# H.R. 2670—NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2024

# SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION

# SUMMARY OF BILL LANGUAGE

# Table Of Contents

# DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

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

### LEGISLATIVE PROVISIONS

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

##### Section 212—Clarification of Role of Partnership Intermediaries to Promote Defense Research and Education

This section would amend section 4124(f)(2) of title 10, United States Code, to clarify the scope of Partnership Intermediary Agreements to ensure that Partnership Intermediaries can continue to assist the defense laboratories with "spin-in" technology in addition to "spin-out" technology.

##### Section 218—Pilot Program on Near-Term Quantum Computing Applications

This section would establish a near-term quantum computing applications pilot program within the Department of Defense, in coordination with a federally funded research and development Center (FFRDC) and the quantum industry.

This section would require an interim briefing not later than March 1, 2024, on the selection of an FFRDC and the methodology and plan for establishing this pilot program as well as annual reports thereafter on the status of the pilot program, problem sets explored, and an analysis of the findings of pilot program engagements.

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

##### Section 242—Intellectual Property Strategy

This section would create a Department of Defense Intellectual Property Strategy to better secure the United States' technological edge, encourage the development of patentable inventions, and thwart adversarial behavior to undermine the U.S. technological base by utilizing intellectual property rights.

##### Section 243—Study on Establishment of Centralized Platform for Development and Testing of Autonomy Software

This section would task the Secretary of Defense, in coordination with the Chief Digital and Artificial Intelligence Officer, to assess the establishment of a centralized platform for all-domain autonomy software development and testing.

Section 244—Annual Report on Incremental and Transformational Research and Development

This section would require the Under Secretary of Defense for Research and Engineering to compile a report on the percentage of their budget spent on projects expected to make an impact for the warfighter in the next 5 years and on projects expected to make an impact beyond the initial 5-year window.

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

## LEGISLATIVE PROVISIONS

### SUBTITLE E—SMALL BUSINESS MATTERS

Section 842—Extension and Modification of Domestic Investment Pilot Program

This section would amend section 884 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92) and extend the domestic investment pilot program under the Small Business Innovation Research program until September 30, 2027. The pilot program will be required to comply with the due diligence program required under subsection (vv) of the Small Business Act (15 U.S.C. 638(vv)).

# TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

## LEGISLATIVE PROVISIONS

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

Section 901—Under Secretary of Defense for Technology Integration and Innovation

This section would rename the Under Secretary of Defense for Research and Engineering to the Under Secretary of Defense for Technology Integration and Innovation. It would expand the responsibilities for the position.

### SUBTITLE B—OTHER DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT MATTERS

Section 911—Organization and Management of the Defense Innovation Unit

This section would elevate the Defense Innovation Unit (DIU) from the Office of the Under Secretary of Defense for Research and Engineering to the Office

of the Secretary of Defense. It would require a resource and staffing assessment of the DIU.

# TITLE X—GENERAL PROVISIONS

## LEGISLATIVE PROVISIONS

### SUBTITLE D—MISCELLANEOUS AUTHORITIES AND LIMITATIONS

#### Section 1041—Modification to Definitions of Confucius Institute

This section would update the definition of a "Confucius Institute."

# TITLE XV—CYBERSPACE-RELATED MATTERS

## LEGISLATIVE PROVISIONS

### SUBTITLE A—CYBER MATTERS

#### Section 1502—Office for Academic Engagement Relating to Cyber Activities

This section would require the Secretary of Defense to establish a central program office, under the authority of the Chief Information Officer of the Department of Defense, to establish, maintain, and oversee the activities of the Department of Defense in its relationship with academia, to include those entities involved in primary, secondary, and post-secondary education.

### SUBTITLE B—PERSONNEL

#### Section 1521—Authority to Accept Voluntary and Uncompensated Services from Cybersecurity Experts

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

# BILL LANGUAGE

**SEC. 212 [Log 77774]. CLARIFICATION OF ROLE OF PARTNERSHIP INTERMEDIARIES TO PROMOTE DEFENSE RESEARCH AND EDUCATION.**

Section 4124(f)(2) of title 10, United States Code, is amended—

(1) by striking ''that assists'' and inserting ''that—

''(A) assists'';

(2) by striking the period at the end and inserting ''; and''; and

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

''(B) facilitates technology transfer from industry or academic institutions to a Center.''.

**SEC. 218 [Log 77375]. PILOT PROGRAM ON NEAR-TERM QUANTUM COMPUTING APPLICATIONS.**

(a) PILOT PROGRAM.—The Secretary of Defense shall carry out a pilot program under which the Secretary, in partnership with the entities specified in subsection (b), establishes and operates a program that enables organizations of the Department of Defense, including the Armed Forces, to test and evaluate how quantum and quantum-hybrid applications may be used—

(1) to solve technical problems and research challenges identified under section 234(e) of the John S. McCain National Defense Authorization Act for Fiscal year 2019 (Public Law 115–232; 10 U.S.C. 4001 note) and such other near-term technical problems and challenges facing the Department and the Armed Forces as the Secretary may identify; and

(2) to provide capabilities needed by the Department and the Armed Forces in the near-term.

(b) ENTITIES SPECIFIED.—The Secretary of Defense shall seek to carry out the pilot program under subsection (a) in partnership with—

(1) a federally funded research and development center; and

(2) one or more private-sector entities with expertise in quantum computing and quantum information science.

(c) ACTIVITIES.—Under the pilot program, the Secretary of Defense, in partnership with the entities specified in subsection (b), shall—

(1) convene a group of experts and organizations to identify challenges faced by the Department of Defense, including the Armed forces, that have the potential to be addressed by quantum and quantum-hybrid applications;

(2) develop and deploy demonstrations, proofs of concept, pilot programs, and other measures to address the challenges identified under paragraph (1) using quantum and quantum-hybrid applications;

(3) ensure that any quantum or quantum-hybrid application based solutions identified under the program are capable of development and deployment in 24 months or less;

(4) assess and utility of commercial quantum and quantum-hybrid applications for meeting the near-term needs of warfighters; and

(5) seek to build and strengthen relationships between the Department of Defense and nontraditional defense contractors (as defined in section

3014 of title 10, United States Code) in the technology industry that may have unused or underused solutions to specific operational challenges of the Department relating to quantum and quantum-hybrid applications.

