code, and establishes a program to report, track, analyze, and remediate covered artificial intelligence incidents and vulnerabilities rising from development, testing, procurement, fielding, or operation of artificial intelligence systems within the Department of Defense.

Sec. 1502—Review and Realignment of Department of Defense Cybersecurity Responsibilities

This section would direct the Secretary of Defense to review and as needed, reorganize the Department of Defense's cybersecurity, information technology, network defense, and defensive cyber operations responsibilities to establish clear accountability, reduce duplication and fragmentation, and improve the alignment and integration of cybersecurity efforts across the Department.

SUBTITLE B—INFORMATION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE

Sec. 1511—Software Planning, Programming, Budgeting, and Execution Reform

This section would amend section 2221 of title 10 United States Code and requires the Department of Defense to revise financial management regulations to allow any of the Department's primary appropriation funds to be used flexibly across the full lifecycle of software capabilities, regardless of appropriation category.

Sec. 1512—Artificial Intelligence Model Rapid Deployment Framework

This section would direct the Chief Digital and Artificial Intelligence Officer to establish an Artificial Intelligence Model Rapid Deployment Framework to enable rapid onboarding, security, authorization, deployment, and governance of artificial intelligence (AI) systems on Department of Defense enterprise AI platforms.

Sec. 1513—Update of Policy on Autonomous and Artificial Intelligence-Enabled Systems

This section would direct the Department of Defense to update its policies governing autonomous weapon systems and artificial intelligence-enabled systems that support, recommend, or materially influence operational decisions associated with the employment of force, including through revisions to the Department of Defense Directive 3000.09. The updated policies are required to establish risk-informed requirements for approval, oversight, testing, human involvement, auditability, operational use, and rapid revalidation of such systems.

SUBTITLE C—REPORTS AND OTHER MATTERS

Sec. 1521—Roadmap for Modernization of Top Secret and Special Access Program Network Architectures

This section would direct the Department of Defense to develop and begin implementing a comprehensive roadmap to modernize Top Secret and Special Access Program network architectures, to include improvements to resilience, interoperability, and artificial intelligence computing infrastructure.

TITLE XVIII—REVITALIZATION OF THE DEFENSE INDUSTRIAL BASE

LEGISLATIVE PROVISIONS

SUBTITLE B—PROVISIONS RELATING TO DEFENSE INDUSTRIAL BASE MANUFACTURING

Sec. 1822—Inclusion of Biotechnology in Uses of the Industrial Base Fund

This section would amend section 4817g of title 10, United States Code, to include biotechnology and biomanufacturing as an eligible use of authority of the Industrial Base Fund.

BILL LANGUAGE

Subtitle B—Program Requirements, Restrictions, and Limitations

SEC. 211 [Log 84890]. BUDGET REVIEW AND CERTIFICATION FOR CERTAIN CATEGORIES OF RESEARCH AND DEVELOPMENT.

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

(1) in subsection (b)—

(A) in paragraph (4), by striking ''and'' at the end;

(B) in paragraph (5), by striking the period at the end and inserting ''; and''; and

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

''(6) in addition to the duties described in subsection (c), promulgating guidance and recommended standards on adequate levels of science and technology spending by elements of the Department of Defense with responsibilities associated with basic research, applied research, and advanced technology development (budget activities 6.1 through 6.3, respectively, as set forth in the Department of Defense Financial Management Regulation (DOD 7000.14-R), or any successor budget classification)

that could be incorporated into budget and planning guidance of the Department as appropriate.'';

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

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

''(c) BUDGET REVIEW AND CERTIFICATION.—

''(1) TRANSMITTAL.—The Secretary of Defense, acting through the Under Secretary of Defense (Comptroller), shall require the Secretaries of the military departments and the heads of the Defense Agencies with responsibilities associated with basic research, applied research, and advanced technology development (budget activities 6.1 through 6.3, respectively, as set forth in the Department of Defense Financial Management Regulation (DOD 7000.14-R), or any successor budget classification) to transmit the proposed budget for such activities for a fiscal year and for the period covered by the future-years defense program submitted to Congress under section 221 of this title for that fiscal year to the Under Secretary of Defense for Research and Engineering for review under paragraph (2) before submitting the proposed budget to the Under Secretary of Defense (Comptroller).

"(2) REPORT AND CERTIFICATION.—The Under Secretary of Defense for Research and Engineering shall review each proposed budget transmitted under paragraph (1) and, not later than January 31 of the year preceding the fiscal year for which the budget is proposed, shall submit to the Secretary of Defense a report containing the comments of the Under Secretary of Defense for Research and Engineering with respect to all such proposed budgets, together with the certification of the Under Secretary regarding whether each proposed budget is adequate.

"(3) REPORT TO CONGRESS.—Not later than 15 days after the date on which the budget of the President for each fiscal year is submitted to Congress pursuant to section 1105(a) of title 31, the Secretary of Defense shall submit to Congress a report specifying each proposed budget contained in the most-recent report submitted under paragraph (2) that the Under Secretary of Defense for Research Engineering did not certify to be adequate. The report of the Secretary shall include the following matters:

"(A) A discussion of the actions that the Secretary proposes to take, together with any recommended legislation that the Secretary con-

siders appropriate, to address the inadequacy of the proposed budgets specified in the report.

''(B) Any additional comments that the Secretary considers appropriate regarding the inadequacy of the proposed budgets.''.

SEC. 212 [Log 84931]. MODIFICATIONS TO RESPONSIBILITIES OF THE DEFENSE INNOVATION UNIT.

(a) IN GENERAL.—Section 4127(d) of title 10, United States Code, is amended—

(1) by redesignating paragraph (11) as paragraph (12); and

(2) by inserting after paragraph (10) the following new paragraph:

''(11) Coordinate with the portfolio acquisition executives of the Army, Navy, Air Force, Marine Corps, and Space Force to—

''(A) identify priority acquisition problems and capability needs and gaps;

''(B) identify platforms, capabilities, and solutions developed by entities working with the Unit that have the potential to address the priority acquisition problems and capability needs and gaps identified under subparagraph (A); and

''(C) assist such portfolio acquisition executives in establishing and carrying out programs for the acquisition of such platforms, capabilities, and solutions.''.

(b) CLARIFYING AMENDMENT TO BOOST PROGRAM.—Section 1833 of the National Defense Authorization Act for Fiscal Year 2026 (Public Law 119–60; 10

U.S.C. 3453 note) is amended by striking ''commercial'' each place it appears.

SEC. 213 [Log 84930]. TEST AND EVALUATION REPOSITORY AND REGIONAL TEST HUBS OF THE TEST RESOURCE MANAGEMENT CENTER.

(a) IN GENERAL.—Section 4173 of title 10, United States Code, is amended—

(1) in subsection (c)(1) by adding at the end the following new subparagraph:

''(G) To carry out the activities described in subsections (j) and (k).'';

(2) by redesignating subsection (j) as subection (l);

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

''(j) REPOSITORY OF TEST AND EVALUATION FACILITIES.—(1) The Director shall establish and maintain a digital repository that identifies and provides relevant information on all testing and evaluation facilities in the United States that could be made available for use by the Department of Defense and qualified partners for the testing and evaluation of weapon systems and innovative technologies.

''(2) The repository established under paragraph (1) shall—

''(A) identify all testing and evaluation facilities that meet the criteria specified in paragraph (1), including—

''(i) facilities owned or operated by the Federal Government, including—

''(I) facilities in the Major Range and Test Facility Base;

''(II) facilities not included in the Major Range and Test Facility Base; and

''(III) National Guard facilities; and

''(ii) facilities owned or operated by—

''(I) State or local governments;

''(II) academic institutions;

''(III) nonprofit organizations; or

''(IV) for-profit entities; and

''(B) with respect to each testing and evaluation facility identified in the repository, provide—

''(i) a description of the facility, including a description of the capabilities and instrumentation available at the facility;

''(ii) points of contact for scheduling range time at the facility; and

''(iii) such other information as the Director determines appropriate.

''(3) The Director shall update the repository under paragraph (1) not less frequently than annually.

''(4) The Director shall make the repository established under paragraph (1) accessible to such elements of the Department of Defense and qualified partners as the Director determines appropriate.

''(k) AUTHORITY TO ESTABLISH REGIONAL TEST AND EVALUATION HUBS.—(1) The Director may establish and maintain regional test and evaluation hubs at locations within and outside the United States for purposes of facilitating or conducting test and evaluation activities.

''(2) In the event the Director exercises the authority to establish and maintain regional test and evaluation hubs under paragraph (1), the Director shall develop a strategy and criteria for the selection of locations for such hubs, which shall include consideration of whether the geographic region served by the hub provides an environment conducive to the simulation of realistic threats and environmental conditions.''; and

(4) in subsection (l), as so redesignated—

(A) in the subsection heading, by striking ''DEFINITION'' and inserting ''DEFINITIONS'';

(B) by striking ''In this section, the term'' and inserting ''In this section:

''(1) The term''; and

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

''(2) The term 'qualified partner' means an entity that the Director determines—

''(A) is engaged in the development of capabilities for the Department of Defense, such as a contractor, academic institution, or other private sector organization; and

''(B) is qualified to conduct test and evaluation activities at a facility described in subsection (j) or a regional test and evaluation hub described in subsection (k).''.