(d) BRIEFING AND REPORTS.—

(1) INTERIM BRIEFING.—Not later than March 1, 2024, the Secretary of Defense shall provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing that—

(A) identifies the federally funded research and development center and any private-sector entities the Secretary has partnered with for purposes of carrying out the pilot program under subsection (a); and

(B) describe the plan of the Secretary for developing and operating the program.

(2) ANNUAL REPORT.—On an annual basis during each year in which the pilot program under subsection (a) is carried out, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report that includes—

(A) a description of the problem sets and capabilities that were evaluated by organiza-

tions of the Department of Defense under the program;

(B) an explanation of whether and to what extent the program resulted in the identification of potential solutions based on quantum and quantum-hybrid applications;

(C) any potential barriers to the use of quantum and quantum-hybrid applications to solve near-term problems for the Department of Defense, including the Armed Forces; and

(D) recommendations regarding how the Department of Defense can better leverage and deploy quantum and quantum-hybrid applications to address near-term military applications and operational needs.

(e) DEADLINE FOR COMMENCEMENT.—The Secretary of Defense shall commence the pilot program under this section not later than March 1, 2024.

(f) 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) DEFINITIONS.—In this section:

(1) The term ''near-term'' means a period of 24 months or less.

(2) The term ''quantum and quantum-hybrid applications'' means algorithms and applications which use quantum mechanics through quantum processing units, including—

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

(B) annealing and gate systems; and

(C) all qubit modalities (including superconducting, trap ion, and photonics).

**SEC. 242 [Log 77778]. INTELLECTUAL PROPERTY STRATEGY.**

(a) STRATEGY.—The Secretary of Defense, in coordination with the Under Secretary of Defense for Research and Engineering, shall develop and implement an intellectual property strategy to enhance the ability of the Department of Defense to procure emerging capabilities and technologies as described in subsection (b).

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

(1) Plans for using intellectual property to enhance the ability of the Department of Defense to innovate and invest in new warfighting capabilities to outpace adversaries of the United States in the areas of new and emerging technology.

(2) Recommendations on the use of intellectual property and its purpose and benefits—

(A) within research and engineering programs of the Department; and

(B) in the context of strategic competition, including in hybrid warfare and deterrence.

(3) Strategies for promoting and encouraging members of the Armed Forces to create and produce new tools and technologies for the Department.

(4) Concepts and actionable steps for accelerating, to the extent practicable, the procurement

and fielding of emerging capabilities and technologies.

(5) Methods for encouraging innovation, solutions that scale, and the use of patents across the Department of Defense by establishing an integrated, cross-service approach to the identification, prioritization, development, and fielding of emerging capabilities and technologies.

(6) Steps to implement measures to protect against the theft of intellectual property.

(7) Enforcement mechanisms to ensure intellectual property rights are protected.

(c) OPTIONAL ELEMENTS.—The strategy under subsection (a) may include the following:

(1) Identification of how intellectual property may be used to enhance the innovation capabilities of the Department of Defense to neutralize the effects of intellectual property theft by competitors of the United States.

(2) An innovation warfare strategy to promote the creation of new and emerging technologies to secure the dominant economic and security position of the United States against adversaries, which may include strategies to—

(A) further develop the technological base of the Department of Defense and create intellectual property security tools needed to outpace adversaries and prevent technological overmatch;

(B) develop machine learning tools to identify possible future technologies;

(C) ensure that Federal research and development spending spur innovation as directed in the 2022 National Defense Strategy;

(D) secure positions that give the United States strategic advantages with respect to the acquisition, procurement, distribution, and protection of new and emerging technologies; and

(E) identity and develop cross-functional capabilities—

(i) for the implementation of the strategy under subsection (a); and

(ii) to facilitate the coordination of efforts to the extent feasible.

(3) Guidance to link priorities, goals, and investments with respect to intellectual property rights with individuals and entities that are critical to the functioning of specific programs of the Department of Defense, including by—

(A) developing and reinforcing relationships with academia, the acquisition workforce (as defined in section 101 of title 10, United States Code), the defense industry, and the commercial sector to create scalable solutions that are protected through intellectual property rights;

(B) developing a marketing strategy to make members of a covered Armed Force aware that the members may be able to patent inventions the members create while serving; and

(C) identifying funding, investments, personnel, facilities, and relationships with other departments and agencies of the Federal Government without which defense capabilities would be severely degraded.

(4) Methods to support the coordination of acquisition priorities, programs, and timelines to meet requirements and security objectives of each covered Armed Force and the combatant commands with the research and engineering activities of the Department.

(5) Recommendations for changes to statute, regulations, or policies to support the achievement of the goals set forth in the strategy.

(6) Processes to inform senior leaders of the Department and Members of Congress of the potential effects of the intellectual property strategy on the development of policies and regulations guiding strategic competition with adversaries of the United States in the military and technology domains.

(7) Methods to support the efficient implementation of the strategy to address near-term, mid-term, and long-term capability gaps, with an emphasis on spurring innovation and overcoming, to the extent practicable, the gap between the research and development of emerging capabilities and technologies and the procurement and fielding of such capabilities and technologies.

(8) Methods to support the issuance and enforcement of patents within the Department of Defense.

(9) An assessment the potential supporting roles of military education institutions and science and technology reinvention laboratories (as designated under section 4121(b) of title 10, United States Code), including roles relating to encouraging innovation, raising awareness of intellectual property rights , and the conceptualization, development, test-

ing, and implementation of innovative solutions for emerging capabilities and technologies.

(d) ALIGNMENT WITH NATIONAL DEFENSE STRATEGY.—The Secretary of Defense shall ensure that the strategy developed under subsection (a) aligns with the National Defense Strategy under section 113(g) of title 10, United States Code.

(e) REPORT.—Not later than February 1, 2024, the Secretary of Defense, in coordination with the Under Secretary of Defense for Research and Engineering, shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the intellectual property strategy developed under subsection (a).

(f) DEFINITIONS.—In this section:

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

(2) The term ''intellectual property'' has the meaning given the term ''IP'' in Department of Defense Instruction 5010.44 titled ''Intellectual Property (IP) Acquisition and Licensing'' (issued October 16, 2019).