(b) DEADLINE.—The Director of the Test Resource Management Center shall establish the repository required under section 4173(j) of title 10, United States Code (as added by subsection (a) of this section), by not later than 180 days after the date of the enactment of this Act.

SEC. 214 [Log 85244]. WEAPON SYSTEM PLATFORM MODERNIZATION AND CYBER HARDENING.

Section 228 of the National Defense Authorization Act for Fiscal Year 2026 (Public Law 119–60; 139 Stat. 786; 10 U.S.C. 4001 note) is amended—

(1) in subsection (b), by inserting after paragraph (2) the following new paragraph:

''(3) The Secretary shall, not later than two years after the date of the enactment of this Act, select not fewer than three additional weapon system platforms for participation in the demonstration.'';

(2) by redesignating subsection (c) as subsection (d), and in such subsection—

(A) in paragraph (1)—

(i) by inserting after ''2027,'' the following: ''and again on January 1, 2028, and January 1, 2029,''; and

(ii) by striking ''with respect to the demonstration conducted pursuant to subsection (a)'' and inserting ''with respect to the activities carried out under subsections (a), (b), and (c)'';

(B) in each of paragraphs (2) and (3), by striking ''The report'' and inserting ''Each report''; and

(C) in paragraph (2)—

(i) by redesignating subparagraph (B) as subparagraph (C); and

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

''(B) The results of the evaluation carried out under subsection (c)(1) and any pilot efforts carried out under subsection (c)(2).'';

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

''(c) OPERATIONAL INTEGRATION.—The Secretary of Defense shall—

''(1) evaluate opportunities to integrate data collected and analyzed from the demonstration into command and control, logistics, sustainment, and maintenance systems of the Department of Defense, prioritizing systems with the greatest operational value; and

''(2) conduct pilot efforts to integrate the monitoring capabilities included in the demonstration into the platforms included in the demonstration, as appropriate.''; and

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

"(e) DURATION OF AUTHORITY.—The authority provided under this section shall remain in effect until September 30, 2028.".

SEC. 215 [Log 85666]. REPEAL OF REQUIREMENT FOR SECRETARY OF DEFENSE TO ACT THROUGH A SPECIFIED OFFICIAL FOR NATO INNOVATION PROGRAM.

(a) REPEAL OF REQUIREMENT TO ACT THROUGH SPECIFIED OFFICIAL.—Subsections (a) and (b) of section 222 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118–31; 137 Stat. 189) are amended by striking ", acting through the Under Secretary of Defense for Research and Engineering," each place it appears.

(b) REPEAL OF EXECUTED REQUIREMENT.—Such section is further amended—

(1) by striking subsection (c); and

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

SEC. 220 [Log 85071]. REALIGNMENT OF THE NATIONAL STRATEGIC RESEARCH INSTITUTE TO THE DEPARTMENT OF THE AIR FORCE.

(a) TRANSFER OF RESPONSIBILITY.—Not later than two years after the date of the enactment this Act, the Under Secretary of Defense for Research and Engineering shall—

(1) designate the Air Force as the primary sponsor of the National Strategic Research Institute University Affiliated Research Center (referred to in this section as the ''Center''); and

(2) coordinate with the Secretary of the Air Force and the Commander of the United States Strategic Command to ensure that the Center receives the funding and other resources necessary to meet the applicable requirements of the UARC Management Plan following such designation.

(b) RESOURCING PLAN.—Not later than 90 days after the date on which the designation under subsection (a)(1) occurs, the Secretary of the Air Force shall submit to the congressional defense committees a plan for providing funding and other resources to the Center in accordance with subsection (a)(2).

(c) DEFINITIONS.—In this section:

(1) The term ''prime sponsor'' has the meaning given that term in the UARC Management Plan.

(2) The term ''UARC Management Plan'' means the publication of the Department of Defense titled ''Department of Defense University Affiliated Research Center (UARC) Management Plan'', dated July 2010 (or any successor to such plan).

SEC. 221 [Log 85277]. PRIZE COMPETITIONS TO SUPPORT THE RESEARCH AND DEVELOPMENT OF BIOTECHNOLOGY FOR THE DEPARTMENT OF DEFENSE.

(a) PROGRAM REQUIRED.—

(1) IN GENERAL.—Pursuant to the authority provided under section 4025 of title 10, United States Code, the Secretary of Defense shall carry out a program (referred to in this section as the ''Program'') to award prizes to support the research, development, and commercialization of biotechnology-based capabilities that address priority areas identified by the Secretary under subsection (b).

(2) ADDITIONAL REQUIREMENTS.—The Secretary shall—

(A) before commencing prize competitions under the Program, establish requirements for the prize competition process, including—

(i) eligibility criteria for participants consistent with paragraph (3); and

(ii) procedures for the testing, judging, and verification of submissions to the competitions; and

(B) ensure that information on the prize competitions is made available to eligible par-

ticipants, including by conducting outreach and posting such information to a publicly accessible website of the Department of Defense.

(3) ELIGIBLE PARTICIPANTS.—To be eligible for a prize award under the Program, an individual or entity shall meet the requirements described in section 24(g)(3) of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719(g)(3)).

(4) JUDGES.—In accordance with section 24(k) of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719(k)), an individual from the private sector may be appointed as a judge for a prize competition under the Program.

(5) COORDINATION.—The Secretary of Defense shall carry out the Program acting through the head of the Biotechnology Management Office of the Department of Defense and in consultation with the Secretaries of the military departments and relevant officials from laboratories of the Armed Forces and other appropriate elements of the Department of Defense.

(6) DEADLINE.—The Secretary of Defense shall commence implementation of the Program not later than one year after the date of the enactment of this Act.

(b) SELECTION OF PRIORITY AREAS.—

(1) IN GENERAL.—Before commencing prize competitions under the Program, but not later than one year after the date of the enactment of this Act, the Secretary of Defense shall identify and select specific, well-defined, and measurable priority areas of biotechnology research and development to be advanced through the award of prizes under the Program.

(2) BIOTECHNOLOGY APPLICATIONS.—In carrying out paragraph (1), the Secretary is encouraged to identify and select priority areas that support the following applications of biotechnology for defense purposes:

(A) Bioenergetics.

(B) Biobased material, including for use in existing and planned systems where such materials could provide improved performance over traditional material.

(C) Biomining, including for critical minerals.

(D) Biomanufacturing platforms and processes, including for modular or deployable systems.

(E) Biotechnology convergence with other technologies and subject areas, including artificial intelligence, advanced manufacturing, and advanced computing.

(3) PUBLIC INPUT AND OTHER CONSIDERATIONS.—In identifying and selecting priority areas under paragraph (1), the Secretary shall—

(A) solicit and consider public input; and

(B) consider—

(i) relevant existing and planned programs and activities of Department of Defense and other research and development entities of the Federal Government;

(ii) the likelihood of relevant research or development being conducted by the private sector without further support from the Federal Government;

(iii) the likelihood that investment in an area by the Department of Defense will result in improved capabilities or readiness, including by increasing supply chain resilience; and

(iv) whether such an investment would foster innovation beyond the primary goal of the proposed priority area.

SEC. 222 [Log 85552]. PILOT PROGRAM TO RECOGNIZE OUTSTANDING ACHIEVEMENTS IN TECHNOLOGY AND PROTOTYPE DEVELOPMENT.

(a) PILOT PROGRAM.—The Director of the Defense Innovation Unit (referred to in this section as the Director) shall carry out a pilot program under which the Director awards prizes, on a competitive basis, to recognize outstanding achievements in technology development and prototype development that——

(1) have the potential to address operational problems and capability gaps identified by the Secretary of Defense, the Secretaries of the military departments, and combatant commanders; or

(2) have potential for application to the performance of the military missions of the Department of Defense.

(b) FORM OF PRIZES.—Prizes awarded under this section may include—

(1) cash prizes; or

(2) the award of contracts or other agreements.

(c) INFORMATION DISSEMINATION.—The Director shall carry out activities to publicize the prize competitions carried out under this section and to solicit participation in such competitions from eligible individuals and entities.

(d) PRIZE MAXIMUM AND COINVESTMENT REQUIREMENTS.—

(1) MAXIMUM VALUE.—The value of a prize awarded under this section may not exceed $15,000,000.

(2) COINVESTMENT.—The Director may award a prize under this section without receiving approval from the Under Secretary of Defense for Research and Engineering if—

(A) the value of the prize is not more than $2,000,000; or

(B) in the case of a prize with a value exceeding $2,000,000, at least half of the funds for the portion of the prize in excess of $2,000,000 are provided by the portfolio acquisition executive of an organization of the Department of Defense outside the Defense Innovation Unit.