(3) The term ''intellectual property rights'' has the meaning given the term ''IP rights'' in Department of Defense Instruction 5010.44 titled ''Intellec-

tual Property (IP) Acquisition and Licensing'' (issued October 16, 2019).

**SEC. 243 [Log 77776]. STUDY ON ESTABLISHMENT OF CENTRALIZED PLATFORM FOR DEVELOPMENT AND TESTING OF AUTONOMY SOFTWARE.**

(a) STUDY REQUIRED.—The Secretary of Defense, in coordination with the Chief Digital and Artificial Intelligence Officer, shall conduct a study to assess the feasibility and advisability of establishing a centralized platform for the development and testing of autonomy software.

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

(1) An assessment of the status of efforts to resource and integrate autonomy software into systems of the Department of Defense, including systems in use by the Department as of the date of the study and systems that may be used in the future.

(2) Identification of systems of the Department of Defense which are, or can be, integrated with autonomy software to enable the continuous operational capability of such systems in GPS- or communications-denied environments, including those systems identified in the report required under section 246 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2022 (Public Law 116–283; 135 Stat. 1622).

(3) An assessment of any gaps in—

(A) program funding relating to the acquisition of autonomy software;

(B) acquisition processes, including the planning, programming, budgeting, and execution process for acquiring and integrating autonomy-enabling capabilities across relevant programs of record;

(C) training capabilities relating to autonomy software;

(D) capabilities for testing, evaluating, verifying, and validating autonomy software in all environments, including virtual and real-world environments; and

(E) efforts to test, resource, and scale commercially available autonomy software for use by the Department.

(4) A plan to address, to the extent practicable, the gaps assessed in paragraph (3), including—

(A) updated procedures to plan for the potential costs of autonomy software at the onset of the acquisition life cycle;

(B) plans to include, in greater detail, the projected costs of autonomy software for applicable programs of record in the future-years de-

fense program submitted to Congress under section 221 of title 10, United States Code; and

(C) plans to standardize the acquisition of autonomy software for programs of record across the Armed Forces.

(c) SUBMITTAL TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the results of the study conducted under subsection (a).

(d) CDAO DEFINED.—In this section, the term ''Chief Digital and Artificial Intelligence Officer'' has the meaning given that term in section 846(b) of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263).

**SEC. 244 [Log 77676]. ANNUAL REPORT ON INCREMENTAL AND TRANSFORMATIONAL RESEARCH AND DEVELOPMENT.**

(a) IN GENERAL.—Not later than 10 days after the date on which the budget of the President is submitted to Congress pursuant to section 1105 of title 31, United States Code, for each of fiscal years 2025 through 2029, the Under Secretary of Defense for Research and Engineering shall submit to the congressional defense committees a report that identifies—

(1) the number of incremental research and development projects that are in progress within the Department of Defense as of the date of the report and the total amount of funding allocated to such projects; and

(2) the number of transformational research and development projects that are in progress within the Department of Defense as of the date of the report and the total amount of funding allocated to such projects.

(b) DEFINITIONS.—In this section:

(1) The term ''incremental research and development project'' means a covered research activity that is in the research and development phase as of the date of the submittal of the report under subsection (a) and that is expected to achieve initial

operational capability by not later than five years after such date.

(2) The term ''transformational research and development project'' means a covered research activity that is in the research and development phase as of the date of the submittal of the report under subsection (a) and that is expected to achieve initial operational capability by not earlier than five years after such date.

(3) The term ''covered research activity'' means a program, project, or other activity of the Department of Defense designated as budget activity 1 (basic research), budget activity 2 (applied research), or budget activity 3 (advanced technology development), as such budget activity classifications are set forth in volume 2B, chapter 5 of the Department of Defense Financial Management Regulation (DOD 7000.14-R).

**SEC. 842.[Log 77373]. EXTENSION AND MODIFICATION OF DOMESTIC INVESTMENT PILOT PROGRAM.**

Section 884 of the National Defense Authorization Act for Fiscal Year 2020 (15 U.S.C. 638 note) is amended—

(1) in subsection (a), by striking ''Not later than 1 year after the date of the enactment of this Act'' and inserting ''Not later than October 1, 2023'';

(2) in subsection (c)—

(A) by striking ''Secretary of Defense may not use'' and inserting the following: ''Secretary of Defense—

''(1) may not use'';

(B) in paragraph (1), as so designated, by striking ''STTR program.'' and inserting ''STTR program; and''; and

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

''(2) shall ensure that such program complies with the requirements of a due diligence program established under subsection (vv) of the Small Business Act (15 U.S.C. 638(vv)).''; and

(3) in subsection (f), by striking ''September 30, 2022'' and inserting ''September 30, 2027''.

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

**SEC. 901 [Log 77614]. UNDER SECRETARY OF DEFENSE FOR TECHNOLOGY INTEGRATION AND INNOVATION.**

(a) IN GENERAL.—Section 133a of title 10, United States Code, is amended to read as follows:

**"§ 133a. Under Secretary of Defense for Technology Integration and Innovation**

''(a) UNDER SECRETARY OF DEFENSE.—There is an Under Secretary of Defense for Technology Integration and Innovation, appointed from civilian life by the President, by and with the advice and consent of the Senate. A person may not be appointed as Under Secretary within seven years after relief from active duty as a commissioned officer of a regular component of an armed force.

''(b) QUALIFICATIONS.—The Under Secretary shall be appointed from among persons who have an extensive technology or science background and experience in—

''(1) private or venture capital, commercial innovation, or prototype-to-production transition; and

''(2) managing complex programs and leveraging public-private capital partnerships.

''(c) DUTIES AND POWERS.—Subject to the authority, direction, and control of the Secretary of Defense, the

Under Secretary shall perform such duties and exercise such powers as the Secretary may prescribe, including—

''(1) serving as the chief technology officer of the Department of Defense with the mission of advancing technology, innovation, and the integration of commercial technology for the armed forces (and the Department);

''(2) establishing policies on, and supervising, all elements of the Department relating to the identification of commercial technology for potential use by the Department and integration of such technology into the armed forces (and the Department), including—

''(A) implementing the preference under section 3453 of this title for the use of commercial technology when suitable to meet the needs of Department; and

''(B) ensuring implementation of a modular open system approach (as defined in section 4401(b) of title 10, United States Code) to encourage increased competition and the more frequent use of commercial technology within the Department;

''(3) establishing policies on, and supervising, all defense research and engineering, technology de-

velopment, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities and programs and unifying defense research and engineering efforts across the Department;

''(4) serving as the principal advisor to the Secretary on all commercial innovation and integration, research, engineering, and technology development activities and programs in the Department; and

''(5) along with the Vice Chairman of the Joint Chiefs of Staff, providing for an alternate path to integrate commercial technology into the Department that does not include applying the Joint Capabilities Integration and Development System process to the acquisition of technology that readily exists in the commercial sector.

''(d) PRECEDENCE IN DEPARTMENT OF DEFENSE.—

''(1) PRECEDENCE IN MATTERS OF RESPONSIBILITY.—With regard to all matters for which the Under Secretary has responsibility by the direction of the Secretary of Defense or by law, the Under Secretary takes precedence in the Department of Defense after the Secretary and the Deputy Secretary of Defense.

''(2) PRECEDENCE IN OTHER MATTERS.—With regard to all matters other than the matters for which the Under Secretary has responsibility by the direction of the Secretary or by law, the Under Secretary takes precedence in the Department of Defense after the Secretary and the Deputy Secretary of Defense.''.

(b) CONFORMING AMENDMENTS.—

(1) TITLE 10.—Title 10, United States Code, as amended by subsection (a), is further amended by striking ''Under Secretary of Defense for Research and Engineering'' each place it appears and inserting ''Under Secretary of Defense for Technology Integration and Innovation''.

(2) TITLE 5.—Title 5, United States Code, is amended by striking ''Under Secretary of Defense for Research and Engineering'' each place it appears and inserting ''Under Secretary of Defense for Technology Integration and Innovation''.

(3) NATIONAL DEFENSE AUTHORIZATION ACTS.—Each of the following Acts is amended by striking ''Under Secretary of Defense for Research and Engineering'' each place it appears and inserting ''Under Secretary of Defense for Technology Integration and Innovation'':

(A) The National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91).

(B) The John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232).

(C) The National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92).

(D) The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283).

(E) The National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81).

(F) The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263).

(c) REFERENCES.—Any reference in any law (other than this section), regulation, map, document, paper, or other record of the United States to the Under Secretary of Defense for Research and Engineering shall be deemed to be a reference to the Under Secretary of Defense for Technology Integration and Innovation.

(d) SERVICE OF INCUMBENT IN POSITION.—The individual serving as Under Secretary of Defense for Research and Engineering as of the effective date specified in subsection (e) may serve as Under Secretary of Defense

for Technology Integration and Innovation commencing as of that date without further appointment under section 133a of title 10, United States Code (as amended by subsection (a)).

(e) EFFECTIVE DATE.—This section and the amendments made by this section shall take effect one year after the date of the enactment of this Act.

# Subtitle B—Other Department of Defense Organization and Management Matters

**SEC. 911 [Log 77410]. ORGANIZATION AND MANAGEMENT OF THE DEFENSE INNOVATION UNIT.**

(a) ORGANIZATION AND MANAGEMENT.—

(1) DIRECT REPORT TO SECRETARY OF DEFENSE.—Chapter 303 of title 10, United States Code, is amended by adding at the end the following new section:

**"§ 4127. Organization and management of the Defense Innovation Unit**

''The Director of the Defense Innovation Unit shall report directly to the Secretary of Defense without intervening authority and may communicate views on matters within the responsibility of the Unit directly to the Secretary without obtaining the approval or concurrence of any other official within the Department of Defense.''.

(2) CONFORMING AMENDMENTS.—Section 1766 of title 10, United States Code, is amended—

(A) in subsection (b), by striking ''as determined by the Under Secretary of Defense for Research and Engineering'' and inserting ''as determined by the Secretary of Defense''; and

(B) in subsection (c)(3), by striking ''as directed by the Under Secretary of Defense for Research and Engineering'' and inserting ''as directed by the Secretary of Defense''.

(3) EFFECTIVE DATE AND IMPLEMENTATION.—

(A) EFFECTIVE DATE.—The amendments made by paragraphs (1) and (2) shall take effect 180 days after the date of the enactment of this Act.

(B) IMPLEMENTATION.—Not later than the effective date specified in subparagraph (A), the Secretary of Defense shall issue or modify any rules, regulations, policies, or other guidance necessary to implement section 4127 of title 10, United States Code (as added by paragraph (1)).

(b) MANPOWER SUFFICIENCY EVALUATION.—

(1) EVALUATION.—The Secretary of Defense shall evaluate the staffing levels of the Defense Innovation Unit to determine if the Unit is sufficiently staffed to achieve its objectives.

(2) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representa-

tives a report on the results of the evaluation under paragraph (1). The report shall include a plan—

(A) to address any staffing shortfalls identified as a part of the assessment; and

(B) for funding any activities necessary to address such shortfalls.

# Subtitle D—Miscellaneous Authorities and Limitations

**SEC. 1041 [Log 77615]. MODIFICATION TO DEFINITIONS OF CONFUCIUS INSTITUTE.**

(a) LIMITATION ON PROVISION OF FUNDS TO INSTITUTIONS OF HIGHER EDUCATION.—Paragraph (1) of section 1062(d) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 10 U.S.C. 2241) is amended to read as follows:

''(1) CONFUCIUS INSTITUTE.—The term 'Confucius Institute' means—

''(A) any program that receives funding from or has any operational ties to—

''(i) the Chinese International Education Foundation; or

''(ii) the Center for Language Exchange Cooperation of the Ministry of Education of the People's Republic of China; or

''(B) any cultural institute directly or indirectly funded by the Government of the People's Republic of China.''.

(b) PROHIBITION OF FUNDS FOR CHINESE LANGUAGE INSTRUCTION.—Paragraph (2) of section 1091(d)

of the of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1998) is amended to read as follows:

"(2) CONFUCIUS INSTITUTE.—The term 'Confucius Institute' means—

"(A) any program that receives funding from or has any operational ties to—

"(i) the Chinese International Education Foundation; or

"(ii) the Center for Language Exchange Cooperation of the Ministry of Education of the People's Republic of China; or

"(B) any cultural institute directly or indirectly funded by the Government of the People's Republic of China.".