(e) USE OF PRIZE AUTHORITY.—Use of prize authority under this section shall be considered the use of competitive procedures for the purposes of chapter 221 of title 10, United States Code.

(f) COMMENCEMENT AND TERMINATION.—

(1) DEADLINE FOR COMMENCEMENT.—The Director shall commence implementation of the pilot program under subsection (a) not later than 90 days after the date of the enactment of this Act.

(2) TERMINATION.—The authority to carry out the pilot program under subsection (a) shall terminate on the date that is three years after the date of the enactment of this Act.

(g) CONGRESSIONAL NOTICE.—

(1) IN GENERAL.—Not later than 15 days after a contract or other agreement that exceeds a fair market value of $2,000,000 is awarded under this section, the Director shall submit to the congressional defense committees written notice of such award.

(2) CONTENTS.—Each notice submitted under paragraph (1) shall include—

(A) the value of the relevant contract or other agreement, as applicable, including all options;

(B) an identification of any portfolio acquisition executive responsible for implementation or oversight of technology development or prototype development (as applicable) for which an award was made under this section, and a brief summary of lessons learned by such portfolio acquisition executive in carrying out such implementation or oversight;

(C) a brief description of the technology development or prototype for which such contract or other agreement, as applicable, was awarded; and

(D) an explanation of the benefit to the performance of the military mission of the Department of Defense resulting from the award.

(h) PORTFOLIO ACQUISITION EXECUTIVE DEFINED.—In this section, the term ''portfolio acquisition executive'' has the meaning given that term in section 1737 of title 10, United States Code.

SEC. 223 [Log 84979]. PILOT PROGRAM ON FORWARD DEPLOYABLE BIOMANUFACTURING CAPABILITIES.

(a) AUTHORIZATION.—The Under Secretary of Defense for Research and Engineering, in coordination with the Secretary of the Army, may carry out a pilot program—

(1) to identify near-term and long-term use cases for forward deployable mobile biomanufacturing capabilities; and

(2) to conduct demonstrations of such capabilities.

(b) ACTIVITIES.—In carrying out the pilot program under subsection (a), the Under Secretary of Defense for Research and Engineering may—

(1) consider the use of novel manufacturing processes and equipment, including automation, modularity, and miniaturization of production capabilities;

(2) collaborate with industry to develop forward deployable mobile biomanufacturing capabilities; and

(3) consider the security measures required for such capabilities when forward deployed.

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

congressional defense committees a report on the status of the pilot program under subsection (a). The report shall include—

(1) an assessment of existing Department of Defense capabilities related to biomanufacturing and an explanation of whether and how those capabilities may be used as part of the pilot program;

(2) identification of near-term and long-term use cases for the deployment of mobile biomanufacturing;

(3) for each use case identified under paragraph (2), a comparison of the estimated cost of fulfilling such use case through domestic biomanufacturing at an industrial scale versus the cost of fulfilling such use case using mobile biomanufacturing at the miniaturized scale;

(4) an assessment of security measures required to deploy forward deployable mobile biomanufacturing capabilities; and

(5) an assessment of the viability of transitioning technology developed under the pilot program into operational use within the Department, including the resources needed for further development and scaling of such technology and the potential benefits of such technology.

Subtitle C—Plans, Reports, and Other Matters

SEC. 231 [Log 85075]. POLICY TO GUIDE THE DEVELOPMENT AND ACQUISITION OF QUANTUM COMPUTING SYSTEMS FOR THE DEPARTMENT OF DEFENSE.

(a) POLICY REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall issue a policy to guide the development and acquisition of quantum computing systems for the Department of Defense. Under the policy, the Secretary shall—

(1) establish a definition of ''quantum computing system'' for purposes of the policy;

(2) establish a process for validating and verifying quantum computing systems before such systems are developed or acquired by the Department; and

(3) ensure that the development and acquisition of such systems is consistent with and informed by the findings and processes of the Quantum Benchmarking Initiative of the Defense Advanced Research Projects Agency (or any successor initiative).

(b) LIMITATION AND WAIVER.—

(1) LIMITATION.—Following issuance of the policy under subsection (a), a quantum computing system may not be developed or acquired by an element of the Department of Defense unless the system has been validated and verified in accordance with such policy.

(2) WAIVER.—The Secretary of Defense may waive the limitation under paragraph (1), on a case by case basis, with respect to a specific quantum computing system. In the event the Secretary issues such a waiver, the Secretary shall provide to the congressional defense committees, not later than 15 days after date on which the waiver was issued—

(A) written notice of such waiver; and

(B) the Secretary's justification for the waiver.

Subtitle A—Cybersecurity

SEC. 1501 [Log 85241]. DEPARTMENT OF DEFENSE AI INCIDENT AND VULNERABILITY REPORTING PROGRAM.

Chapter 131 of title 10, United States Code, is amended by inserting after section 2224a the following new section:

"§ 2224b. Artificial intelligence incident and vulnerability reporting program

''(a) IN GENERAL.—The Secretary of Defense shall establish a centralized Department-wide program for the reporting, tracking, analysis, and remediation of covered AI incidents and covered AI vulnerabilities arising from the development, testing, procurement, fielding, or operation of artificial intelligence systems within the Department of Defense.

''(b) PURPOSE.—The purpose of the program established under subsection (a) shall be to—

''(1) identify recurring risks, failure modes, vulnerabilities, and systemic weaknesses in artificial intelligence systems;

''(2) support mitigation of significant risks; and

''(3) inform testing, procurement, cybersecurity, and deployment decisions to improve the safety, se-

curity, reliability, and operational effectiveness of such systems.

''(c) REQUIREMENTS FOR PROGRAM.—The program shall—

''(1) be designed using practices drawn from established safety incident reporting programs, vulnerability disclosure programs, and programs to identify and develop lessons learned;

''(2) emphasize non-punitive reporting, protection of sensitive and proprietary information, and dissemination of lessons learned, as appropriate; and

''(3) include a mechanism to enable timely access to and sharing of relevant logs, system data, and model information as necessary to support analysis and response.

''(d) DESIGNATION OF OFFICIAL.—The Secretary shall designate an appropriate official for the reporting, tracking, analysis, and remediation of covered AI incidents and covered AI vulnerabilities under this section. The Secretary, acting through such official, shall receive and standardize reports, conduct trend analysis, identify recurring risks and failure modes, and issue guidance, alerts, and recommendations, as appropriate.

''(e) REPORTING AND CATEGORIZATION.—(1) The Secretary shall require prompt reporting to the official designated under subsection (d) of—

''(A) any covered AI incident; and

''(B) any covered AI vulnerability.

''(2) The Secretary, acting through the official, shall categorize each incident or vulnerability reported to the official according to whether the incident or vulnerability requires—

''(A) a Department-wide response;

''(B) a response at the program level; or

''(C) a response at a local level.

''(f) DEPARTMENT-WIDE AND PROGRAM-LEVEL MATTERS.—(1) In the case of any incident or vulnerability categorized under subsection (e)(2)(A) or (B), the Secretary, acting through the official designated under subsection (d), shall coordinate any responses that the Secretary considers appropriate, such as remediation, retesting, mitigation measures, or deployment restrictions.

''(2) In addition, in the case of any incident or vulnerability described in subsection (e)(2)(A), the Secretary, acting through the official, shall require—

''(A) a documented corrective action plan; and

''(B) validation that the mitigation measures, if any, in such plan have been implemented before continued operational use.

''(g) PROTECTION OF REPORTS.—(1) The Secretary shall establish a protected disclosure process, informed by established vulnerability disclosure practices, through which members of the Armed Forces, civilian employees, contractors, and subcontractors at any tier may report covered AI incidents and covered AI vulnerabilities in good faith.

''(2) The Secretary shall ensure that a person making a report in good faith under paragraph (1) is not, on the basis of that report alone, subject to adverse contract action, subject to adverse personnel action, or otherwise retaliated against by the Department.

''(h) PROTECTION OF INFORMATION.—The Secretary shall establish procedures to protect sensitive, proprietary, and classified information submitted through the protected disclosure process under subsection (g).

''(i) ANNUAL REPORT.—(1) In each of years 2027 through 2031, the Secretary shall submit to the congressional defense committees an annual report on the program. The report shall include—

''(A) the number of reports made of incidents and vulnerabilities and the categorizations of such reports;

''(B) a summary of significant trends, recurring risks, systemic issues, and corrective actions taken in response; and

''(C) any recommendations for changes to testing, procurement, cybersecurity, or deployment policies relating to artificial intelligence systems.

''(2) Each report under this subsection shall be submitted in unclassified form but may include a classified annex.

''(j) DEFINITIONS.—In this section:

''(1) The term 'artificial intelligence' has the meaning given such term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

''(2) The term 'covered AI incident' means an event in which an artificial intelligence system—

''(A) causes unintended operational, safety, or security harm;

''(B) operates outside approved safety, legal, or mission guardrails;

''(C) materially degrades mission performance or reliability in a real-world or operationally representative environment; or

''(D) operates in a manner that, under reasonably foreseeable circumstances, could have resulted in significant unintended operational, safety, or security harm.