**SEC. 1502 [Log 78038]. OFFICE FOR ACADEMIC ENGAGEMENT RELATING TO CYBER ACTIVITIES.**

(a) ESTABLISHMENT.—Chapter 111 of title 10, United States Code, is amended by inserting after section 2192b the following new section:

**"§ 2192c. Office for academic engagement relating to cyber activities**

''(a) ESTABLISHMENT.—The Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, shall establish an office to establish, maintain, and oversee any activities of the Department of Defense that pertain to the relationship between the Department and academia, including with entities involved in primary, secondary, or postsecondary education, with respect to cyber-related matters (in this section referred to as the 'Office').

''(b) DIRECTOR.—The Office shall have a Director who shall report directly to the Chief Information Officer of the Department of Defense. An individual serving as Director shall, while so serving, be a member of the Senior Executive Service.

''(c) RESPONSIBILITIES.—(1) The Office shall be responsible for the following:

''(A) Serving as the consolidated focal point for engagements carried out between the Department of

Defense and academia with respect to cyber-related matters.

''(B) Coordinating covered academic engagement programs for the Department of Defense.

''(C) Conducting ongoing analysis, as determined necessary by the Director, of the performance of cyber-related educational scholarships, camps, support efforts, and volunteer partnerships of the Department of Defense.

''(D) Identifying actions the Secretary of Defense may take to improve the cyber skills of personnel within the Department of Defense through participation by such personnel in covered academic engagement programs, for the purposes of assisting the Secretary in cyber-related matters and meeting the long-term national defense needs of the United States for personnel proficient in such skills.

''(E) Managing funds and resources for the National Centers for Academic Excellence in Cybersecurity program, the Department of Defense Cyber Scholarship Program, the National Defense University College of Information and Cyberspace, the University Consortium for Cybersecurity, and the senior military colleges.

''(F) Establishing requirements, policies, and procedures to collect data on, and to monitor and evaluate, the performance of covered academic engagement programs with respect to the involvement in such programs by the Department of Defense.

''(G) Monitoring and evaluating through applicable performance measurements (including those established pursuant to subparagraph (F)) the performance of covered academic engagement programs with respect to the involvement in such programs by the Department of Defense, and advising the Secretary of Defense on whether to continue, modify, or terminate such involvement.

''(H) Making budgetary determinations, taking into consideration the findings of performance evaluations under subparagraph (G), with respect to—

''(i) the involvement in covered academic engagement programs by the Department of Defense; and

''(ii) other matters relating to the responsibilities under this subsection.

''(2) Notwithstanding any provision of law to the contrary, the Office shall be the office of primary responsibility for carrying out, among other legislative provisions, the following:

''(A) Section 1633 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 2125).

''(B) Section 1640 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2200 note).

''(C) Section 1649 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 133 Stat. 1758).

''(D) Section 1659 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 10 U.S.C. 391 note).

''(E) Section 1710 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 134 Stat. 4086).

''(F) Section 1726 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 10 U.S.C. 1599f note).

''(G) Section 1530 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81; 135 Stat. 2049).

''(H) Section 1532 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81; 10 U.S.C. 2191 note prec.).

''(I) Section 1505 of the National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263).

''(J) Section 1535 of the National Defense Authorization Act for Fiscal Year 2023 (Public Law 117–263).

''(d) AUTHORITY RELATING TO COMPLIANCE.—The Secretary of Defense shall take such steps as may be necessary to ensure that the Director of the Office has sufficient authority to compel and enforce compliance with any decisions or directives issued pursuant to the responsibilities under subsection (b).

''(e) ADDITIONAL AUTHORITIES.—In carrying out this section, the Director of the Office may, under any provision of this chapter or any other provision of this title providing for the support of educational programs in cyber-related matters (and unless otherwise specified in such provision)—

''(1) enter into contracts and cooperative agreements;

''(2) make grants of financial assistance;

''(3) provide cash awards and other items;

''(4) accept voluntary services; and

''(5) support national competition judging, other educational event activities, and associated award ceremonies in connection with covered academic engagement programs.

''(f) RELATIONSHIP TO OTHER ENTITIES.—The Under Secretary of Defense for Research and Engineering and the Secretaries concerned shall coordinate and collaborate with the Director of the Office on covered academic engagement programs sponsored by the Under Secretary as Science, Technology, Engineering, and Mathematics (STEM) programs and activities.

''(g) COVERED ACADEMIC ENGAGEMENT PROGRAM DEFINED.—In this section, the term 'covered academic engagement program' means any of the following:

''(1) A primary, secondary, or post-secondary educational program with a cyber focus.

''(2) A program of the Department of Defense for the recruitment or retention of cyberspace civilian and military personnel, including scholarship programs.

''(3) An academic partnership focused on establishing cyber talent among the personnel referred to in paragraph (2).''.

(b) DEADLINE FOR ESTABLISHMENT.—The Secretary of Defense shall establish the office under section 2192c of title 10, United States Code, as added by subsection (a), by not later than 270 days after the date of the enactment of this Act.

# Subtitle B—Personnel

**SEC. 1521 [Log 77852]. AUTHORITY TO ACCEPT VOLUNTARY AND UNCOMPENSATED SERVICES FROM CYBERSECURITY EXPERTS.**

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

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

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 167b of such title, as amended by subsection (a), is further amended—

(1) in subsection (a)—

(A) in paragraph (1), by striking ''referred to as the 'cyber command' '' and inserting ''referred to as the 'United States Cyber Command' ''; and

(B) in paragraph (2), by striking ''Cyber Command'' and inserting ''United States Cyber Command'';

(2) in subsection (b), by striking ''Cyber Command'' each place it appears and inserting ''United States Cyber Command'';

(3) in subsections (c) and (d)—

(A) by striking ''cyber command'' each place it appears and inserting ''United States Cyber Command'';

(B) by striking ''commander of the'' each place it appears and inserting ''Commander of the''; and

(C) by striking ''commander of such command'' each place it appears and inserting ''Commander of such Command''; and

(4) in subsection (d)(3)(C), by striking ''of the commander'' and inserting ''of the Commander''.