''(3) The term 'covered AI vulnerability' means an exploitable weakness, vulnerability, or systemic issue in an artificial intelligence system or related component that could materially affect mission performance, compromise system integrity, create safety risk, or result in unauthorized or unintended behavior.''.

SEC. 1502 [Log 84973]. REVIEW AND REALIGNMENT OF DEPARTMENT OF DEFENSE CYBERSECURITY RESPONSIBILITIES.

(a) REVIEW AND REALIGNMENT.—

(1) REVIEW REQUIRED.—The Secretary of Defense shall conduct a comprehensive review of the roles, responsibilities, relationships, authorities, and governance structures relating to cybersecurity, information technology, network defense, and defensive cyber operations within the Department of Defense in order to achieve the following goals:

(A) Establish clear accountability for the cybersecurity of Department of Defense information networks, including identification of one official designated as the single accountable official responsible for the cybersecurity of Department of Defense information networks.

(B) Improve the operational effectiveness, responsiveness, and unity of effort of Department-wide cybersecurity, information technology, network defense, and defensive cyber operations.

(C) Eliminate structural overlap, duplication, and fragmentation across organizations responsible for cybersecurity, information tech-

nology, network defense, and defensive cyber operations.

(D) Reduce overlapping responsibilities and ensure alignment of policy, strategy, budgetary oversight, and operational support necessary for the cybersecurity of Department of Defense information networks in an evolving threat environment.

(2) SCOPE.—The review conducted under this subsection shall include an assessment of the roles, responsibilities, relationships, and authorities among—

(A) the Chief Information Officer of the Department of Defense;

(B) the Assistant Secretary of Defense for Cyber Policy;

(C) the Principal Cyber Advisor to the Secretary of Defense;

(D) the Commander of the United States Cyber Command;

(E) the Department of Defense Cyber Defense Command; and

(F) such other offices, elements, or organizations as the Secretary determines appropriate.

(3) REALIGNMENT.—As a result of the review, and in order to achieve the goals specified in paragraph (1), the Secretary may, consistent with applicable law—

(A) realign, consolidate, or modify the roles, responsibilities, relationships, and authorities of the officials, offices, elements, and organizations specified in paragraph (2);

(B) reassign functions, personnel, and resources among such officials, offices, elements, and organizations;

(C) eliminate duplicative functions; and

(D) clarify or revise reporting relationships and lines of authority.

(b) PRESERVATION OF FUNCTIONS.—In carrying out subsection (a), the Secretary shall ensure that all functions necessary for the governance, defense, and operation of Department of Defense information networks are maintained, regardless of the organizational structure to which such functions are assigned.

(c) LIMITATION ON ESTABLISHMENT OF NEW OFFICE OR ORGANIZATION.—The Secretary may not establish a new office or organization for the purpose of carrying out this section unless the Secretary determines that such establishment is necessary to achieve the goals speci-

fied in subsection (a)(1) and consistent with applicable law.

(d) LIMITATION ON REASSIGNMENT OR ELIMINATION OF FUNCTION.—The Secretary may not reassign or eliminate a function associated with an official, office, element, or organization for the purpose of carrying out this section unless the Secretary submits to the congressional defense committees a notification of the reassignment or elimination of the function and a period of 15 days has elapsed after the date on which the notification was submitted.

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to authorize the Secretary of Defense to modify, transfer, eliminate, or otherwise alter any role, responsibility, relationship, authority, function, or any other matter expressly required by law.

(f) REPORT.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report on the results of the review conducted under subsection (a).

(2) ELEMENTS.—The report shall include—

(A) identification of the official designated as the single accountable official responsible for the cybersecurity of Department of Defense in-

formation networks, as specified in subsection (a)(1)(A);

(B) a description of any realignment, consolidation, or modification made, or to be made, to the roles, responsibilities, relationships, and authorities of the officials, offices, elements, and organizations reviewed, as specified in subsection (a)(3)(A);

(C) a description of any reassignment of functions, personnel, and resources made, or to be made, among the officials, offices, elements, and organizations reviewed, as specified in subsection (a)(3)(B);

(D) a description of any duplicative functions eliminated, or to be eliminated, as set forth in subsection (a)(3)(C);

(E) a description of any clarification or revision made, or to be made, to reporting relationships and lines of authority, as set forth in subsection (a)(3)(D);

(F) a mapping of the responsibilities and authorities assigned as of the date of the enactment of this Act to each respective official, office, element, or organization reviewed (including an identification of whether the responsi-

bility or authority is required by law to be assigned to such official, office, element, or organization, and an mapping of the responsibilities and authorities as they will be assigned after completion of the activities specified in subsection (a)(3);

(G) a timeline for implementation of the activities specified in subsection (a)(3), under which all such activities shall be implemented not later than one year after the date of the enactment of this Act;

(H) identification of any legislative recommendations, including any provisions of law requiring amendment, to fully implement the goals specified in subsection (a)(1) and the activities specified in subsection (a)(3); and

(I) a justification for the new structure, including an explanation for how the new structure better achieves the goals specified in subsection (a)(1) than the current structure.

(g) BRIEFING.—Not later than 45 days after the date of the enactment of this Act, the Secretary shall provide a briefing to the congressional defense committees on preliminary findings of the review.

Subtitle B—Information Technology and Artificial Intelligence

SEC. 1511 [Log 84971]. SOFTWARE PLANNING, PROGRAMMING, BUDGETING, AND EXECUTION REFORM.

(a) IN GENERAL.—Chapter 131 of title 10, United States Code, is amended by inserting after section 2220 the following new section:

"§ 2221. Availability of appropriations accounts for full lifecycle of software capabilities: regulations

''(a) IN GENERAL.—The Secretary of Defense shall ensure that the relevant financial management regulations of the Department provide guidance for the budgeting and execution of funds for software capabilities. Such guidance shall—

''(1) reflect that amounts appropriated for operations and maintenance, procurement, or research, development, test, and evaluation may be used at each stage in the lifecycle of a software capability, consistent with applicable law;

''(2) clarify that such amounts may be used, as appropriate, for all activities at each such stage in the lifecycle of a software capability;

''(3) provide that, for any program or activity of the Department that requires a new software capability, the appropriations account primarily available for that program or activity shall be available for that new software capability;

''(4) not impose restrictions on the availability of funds for software capabilities, except as required by law; and

''(5) maintain consistency, to the maximum extent practicable, with Recommendation 11A of the final report (dated March 2024) of the Commission on Planning, Programming, Budgeting, and Execution Reform, as submitted under section 1004 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81; 135 Stat. 1884).

''(b) DEFINITION.—In this section, the term 'lifecycle' includes stages such as development, prototyping, testing, fielding, modification, upgrading, licensing, sustainment, and retirement.''.

(b) ISSUANCE OF REVISED REGULATIONS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall issue revised regulations to implement section 2221 of title 10, United States Code, as added by this section.

(2) NOTIFICATION.—Not later than 30 days after the Secretary issues the revised regulations under paragraph (1), the Secretary shall notify the congressional defense committees of the revisions.

(c) UPDATES AND REPORT.—

(1) WRITTEN UPDATES.—Not later than 180 days after the date of the enactment of this Act, and every 90 days thereafter until the revised regulations required by subsection (b) are issued, the Secretary shall submit to the congressional defense committees a written update containing—

(A) a description of the progress made toward completing the revised regulations, along with specific actions taken and remaining milestones;

(B) the most up-to-date working draft of the revised regulations, or an outline of such working draft in sufficient detail to demonstrate the manner in which, and the extent to which, the working draft implements section 2221;

(C) a description of any anticipated barriers to full and timely issuance of the revised regulations and full and timely implementation of such regulations;

(D) any recommendations for legislation to fully implement such revised regulations; and

(E) if the Secretary has not issued such revised regulations within the period described in subsection (b), an explanation for the delay and the anticipated timeline for issuing the revised regulations.

(2) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees a report containing—

(A) the revised regulations required by subsection (b); and

(B) any remaining barriers to full and timely implementation of such revised regulations.

SEC. 1512 [Log 85276]. ARTIFICIAL INTELLIGENCE MODEL RAPID DEPLOYMENT FRAMEWORK.

(a) FRAMEWORK REQUIRED.—The Secretary of Defense, acting through the Chief Digital and Artificial Intelligence Officer of the Department of Defense, shall establish a framework for the rapid deployment of artificial intelligence (''AI''), to be known as the Artificial Intelligence Model Rapid Deployment Framework (in this section referred to as the ''Framework''), to enable the evaluation, authorization, and deployment of AI systems on Department enterprise AI platforms, as appropriate. The objective of the Framework shall be to enable deployment of such systems on such platforms within 30 days after public availability.

(b) ELEMENTS.—The Framework shall include the following elements:

(1) VENDOR AND MODEL ONBOARDING PROCESS.—Establishment of standardized processes for deploying AI systems onto Department enterprise AI platforms, including security reviews, technical assessments, and integration with other Department systems and platforms.

(2) SECURITY TESTING AND EVALUATION.—Establishment of security testing and evaluation capabilities to support security assessments for AI systems deployed on Department enterprise AI plat-

forms, including adversarial testing, supply chain risk assessments, and other security testing appropriate for AI systems, consistent with existing cybersecurity and test and evaluation policies.

(3) MULTI-CLASSIFICATION DEPLOYMENT.—Establishment of capability to deploy AI systems on Department enterprise AI platforms across multiple classification levels, as appropriate, with appropriate security controls and data isolation.

(4) STREAMLINED SYSTEM AUTHORIZATION PROCESSES.—In coordination with the Chief Information Officer of the Department, establishment of streamlined processes for authorization of AI systems deployed on Department enterprise AI platforms, including reuse of authorization artifacts, common control inheritance, and continuous monitoring capabilities.

(5) REGISTRY AND GOVERNANCE SYSTEMS.—Implementation of registry and governance processes to track version history, performance, security status, and compliance for AI systems deployed on Department enterprise AI platforms.

(c) INTEGRATION WITH OTHER FRAMEWORKS.—The Secretary shall ensure that the rapid deployment of AI systems under the Framework is achieved in a manner

that maintains security standards through integration with other relevant frameworks, including—

(1) the plans, strategies, and other matters relating to AI required by section 1544 of the National Defense Authorization Act for Fiscal Year 2024 (10 U.S.C. 4001 note);

(2) the Defense-wide policy required by section 1512 of the National Defense Authorization Act for Fiscal Year 2026 (10 U.S.C. 394 note); and

(3) the framework and other requirements required by section 1513 of the National Defense Authorization Act for Fiscal Year 2026 (10 U.S.C. 2224 note).

(d) COMPLIANCE WITH REQUIREMENTS.—The Secretary shall ensure that the Framework complies with all applicable requirements for test and evaluation of Department systems in accordance with applicable law, policy, and guidance.

(e) METRICS AND REPORTING.—The Chief Digital and Artificial Intelligence Officer shall—

(1) establish metrics to measure the time required to evaluate, authorize, deploy, and update AI systems on Department enterprise AI platforms; and

(2) in each of fiscal years 2027, 2028, 2029, and 2030, submit an annual report to the congres-

sional defense committees on progress toward achieving the objective stated in subsection (a).

(f) DEFINITION.—In this section, the term ''Department enterprise AI platform'' means a centrally managed platform that hosts or provides AI services or applications for use across multiple elements of the Department, rather than for a single program, system, or mission application.

SEC. 1513 [Log 85788]. UPDATE OF POLICY ON AUTONOMOUS AND ARTIFICIAL INTELLIGENCE-ENABLED SYSTEMS.

(a) POLICY UPDATE REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Defense shall update policies and guidance of the Department of Defense, including by revising Department of Defense Directive 3000.09 (relating to Autonomy in Weapon Systems) and establishing or revising such additional Department policies and guidance as may be appropriate, governing—

(1) autonomous and semi-autonomous weapon systems; and

(2) artificial intelligence-enabled systems intended to support, recommend, or materially influence operational decisions associated with the employment of force, including systems used for operational planning, target development, weaponeering, or engagement recommendation.

(b) REQUIRED POLICY ELEMENTS.—In updating the policies and guidance required by subsection (a), the Secretary shall ensure such policies and guidance include—

(1) criteria for categorizing systems according to such factors as mission context, autonomy, human involvement, and operational consequence;

(2) appropriate and operationally responsive requirements for approval, validation, oversight, and authorized operational use applicable to categories of systems identified pursuant to the criteria in paragraph (1);

(3) realistic and combat-effective requirements for operator intervention, override mechanisms, and operational resilience;

(4) appropriate requirements for auditability, traceability, and accountability;

(5) criteria and procedures for rapidly fielding capabilities following material changes to software, models, data, or operational context;

(6) requirements for appropriate and operationally responsive risk mitigation measures and notifications applicable to systems granted conditional or temporary operational use;

(7) requirements for operational testing, evaluation, and human training commensurate with mission risk and operational consequence; and

(8) processes and timelines for periodic review and reevaluation of approved systems and operational use cases.

(c) COMPLIANCE WITH LAW.—The Secretary shall ensure that the policies and guidance required by sub-

section (a) are consistent with applicable provisions of Federal law and applicable Department policies and regulations.

(d) CONTINUITY OF OPERATIONS.—This section does not require the Secretary to suspend or terminate any ongoing operations, activities, or programs pending completion of the updates required by subsection (a).

(e) INTERIM REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall provide a report to the congressional defense committees describing the progress of the Department toward completion of the updates required by subsection (a), including a preliminary assessment of the matters described in subsection (b).

(f) FINAL POLICY BRIEFING.—Not later than 30 days after the completion of the updates required by subsection (a), the Secretary shall provide a briefing to the congressional defense committees on—

(1) the updates completed under subsection (a);

(2) the rationale supporting the updates, including the assessment of the Secretary with respect to each matter described in subsection (b); and

(3) any recommendations for authorities, resources, or statutory changes.

(g) SEMIANNUAL REPORTS.—Not less frequently than semiannually through December 31, 2032, the Secretary of Defense shall provide a report to the congressional defense committees regarding the implementation of the updates required by subsection (a), including—

(1) systems and use cases reviewed under the updates required by subsection (a), including whether such systems and use cases were approved, restricted, suspended, or subject to additional review; and

(2) any significant acquisition, resourcing, sustainment, or programmatic impacts resulting from implementation of the udpates required by subsection (a).

Subtitle C—Reports and Other Matters

SEC. 1521 [Log 85463]. ROADMAP FOR MODERNIZATION OF TOP SECRET AND SPECIAL ACCESS PROGRAM NETWORK ARCHITECTURES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall develop and submit to the congressional defense committees, and begin implementation of, a roadmap for the modernization of Department of Defense networks that process, store, or transmit information that is classified at the level of top secret or is designated as being within a special access program.

(b) ELEMENTS.—The roadmap required under subsection (a) shall include the following elements:

(1) An assessment of the current architecture, capacity, security posture, and technical limitations of such networks, including identification of major capability gaps, cybersecurity risks, infrastructure limitations, and technical debt.

(2) Target or reference architectures for modernized environments for such networks, including enterprise-level and component-level networks, as appropriate.

(3) Milestones and timelines for transition from current environments to the target or reference architectures.

(4) Plans to improve resilience, survivability, and operations of such networks in contested, degraded, or disconnected environments.

(5) Plans to improve interoperability and data sharing across such networks and relevant mission partner environments, as appropriate.

(6) An assessment of high-performance computing and distributed computing requirements, whether locally or in cloud environments, necessary to support real-time sensor data fusion, advanced analytics, and artificial intelligence capabilities.

(7) An assessment of the extent to which such networks support the operational requirements of combatant commands, including the ability to enable integration with joint and mission partner environments.

(8) Identification of governance, roles, and responsibilities for modernization of such networks across the Department.

(9) Estimated resource requirements necessary to implement the roadmap.

(c) ANNUAL REPORT.—Not later than one year after the date of the enactment of this Act, and annually thereafter for each of the next five years, the Secretary shall submit to the congressional defense committees a report on progress in implementing the roadmap required under subsection (a).

(d) REPORT ELEMENTS.—Each report submitted under subsection (c) shall include the following:

(1) Progress made toward roadmap milestones and modernization goals.

(2) Updates to the roadmap, as appropriate.

(3) Major risks, delays, or challenges affecting implementation.

(4) Budgetary resources requested and obligated for modernization of such networks.

(5) Any recommendations that the Secretary considers appropriate for legislative or funding actions to implement the roadmap.

(e) FORM OF ROADMAP AND REPORTS.—The roadmap required by subsection (a) and the reports required by subsection (c) shall be submitted in classified form, but may include an unclassified summary.

SEC. 1822.[Log 85280]. INCLUSION OF BIOTECHNOLOGY IN USES OF THE INDUSTRIAL BASE FUND.

(a) IN GENERAL.—Section 4817(g)(1) of title 10, United States Code, as amended by section **[**18xx**]** **[***log 85238***]**, is further amended by adding at the end the following new subparagraph:

''(Q) Biotechnology and biomanufacturing.''.

(b) LIMITATION ON USE OF CERTAIN AMOUNTS.—The Secretary of Defense may not use amounts made available before the date of the enactment of this Act to carry out activities under the authority of subparagraph (Q) of section 4817(g)(1) of title 10, United States Code, as added by this section.

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

Advanced LIDAR Integration for Defense Systems

The committee notes the important research conducted by Army Research Lab (ARL) and Air Force Research Lab (AFRL) as it relates to light detection and ranging (LiDAR) technology. The committee is aware of the importance of LiDAR technology for autonomous navigation, perception in low-visibility areas, and three-dimensional mapping and reconnaissance. The committee is also aware that further integration of LiDAR technologies onto both ground and airborne platforms could provide warfighters with essential navigation and visibility capabilities.