# DIRECTIVE REPORT LANGUAGE

# Table Of Contents

# DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

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

### RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, ARMY

#### Items of Special Interest

*Army use of digital engineering for rotorcraft predictive maintenance*

The committee understands that the Army's Future Vertical Lift (FVL) drive systems represent a significant portion of the cost, schedule, and technical risk for the Future Long-Range Assault Aircraft and the Future Attack Reconnaissance Aircraft programs. Dual-use digital engineering technologies can prove exceptionally valuable in prognostics and predictive maintenance for these programs. The committee encourages the Army to leverage innovative technologies including digital twins, high-performance computing, artificial intelligence, and cloud computing technologies to support prognostic and predictive maintenance for FVL programs.

Therefore, the committee directs the Secretary of the Army to provide a briefing to the House Committee on Armed Services not later than December 1, 2023, on how the Army plans to incorporate digital engineering, artificial intelligence, and other dual-use capabilities to assess FVL rotorcraft drive systems. The briefing should also include how these technologies might reduce risk to and cost of Army FVL programs.

*Hyperspectral sensors for autonomous operations and survivability*

The committee understands the need for modular, adaptive unmanned ground and aerial vehicle payloads to detect adversary threats and mobility hazards. Currently deployed optical sensors often cannot provide the spectral data needed to easily identify, detect, and engage targets and other hazards. The committee notes the value of hyperspectral imaging sensors in effectively identifying these threats, particularly Ultra-Compact Hyperspectral Imaging Systems (UCHIS) which are more mobile and maneuverable. UCHIS provide the necessary discrimination required to detect, identify, and defeat existing and future adversaries more rapidly and can be fitted on existing and future Army platforms including combat vehicles, unmanned aircraft systems, and more. However, the committee is concerned with the pace of development of this critical technology.

Therefore, the committee directs the Secretary of the Army to provide a briefing to the House Committee on Armed Services not later than December 1, 2023, on the Army's plans and strategy to incorporate and develop UCHIS capabilities for current and next generation Army platforms. The briefing should include:

(1) investments to date in the development of UCHIS sensing systems;

(2) overall development and integration timeline for UCHIS capabilities; and

(3) total anticipated program cost.

*Next generation hybrid and electric vertical take-off and landing vehicles for Army modernization*

The committee understands the important role that Future Vertical Lift (FVL) will play in the Army's modernization efforts and future warfighting concepts, including hybrid and electric vertical take-off and landing (VTOL) capabilities. These systems will enable more modern, versatile, and lethal power projection in support of Army multi-domain operations (MDO). The committee encourages the Army to continue to explore the development of novel VTOL concepts, including hybrid and electric propulsion technologies for unmanned aircraft systems that enable Army MDO. The committee also encourages the Army, in coordination with industry, to continue research and development efforts for hybrid and electric VTOL power systems to ensure these battery sources have the necessary power output, decreased heat signatures, and stability to withstand the environmental conditions associated with vertical flight.

Therefore, the committee directs the Secretary of the Army to submit a report to the House Committee on Armed Services not later than December 15, 2023, on the Army's current and future hybrid and electric VTOL research and development efforts. The report should include:

(1) how the Army is incorporating hybrid and electric VTOL solutions into FVL modernization efforts and the impact such systems will have on the Army's ability to conduct MDO;

(2) an overview of current and future research efforts focused on hybrid and electric VTOL battery sources, including ongoing efforts to improve the size, weight, power, and cost of future VTOL systems and power sources;

(3) any future fielding strategies for hybrid and electric VTOL platforms within the Army; and

(4) an overview of collaboration between the Army and the Air Force's Agility Prime program on the research, development, or fielding of next generation hybrid and electric VTOL solutions.

## RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, NAVY

### Items of Special Interest

*Maritime Domain Awareness*

The committee recognizes that the growing presence of Chinese dual-use vessels in disputed waters threatens U.S. national security and economic interests. The committee is increasingly concerned about the ability of the United States to counter this threat due to the vastness of the maritime environment. Maritime Domain Awareness (MDA), driven by artificial intelligence (AI), would enhance the Navy's ability to monitor the maritime environment, increase strategic planning activities, and expose emerging threats through lead generation. In addition, unclassified commercial capabilities would improve the Navy's ability to share relevant information with allies and partners in real time.

Therefore, the committee directs the Secretary of the Navy to provide a briefing to the House Committee on Armed Services not later than February 1, 2024, on the Navy's utilization of AI-powered MDA systems and any capability gaps. The briefing should include the following:

(1) a review and assessment of current unclassified AI MDA tools for enhanced lead generation, decision-making, and identification of capacity gaps;

(2) an analysis of the potential for existing commercial MDA tools with artificial intelligence capabilities to enhance current unclassified and classified systems; and

(3) an assessment of the potential integration of commercial technology into existing MDA tools to fill capability gaps including, but not limited to: evolving short- and long-term behavioral analysis, predictive insights using AI-driven recommendations to increase asset utilization and deployment, tipping and cueing of remote sensors, and enhancing information-sharing with international partners.

## RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, AIR FORCE

### Items of Special Interest

*Air Force Research Laboratory's "one laboratory serving two services" policy*

The committee notes the close collaboration between the U.S. Air Force (USAF) and U.S. Space Force (USSF) at the Air Force Research Laboratory (AFRL) and the value of AFRL's "one laboratory serving two services" policy. The committee expects continued close collaboration between the two services moving forward.

Therefore, the committee directs the Secretary of the Air Force to submit a report to the House Committee on Armed Services not later December 1, 2023, on the following:

(1) a review of the effectiveness of the Air Force Research Laboratory's "one laboratory serving two services" policy;

(2) identification of the scientific areas of common relevance to both USAF and USSF;

(3) a review of the synergies and effectiveness of maintaining the "one laboratory serving two services" policy for space-related scientific areas to advance

operations outside the Earth's atmosphere, including: artificial intelligence, autonomy, biotechnology, cyber, quantum, microelectronics, materials, sensors, human systems, propulsion, directed energy, and hypersonics;

(4) recommendations for any organizational and administrative changes needed to strengthen mission-effectiveness and cost-effectiveness and meet the needs of both USAF and USSF through maintaining the "one laboratory serving two services" policy; and

(5) recommendations for any changes to existing authorities or need for new authorities to optimize defense-focused space-related science and technology missions.