Therefore, the committee directs the Secretary of the Air Force, in coordination with the Secretary of the Army, to provide a briefing to the House Committee on Armed Services, not later than December 1, 2026, on the integration of advanced LiDAR technologies into ground and airborne systems. The briefing should include:

(1) an overview of ongoing and planned LiDAR research, development, test, and evaluation activities;

(2) an assessment of integration into current and future ground and airborne platforms;

(3) a description of transition pathways to operational capability;

(4) an assessment of domestic industrial base capacity and supply chain vulnerabilities; and

(5) a detailed assessment of the role of the AFRL, including AFRL Rome, in supporting research, prototyping, testing, validation, and integration of advanced LiDAR technologies.

Anti-Tamper and Incursion Response Technologies

The committee is aware of the Army Research Laboratory's ongoing efforts to research and explore hardware protection and anti-tamper technologies through multimodal sensing, secure radio frequency communications, and edge computing. The committee notes the growing threat to the security of critical technologies, devices, and information and recognizes the need for rapid development and implementation of anti-tamper and intrusion response technologies for supply chain assurance.

Therefore, the committee directs the Secretary of the Army to provide a report to the congressional defense committees, not later than December 1, 2026, on the Army's current and planned efforts to support the development and deployment

of advanced hardware protection and anti-tamper technologies. At a minimum, the report should include:

(1) the timeline to resource a sustained research and development program that addresses current and future anti-tamper and protection technology gaps;

(2) the Army's operational needs relevant to such current and future threats; and

(3) a prioritization of current shortfalls in protection and anti-tamper technologies.

Expanding the Innovation Ecosystem at the United States Military Academies

The committee supports the ongoing research, development, test, and evaluation (RDT&E) efforts being undertaken by the United States Military Academies. For example, the committee is aware of the launch of the West Point Innovation Hub (WP Werx), an initiative that connects cadets from diverse disciplines with partners across the Department of Defense, industry, and academia to drive innovation and address complex challenges in a collaborative setting.

The committee notes the potential of such partnerships like WP Werx to help expand the role of the Military Academies in the Department of Defense's innovation ecosystem. Therefore, the committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Assistant Secretary of the Army for Acquisition, Logistics, and Technology, to submit a report to the House Committee on Armed Services not later than December 1, 2026, on the RDT&E and innovation efforts at the Military Academies. The report shall include:

(1) an assessment of current innovation-driven project-based learning and scholarly research efforts at the Military Academies;

(2) an assessment of the feasibility, viability, and potential impacts of expansion of such efforts across academia, industry, and the Department of Defense; and

(3) such other information as the Under Secretary deems appropriate.

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, AIR FORCE

Items of Special Interest

Anti-Jam Capability Assessment

The committee is aware of supply constraints with regard to the Common Architecture for Assured Positioning, Navigation and Timing (CAAP) Application Specific Integrated Circuit (ASIC) inventory due to the planned shutdown of the 45 nanometer ASIC process line. The committee directs the Secretary of the Air Force to submit a report to the Senate Committee on Armed Services and the House Committee on Armed Services, not later than December 31, 2026, on the current and projected status of its CAAP ASIC inventory. The report should include:

(1) the anticipated rate of consumption of the chips, by system, over the next decade in support of United States and allied requirements;

(2) any emerging additional demand, including from new systems, for the existing stock of ASICs;

(3) the available capacity and necessary timelines needed for the industrial base to manufacture a new configuration; and

(4) potential opportunities for an updated architecture, including with regard to emergent demand for affordable mass munitions.

Reusable Hypersonics Development and Transition

The committee supports the Defense Advanced Research Projects Agency (DARPA)'s development of reusable hypersonic aircraft, including efforts to produce a Next Generation Responsive Strike (NextRS) prototype aircraft and transition the platform to the Air Force for flight test and fielding. However, the committee is concerned with delays to the planned transition schedule. The committee notes that initiation of novel development activities, rather than the use of propulsion and other technologies already developed under previous and ongoing development activities, can significantly increase schedule risk.

The committee directs the Secretary of the Air Force, in coordination with the Director of DARPA, to submit a report to the House Committee on Armed Services not later than December 1, 2026, on efforts to leverage ongoing and past Air Force Research Lab activities, including those associated with or managed by DARPA, into the fielding of NextRS. The report shall include:

(1) expected timelines for NextRS transition;

(2) expected funding required to maintain the current roadmap;

(3) any funding, administrative, or technology development obstacles anticipated to cause delay or that pose significant schedule or cost risk; and

(4) such other information as the Secretary deems appropriate.

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

Items of Special Interest

Analytical Tools to Improve Department of Defense Research Security

The committee remains concerned that research conducted or sponsored by the Department of Defense is the target of ongoing efforts by multiple foreign influence groups to access sensitive research processes, data, and results. Given this concern, the committee has included several provisions in previous National Defense Authorization Acts to better secure Department-sponsored research at universities and the defense industrial base.

The committee also recognizes that existing disclosure and compliance standards in place by the Department and academia may not consistently identify the full scope of foreign influence risks associated with Department of Defense–

funded research and that modern analytical tools could assist in improving these processes. Therefore, the committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Intelligence and Security, to provide a report to the House Committee on Armed Services, not later than March 15, 2027, on how the Department could adopt a risk-based approach to strengthening research security screening and oversight across Department of Defense research activities, including consideration of appropriate analytical capabilities to improve visibility into existing and future high-risk foreign affiliations and evolving foreign influence threats over time.

Commercialization Potential of Shelf-Stable Blood

The committee supports the Defense Advanced Research Projects Agency's (DARPA) research and prototyping of shelf-stable blood through the Fieldable Solutions for Hemorrhage with bio-Artificial Resuscitation Products (FSHARP) program. Utilizing biotechnology, this technology has the potential to save warfighters' lives by enabling rapid access to blood at the front lines. 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, 2027, on the status of the shelf-stable blood program. The briefing should include:

(1) the current status of the research and prototyping efforts;

(2) efforts to commercialize the research, including identification of transition partners within the Department of Defense and broader Federal Government and industry;

(3) challenges to commercialization and a plan to address those challenges;

(4) the known and anticipated benefits of fielding shelf-stable blood, including cost savings and a quantitative assessment of warfighter lives saved; and

(5) a plan for deployment and operational fielding of the shelf-stable blood product.

Countering Biotechnology Threats from Foreign Adversaries

The committee notes the rapid advancements in biotechnology made by potential foreign adversaries, and believes that such advancements could threaten national security. The committee remains concerned that the United States may face gaps both in its ability to keep pace with its biotechnology capability development and its ability to defend against biotechnology threats from adversaries.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on current biotechnology threats. The briefing should include, at a minimum:

(1) an examination of existing gaps in biotechnology threat defense;

(2) an analysis of foreign adversaries' likely use of biotechnology capabilities against the United States; and

(3) a proposed strategy to counter biotechnology threats from foreign adversaries, including recommended interagency actions.

Defense Innovation Unit Collaboration with Service Portfolio Acquisition Executives

The committee supports the efforts of the Defense Innovation Unit (DIU) to bring commercial, dual-use technologies to the Department of Defense. The committee remains concerned, however, that gaps still exist between DIU and the military services, which inhibits the timely transition of technologies into service programs. Accordingly, the committee includes a provision elsewhere in this Act that would modify DIU's statutory authorities to enable more robust collaboration with the military service Portfolio Acquisition Executives (PAEs). The committee also directs the Director of DIU, in coordination with the service PAEs, to provide a report to the House Committee on Armed Services, not later than December 1, 2026, on efforts to formalize collaboration mechanisms between DIU and the services. The report shall include:

(1) a plan for how the services and DIU plan to formalize and standardize collaboration and transition efforts between each service and DIU, to include enabling budgetary resourcing in current and future fiscal years;

(2) a plan for service allocation of appropriate billets to DIU positions and for a standardized and consistent process for the services to assign personnel with appropriate military occupational specialties, skillsets, and technical expertise; and

(3) a description of current and planned co-funding and co-development mechanisms, including any additional required authorities.

Hypersonic Test and Evaluation Workforce Development Partnerships

The committee notes the increasing importance of hypersonic systems to the national security of the United States, and understands the rapid pace at which it must develop such capabilities. The committee remains concerned that the speed of Department of Defense test and evaluation (T&E) of hypersonic systems is not keeping pace with adversary development programs and believes that coordinated, systemic effort is required. In particular, the committee believes that sustained funding for university-based T&E workforce development is critical to building and maintaining technology advantage in hypersonics.

The committee is aware of various efforts across academic research institutions, such as the joint Hypersonics T&E Workforce Development Partnership, that leverage advanced facilities at multiple institutes of higher education to more effectively provide and coordinate testing for hypersonic systems. The committee also notes that collaboration between these institutions could accelerate U.S. capabilities in high-temperature materials, advanced manufacturing, and system-level testing.