*Digital engineering and prototyping capability for Air Force Research Lab Munitions Directorate*

The committee notes the important role that emerging technologies like digital engineering can play in the development of critical military weapon systems while also cultivating the necessary science and technology workforce of the future at key military installations. The committee encourages the Air Force Research Laboratory to leverage public-private partnerships to collaborate across academia, industry, and government for these critical technologies and capabilities, including digital engineering. These collaborative partnerships would enable the creation of a technically skilled talent pipeline for high-demand, multidisciplinary engineering and cyber careers to support digital engineering efforts.

Therefore, the committee directs the Commander, Air Force Research Laboratory to provide a briefing to the House Committee on Armed Services not later than December 1, 2023, on:

(1) plans to leverage public-private partnerships for digital engineering; and

(2) the impact such engagements would have on workforce development in surrounding military installation communities.

*Joint All-Domain Command and Control concept of operations for digital engineering*

The committee is aware that the U.S. Air Force released Doctrine Note 1-21, Agile Combat Employment, in December 2021. The document highlights a 65 percent reduction in overseas basing since the end of World War II because adversary technology has advanced to a point where once secure overseas bases are now under threat. As a result, the Air Force is investing heavily in a concept called Agile Combat Employment (ACE). This emerging concept is designed to execute logistical activity such as refueling, repairs, and rearming and then return aircraft to battle before an adversary can react.

The committee is also aware that the Department of Defense is developing the Joint All-Domain Command and Control (JADC2) system to connect sensors from each of the military services into a single network and use the data collected

and processed by artificial intelligence to enable commanders to make better decisions across the entire spectrum of defense-related activities. The committee believes that the Air Force would benefit from a JADC2 system that includes a concept of operations for digital engineering, including sustaining military operations in a contested logistics environment enabled by Digital Materiel Management, advanced onsite inspection, and deployed manufacturing and repair capabilities.

Therefore, 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 January 30, 2024, on a strategy to integrate Digital Material Management in contested environments into a JADC2 framework. Such a report shall include, but is not limited to, the following:

(1) elements of a Digital Materiel Management System necessary to transform supply and distribution systems from fully connected "pull" systems optimized for efficiency to "push" systems that maximize distributed mission effectiveness in an ACE environment;

(2) the potential for rapid, repetitive, and real-time modeling and simulation analysis of big data to aid in the development of the Digital Materiel Management System;

(3) an assessment of the potential benefits of artificial intelligence and machine learning in a Digital Material Management System; and

(4) the cost and timeline associated with implementing such a strategy.

*Report on commercial rocket accelerated flight testing program*

Maintaining the United States' superiority in aerospace propulsion is critical to ensure U.S. leadership in technology areas including missile defense, hypersonics, cislunar and deep space, and more. To accomplish this, the committee believes the United States needs a reliable testing infrastructure for propulsion systems, including commercial rocket and propulsion systems. The committee understands that currently no program dedicated to flight testing new commercial propulsion technologies and vehicle systems developed under Department of Defense contracts exists, which threatens the United States' ability to compete against foreign competitors like China, which is investing extensively in next generation propulsion capabilities.

Given the criticality of testing new propulsion technologies, the committee recommends the Department of the Air Force, working through the Air Force Research Laboratory, establish a commercial rocket accelerated flight testing program. This program would be an invaluable resource for the Air Force, Space Force, and industry and help mature high-priority propulsion systems, integral components, and vehicle designs to ensure operational readiness, meet the needs of the future force, and stay ahead of future national security threats.

Therefore, the committee directs the Secretary of the Air Force to submit a report to the House Committee on Armed Services not later than December 1, 2023,

on how the Air Force would establish and execute a commercial rocket accelerated flight testing program. The report should include, but not be limited to:

(1) an overview of the current flight testing facilities and capabilities the Air Force uses to test new propulsion technologies and vehicle systems;

(2) how much funding over the Future Years Defense Program would be required to successfully establish and execute a commercial rocket accelerated flight testing program;

(3) contracting mechanisms to be used to select qualified flight providers, experimental systems, and test flight campaigns; and

(4) options for streamlining vehicle and launch authorization procedures to enable flight testing to occur on Air Force bases in 12 months or less from the date of contract issuance.

The committee also encourages the Air Force to look to existing testing programs across the U.S. Government, like the National Aeronautics and Space Administration Flight Opportunities program, as a model for future flight testing programs.

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

### Items of Special Interest

*Expansion of electromagnetic spectrum sensing capabilities*

The committee understands that cyber and electronic warfare-contested environments present an acute challenge in conflict with a technologically advanced near-peer adversary. Maintaining the highest levels of battlefield awareness will require warfighters to have the ability to rapidly detect, analyze, and identify new signals in the electromagnetic spectrum (EMS). The ongoing conflict in Ukraine has exposed the threat that adversarial electronic warfare systems pose. Accordingly, the committee believes that the Department of Defense should pursue capabilities that give the warfighter the ability to maintain awareness of the EMS environment and rapidly develop insights at the tactical edge.

The committee is aware that special operations forces have successfully employed mature, artificial intelligence (AI)-enabled EMS classification technologies in recent deployments. The committee believes that the Department of Defense should take steps to increase the adoption of such technologies, including by conventional units, to ensure reliable EMS awareness across the joint force.

Therefore, the committee directs the Secretary of Defense to submit a report to the House Committee on Armed Services not later than December 1, 2023, on the Department's efforts to expand the use of proven AI-enabled EMS classification technologies to conventional units. The report should include, but is not limited to, the following elements:

(1) an assessment of the Department's conventional EMS sensing and classification capabilities and operational requirements;

(2) efforts to expand the use of proven, AI-enabled EMS classification systems to conventional units;

(3) efforts to develop next generation EMS classification systems for conventional units; and

(4) market research to determine whether scalable, commercially available solutions exist that can meet the operational requirements of conventional units.