Therefore, the committee directs the Secretary of Defense, in coordination with the Secretary of the Army and the Secretary of the Air Force, to provide a

briefing to the House Committee on Armed Services, not later than March 1, 2027, on the Department's plan for hypersonic T&E workforce development and investment. The briefing should include the following:

(1) the current funding level and scope of the Hypersonics T&E Workforce Development Partnership and other relevant partnerships across academia, including funding and other support provided by the Department of Defense;

(2) a description of current and projected gaps in the national hypersonic T&E workforce and infrastructure relative to current and projected program requirements;

(3) the Department's plan to sustain and expand university-based hypersonic T&E partnerships in fiscal year 2028 and beyond; and

(4) such other information as the Secretary deems appropriate and relevant.

Privately Funded Dual-Use Innovation Exchanges

The committee recognizes that the transition of commercially developed technologies into defense applications remains a persistent challenge for the Department of Defense. The committee is also aware that several privately funded dual-use innovation exchange organizations have been established to help facilitate collaboration between the Department of Defense and nontraditional defense contractors, manufacturing and infrastructure partners, and private capital providers. The committee encourages the Department to continue to leverage these relationships to help enable and accelerate technology transition.

Accordingly, 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 March 1, 2027, on the Department's current and planned engagement with privately funded dual-use innovation exchange organizations. The briefing shall include the following:

(1) a description of existing Department relationships with privately funded dual-use innovation exchange organizations and the supported technology areas or programs;

(2) an assessment of statutory, regulatory, or policy barriers to increased or more consistent Department engagement with these organizations; and

(3) recommendations for policy changes that would allow the Department to more effectively leverage privately funded dual-use innovation infrastructure without duplicating existing Department manufacturing, acquisition, or industrial base activities.

Protecting Defense Innovation from Adversaries

The committee remains concerned about ongoing efforts by foreign adversaries to exploit defense-relevant innovation, critical technologies, and trusted supplier networks in the United States. The committee believes that safeguarding

both academia and the defense industrial base are essential to maintaining the technological advantage of the Department of Defense.

Accordingly, the committee directs the Secretary of Defense to submit a report to the congressional defense committees not later than March 15, 2027, that assesses vulnerabilities in defense supply chains, outbound investment, and development activities that could enable adversarial exploitation. The report shall include, but not be limited to:

(1) an assessment of risks associated with foreign ownership, control, or influence within the defense industrial base and programs supporting major defense acquisition efforts;

(2) an evaluation of standards applicable to Department-funded contractors, subcontractors, and research and development institutions with foreign partnerships or investment exposure that may present national security risk; and

(3) recommendations for legislative or policy changes necessary to strengthen protections for Department-funded development activities and critical supply chains.

Ultra Short Reach Interconnect and Advanced Packaging for Defense Systems

The committee recognizes that size, weight, and power (SWaP) constraints remain critical drivers for ground, airborne, and space-based defense systems. The committee further notes that heterogeneous integration and chiplet-based architectures could offer a path to increased performance, resilience, and manufacturability without sole reliance on lower technical readiness level (TRL) semiconductor process technology nodes.

The committee is aware that Ultra Short Reach (USR) interconnect technologies may enable the Department of Defense to leverage mature-node semiconductor technologies in combination with advanced packaging to accelerate deployment timelines and reduce program cost and technical risk. The committee encourages the Department to explore investment in USR-enabled heterogeneous integration technologies, including chiplet-based architectures, as part of broader microelectronics modernization efforts. Such investments could support applications across ground, airborne, and space missions where SWaP constraints are paramount.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than January 31, 2027, on the Department's strategy to mature USR interconnect technologies and integrate them into defense-relevant advanced packaging programs, including activities conducted under the Defense Advanced Research Projects Agency's Next-Generation Microelectronics Manufacturing program.

TITLE XV—CYBERSPACE-RELATED MATTERS

ITEMS OF SPECIAL INTEREST

Accelerating Agentic Artificial Intelligence for Joint Planning and Decision Advantage

The committee supports recent Department of Defense actions to accelerate the development and integration of agentic artificial intelligence systems to improve the speed and quality of military decision-making. The committee notes the Defense Innovation Unit's establishment of Project Thunderforge designed to integrate artificial intelligence (AI) agents to assist military planning, simulation, and operational decision-making. As the military importance of agentic AI grows, the committee encourages the Department to adopt and integrate commercial software technologies, wherever possible, to improve military decision advantage and accelerate responsible human-machine teaming.

Therefore, the committee directs the Secretary of Defense to submit a report to the congressional defense committees not later than March 1, 2027, on an evaluation of Project Thunderforge, incorporating inputs from all participating Combatant Commands regarding:

(1) the overall impact of the program on the quality and speed of joint military planning;

(2) the ability to discover non-obvious strategies or constraints in plans by analyzing large volumes of simulation inputs and outputs;

(3) the ability of the program to accelerate the joint operational planning process by leveraging AI agents to manipulate simulated courses of action directly and test new strategies without manual configuration; and

(4) the proposed plan to transition Project Thunderforge out of prototyping, provide enduring funding and program management, and scale the capability across the joint force.

Competition of Autonomous Software Capabilities for Weapon Systems

The committee recognizes progress made by the Department of Defense in developing and fielding autonomous control software capabilities across a range of weapon systems. However, the committee remains concerned that the use of proprietary or tightly coupled software architectures may limit competition, reduce interoperability, and slow the adoption of improved capabilities over time.

Therefore, the committee encourages the Department to maximize competition for autonomous software capabilities to the greatest extent practicable, including through approaches that enable autonomy software to be developed, integrated, and competed separately from platform-specific hardware and software.

Accordingly, the committee directs the Under Secretary of Defense for Acquisition and Sustainment to provide a briefing to the House Committee on Armed Services not later than June 30, 2027, on the Department's plan to promote competition for autonomous software capabilities across a variety of weapon programs. The briefing shall include:

(1) a strategy for promoting competition in autonomous software capabilities, including approaches to enable autonomy software to be developed and competed independently from the underlying weapon platform;

(2) a list of candidate weapon programs for which competing autonomous software capabilities may be appropriate;

(3) a list of weapon programs for which competing autonomous software capabilities may not be appropriate, including the rationale for such determinations;

(4) the methodology for evaluating autonomy software efficacy; and

(5) the estimated impact on cost and schedule of competing autonomy software capabilities.

Defense Industrial Base Cybersecurity

The committee remains concerned by increasingly sophisticated malicious cyber activity from actors affiliated with China, including the pre-positioning of capabilities intended to disrupt critical defense infrastructure within the United States and degrade military readiness during a potential crisis or conflict. The committee notes such activity often targets the Defense Industrial Base (DIB) and frequently employs "living-off-the-land" techniques to maintain undetected persistence on these networks.

The committee is aware of the National Security Agency Cybersecurity Collaboration Center attack surface management (ASM) program, which provides DIB entities with asset discovery and vulnerability assessments to proactively prevent compromise of mission-critical systems and Department of Defense data.

The committee directs the Chief Information Officer of the Department of Defense, in coordination with the Director of the National Security Agency, to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the ASM program. The briefing shall include the following:

(1) an assessment of the program's effectiveness in reducing the DIB attack surface over the preceding fiscal year;

(2) a plan to scale ASM coverage to additional priority DIB entities; and

(3) milestones and resource requirements associated with the proposed scaling.

Department of Defense Zero Trust Implementation

The committee welcomes the Department of Defense's recent updates to its zero trust implementation strategy, which reflect a modernized approach to continuous, automated security and platform consolidation. The committee is concerned, however, that fragmented point solutions and manual processes may continue to impede the Department's progress in achieving target-level zero trust maturity. To evolve from passive visibility to automated detection and response, the Department must accelerate adoption of architectures that unify data models and enable artificial intelligence (AI)-driven security operations.

The committee urges the Department to deploy modern, scalable architectures that ensure zero trust controls are enforced continuously across the enterprise, including within Disconnected, Intermittent, and Low-Bandwidth and browser-based environments. Such architectures should reduce latency, ease network defender workload, and ensure policies can dynamically adapt to emerging threats without extensive manual reconfiguration.

The committee directs the Chief Information Officer of the Department of Defense to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the implementation of the Department's zero trust strategy. The briefing should include the following:

(1) how acquisition efforts align with AI-driven security operations; and

(2) the estimated cost savings and operational efficiencies achieved through capability consolidation and automation.

Edge-Based Artificial Intelligence and Supporting Infrastructure in Denied Environments

The committee recognizes the strategic importance of artificial intelligence (AI) capabilities that operate in communications-denied and contested environments. The committee notes that connectivity in operational environments is often constrained, including through adversary actions that target communications infrastructure. While the Department has begun advancing edge-based AI capabilities, the committee believes additional emphasis is warranted on systems capable of autonomous operation without persistent network connectivity, as well as rapid and reliable deployment of supporting infrastructure at the tactical edge. This includes the development and integration of agentic AI, automation, and infrastructure-as-code approaches. The committee further notes that such technologies may reduce deployment timelines, human error, and onsite support requirements in operational environments.

Therefore, the committee directs the Chief Digital and Artificial Intelligence Officer, in coordination with the Under Secretary of Defense for Acquisition and Sustainment, to provide a report to the congressional defense committees not later than March 31, 2027, on the Department's strategy for identifying, evaluating, and rapidly fielding edge-based AI capabilities for use in disconnected and contested environments. The report shall include:

(1) the Department's approach to identifying and prioritizing edge-based AI and supporting infrastructure technologies;

(2) how such technologies are being evaluated, including in operationally relevant environments;

(3) the extent to which automation, including infrastructure-as-code, can improve the speed, consistency, and scalability of deploying edge capabilities and reduce support requirements;

(4) a plan for integrating such capabilities into existing tactical networks and operations;

(5) barriers to adoption, including acquisition, deployment, and integration challenges; and

(6) identification of at least three commercially available edge AI platforms suitable for evaluation in operationally relevant exercises.

Enterprise and Operational Integration of Agentic Artificial Intelligence

As the Department of Defense implements its recently released Artificial Intelligence (AI) strategy to transform into an AI-first force, maintaining security and control over the Department's data and workflows is critical. Likewise, ensuring interoperability and scalability of these technologies will be imperative to keep pace with rapid technical innovation. The committee further recognizes that agentic AI systems have the potential to support a range of joint operational functions and deliver decision advantage across mission areas.

Therefore, the committee directs the Chief Digital and Artificial Intelligence Officer to provide a briefing to the House Committee on Armed Services not later than March 31, 2027, on the Department's agentic AI strategy and its operational integration. The briefing shall include:

(1) the status and initial demonstration results of the Enterprise Agents Pace-Setting Project identified in the Department’s January 2026 AI Strategy;

(2) identification of priority use cases for agentic AI, including those aligned to joint functions such as command and control, intelligence, fires, movement and maneuver, protection, information, and sustainment;

(3) an assessment of the security, scalability, cost, interoperability, and data sovereignty considerations for all cloud computing deployment options, including private, hybrid, and public cloud environments;

(4) identification of not fewer than five efforts employing agentic AI capabilities in support of joint functions, including the supported combatant command, military department, or defense agency; and

(5) identification of any barriers to rapid deployment and operational adoption, including challenges related to lifecycle management and sustainment, with recommendations for remediation.

Interoperable Multi-Cloud Solutions Across the Defense Enterprise

The committee is aware that the Department of Defense's current approach to cloud infrastructure has led to a proliferation of stove-piped systems, limiting the Department's ability to move data, integrate across systems, and operate in contested or degraded environments. The committee believes the Department’s mission is best served by an interoperable multi-cloud environment that enables flexibility, resilience, and competition while reducing dependence on any single provider.

Therefore, the committee directs the Secretary of Defense to provide a report to the congressional defense committees not later than March 1, 2027, that includes the following:

(1) a description of the Department's current multi-cloud architecture and its approach to interoperability across cloud environments;

(2) case studies of the War Data Platform and the GenAI.mil platform, including the extent to which data, applications, and artificial intelligence workloads can be moved across cloud environments without significant reengineering, along with the time, costs, and technical effort required;

(3) a summary of security challenges regarding multi-cloud implementation, including issues related to reciprocity of authorizations to operate and differences in security controls and authorization timelines across cloud environments;

(4) a description of barriers to interoperability and data portability, including licensing, propriety services, data formats, and application dependencies; and

(5) a description of the technical, acquisition, governance, and policy changes necessary to transition to a vendor-agnostic multi-cloud architecture.

Open-Source Software Supply Chain Security

The committee recognizes that modern software applications used throughout the Department of Defense rely extensively on open-source software (OSS) components developed and maintained by globally distributed contributors. While OSS provides significant innovation and cost advantages, the committee is concerned that the Department lacks sufficient visibility into the origins, maintenance, and security of OSS applications and software dependencies. The committee notes that some Department organizations, such as the Space Development Agency, have begun efforts to improve OSS supply chain visibility and risk mitigation, but believes a coordinated Department-wide strategy is required to scale secure OSS supply chain practices.

Therefore, the committee directs the Department of Defense Chief Information Officer, in consultation with the Chief Information Officers of the military departments, to provide a report to the congressional defense committees not later than December 1, 2026, containing a plan to scale secure OSS supply chain practices across the Department of Defense. The report shall include:

(1) an assessment of current Department-wide visibility into OSS components and software dependencies used in Department systems, including identification of adversarial foreign ownership, control, or influence;

(2) a plan to improve traceability, risk identification, and mitigation within OSS supply chains;

(3) recommendations for policies, standards, and acquisition requirements necessary to ensure secure use and maintenance of OSS components;

(4) identification of implementation pathways and the capabilities required to scale secure OSS supply chain practices across the Department; and

(5) an estimate of resources required to execute this plan.

Phased Implementation of Operational Technology Cybersecurity

The committee notes that the Department of Defense does not expect to achieve "target level" zero trust for operational technology (OT) systems until fiscal year 2030 and finds that this timeline creates unacceptable risk to mission readiness given the threats to Defense Critical Infrastructure. The committee is further concerned that current implementation approaches do not sufficiently prioritize foundational capabilities needed to reduce near-term risk and enable progress toward zero trust outcomes.

Therefore, the committee directs the Chief Information Officer of the Department of Defense to submit a report to the congressional defense committees not later than March 1, 2027, on a phased and operationally sustainable approach to improving OT cybersecurity across the Department. The report shall include:

(1) a prioritized implementation framework for OT cybersecurity, aligned to the Department's zero trust framework, that breaks "target level" zero trust outcomes into sequenced increments with defined objectives, timelines, and metrics;

(2) a plan to achieve enterprise-wide visibility into OT assets and network communications, including system dependencies and external connections;

(3) a plan to implement foundational cybersecurity practices across OT environments, including configuration management, risk-informed patching, passive monitoring, and other measures necessary to reduce risk; and

(4) an assessment of the feasibility of accelerating OT cybersecurity measures for Tier 1 Mission Assurance installations to not later than fiscal year 2028, including associated resource requirements and barriers to implementation.

Real-time Audit Capabilities Using Software and Artificial Intelligence

The committee recognizes the Department of Defense's growing adoption of advanced software and artificial intelligence capabilities across operational and administrative functions. The committee notes that the Department of the Navy, in particular, has demonstrated successful implementation of digital tools for shipbuilding, logistics, and program management.

The committee believes these technological capabilities present a significant opportunity to transform the Department of Defense's financial management and auditability. Despite years of effort and billions of dollars invested, the Department of Defense has yet to achieve a clean financial audit, and traditional periodic audit approaches have proven insufficient to address the scale and complexity of defense financial operations. The committee believes that continuous transaction validation and asset tracking to improve financial visibility may provide a more effective path toward achieving a clean audit.

Therefore, the committee directs the Secretary of Defense to provide a report to the congressional defense committees not later than December 1, 2026, on plans to implement real-time audit capabilities using software and artificial intelligence technologies. The report shall include:

(1) an assessment of existing software and artificial intelligence platforms that could be expanded to support continuous financial monitoring and auditability;

(2) a roadmap for implementing real-time audit capabilities to enable continuous transaction validation and asset tracking;

(3) identification of integration requirements necessary to provide enterprise-wide financial visibility across Department financial systems;

(4) an assessment of how real-time audit capabilities could improve financial decision-making, fraud detection, and waste reduction; and

(5) identification of any policy, regulatory, or contractual barriers that may impede implementation of real-time audit capabilities.

Resilient Command, Control, and Communications for Taiwan

The committee recognizes that resilient communications between the United States and Taiwan are essential to support effective coordination during both steady-state operations and crisis scenarios. The committee is concerned that disruption or degradation of communications infrastructure in a contested environment could significantly limit Taiwan's ability to communicate with United States forces and partners. The committee believes it is necessary to assess current capabilities and address gaps now to ensure continuity of communications under stressed conditions.

Therefore, the committee directs the Secretary of Defense to provide a report to the congressional defense committees not later than March 1, 2027, assessing the extent to which mobile ad hoc networking and commercially derived communications systems in Taiwan support United States operational requirements in contested or degraded environments. The report shall include:

(1) key Taiwan communications networks across civil and military organizations necessary to support United States and coalition operations;

(2) connectivity and integration of Department of Defense systems with such networks;

(3) gaps in Taiwan's ability to communicate with United States forces under contested conditions;

(4) network architectures enabling resilient, infrastructure-independent communications, including secure, segmented data transmission;

(5) opportunities to rapidly field and scale solutions, including through the use of existing equipment;

(6) cybersecurity and supply chain risks affecting such communications; and

(7) prioritized potential actions to improve resilient and interoperable communications, including continued progress on coalition information sharing.