*Magnetoresistive random-access memory*

Due to the high sensitivity of computing memory to both natural and man-made radiation, satellites and other critical defense applications utilizing traditional memory storage are at significant risk to disruption or degradation. Advances in silicon-based memory devices that store information in magnetic fields, magnetoresistive random-access memory (MRAM), have proven to create a commercially viable, hardened memory storage solution that provides protection against disruption or corruption in these critical Department systems.

The committee believes that there is a critical need for a supply of radiation-hardened memory storage used for civil and Department of Defense applications but recognizes that a current dependency on an overseas supply chain exacerbates the vulnerabilities of Department systems.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later December 31, 2023, on the Department's plans to utilize current onshore suppliers for the advancement of MRAM solutions across the military services.

*Mobile nuclear reactors*

The committee is aware of the Department of Defense's efforts to address the growing challenges of reliable, sustainable, and resilient energy sources to power its various military installations and forward operating positions around the world. The committee has directed investments in previous years in micro-nuclear reactors as a promising emerging technology to provide portable, safe, consistent, clean electric and thermal power, regardless of environmental or operational conditions.

The committee notes Congress' effort to establish a second source for the mobile microreactor program which greatly improves the Strategic Capabilities Office's ability to develop electrical power sources that are responsive to differing military service requirements. However, the importance of mobile nuclear reactors is critical to the future fight.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services, not later than February 1, 2024, on the Department's research and development efforts related to micro-nuclear reactors, including diverse development avenues, a cost-benefit analysis of their viability, identification of any logistical or statutory challenges to the supply

chain to fuel these reactors, and an evaluation of the whether or not an executive agent should be designated for the program.

*MyTravel implementation*

The committee notes that the Department of Defense has invested significant resources to replace the Defense Travel System with a modern travel system, MyTravel. This is expected to improve the travel experience for Department of Defense personnel, create efficiencies, drive down costs, and allow the Department to retire legacy travel systems. On October 21, 2022, the Department designated MyTravel as the "single official travel system for currently supported travel functions as well as those supported in the future, as they become available."

The committee is concerned that the military services and some Department of Defense entities have not complied with this direction. Delayed implementation of MyTravel wastes resources that could be reallocated to other Department priorities and keeps outdated process and legacy systems in place.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than December 1, 2023, on the status of implementation of MyTravel across the military services and a plan for transitioning any military services or Department entities that have not yet transitioned to MyTravel.

*Near-term and long-term science and technology*

With the conflict in Ukraine and China's aggression towards Taiwan, the United States cannot predict when and where the Department of Defense's capabilities and technology will be needed.

The Department's research and development enterprise is the foundation for the Department's future capabilities and technology. However, with the uncertainty of where and when these capabilities and technologies may be needed, the science and technology portfolio must be balanced between capabilities and technologies that will transition in the near-term, within 5 years, and those which will transition in the long-term, after 5 years.

The committee is concerned with the balance of the science and technology portfolio. Therefore, the committee directs the Under Secretary of Defense for Research and Engineering to submit a report to the House Committee on Armed Services not later than February 1, 2024, detailing a metric or analysis to determine which capabilities are near-term transition capabilities and which are long-term and a methodology for how these two should be balanced.

*Northeast Multi-Domain Operations Consortium*

The committee recognizes that electronic warfare (EW), commercial telecommunications capabilities, and cyber operations are key enablers for Multi-domain Operations (MDO). The committee further recognizes that China has

advanced its ability to deny, disrupt, and degrade U.S. underlying networks and infrastructure by developing its own multi-domain capabilities. In response to this operational reality, the committee is concerned by the Department of Defense's current lack of resources and terrain to test, evaluate, and train MDO capabilities in contested EW environments.

The committee notes the progress of the Northeast Regional National Security Consortium in creating a joint, interagency MDO training environment. The consortium endeavors to promote research, experimentation, and training in realistic environments that represent near-peer adversary EW capabilities and activities. This cooperative effort between the military, industry, academia, and Native American organizations, throughout a multistate region, is unique in its approach and scope.

Therefore, the committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Commander, Air Force Research Laboratory, the Assistant Secretary of the Army for Acquisition, Technology and Logistics, and others the Under Secretary deems relevant, to provide a briefing to the House Committee on Armed Services not later than December 31, 2023, on how the unique environment of the Northeast can be utilized for training in EW and MDO. The briefing should include:

(1) a description of the current state of non-kinetic MDO training ranges for use by the Department of Defense, including limitations of the Department to effectively conduct MDO at these ranges;

(2) an assessment of existing capabilities in the Northeast region and the potential to expand MDO training opportunities in the Northeast region;

(3) identification of future sites, including contractor-owned, contractor-operated sites, that are uniquely postured for MDO training;

(4) recommendations on how to streamline continuous training, testing, and evaluation activities that replicate an EW-contested environment; and

(5) opportunities to enhance integration of the National Guard Bureau within the aforementioned constructs.

*Reusable hypersonic multi-mission aircraft*

The committee notes the potential applications of reusable hypersonic multi-mission aircraft to critical intelligence, surveillance, and reconnaissance, and strike missions, particularly in exclusion areas in the Indo-Pacific theater of operations. Peer adversaries continue to advance in hypersonic technology, including reusable systems, that pose a threat to U.S. national security interests.

However, the committee is concerned by the lack of research and development funding directed towards fielding a reusable hypersonic platform with aircraft-like operations and qualities. Therefore, the committee directs the Under Secretary of Defense for Research and Engineering to submit a report to the House Committee on Armed Services not later than December 31, 2023, on the status of budgeting for future development of reusable hypersonic multi-mission aircraft, as

well as requirements for development and key technology activities determined necessary. The report should be submitted in unclassified format but may contain a classified annex.

*Science and technology transition definitions*

The committee recognizes that while not every research and development project should become a program of record, there are challenges across the Department of Defense in transitioning technologies to support the warfighter. The "valley of death" is a problem recognized by those both inside and outside of the Department, but few can clearly define it.

Therefore the committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Acquisition and Sustainment, to submit a report to the House Committee on Armed Services not later than December 31, 2023, detailing quantitative measures of effectiveness and performance to assess and track transition of science and technology projects from the initial stages of research and development to fielded capabilities or technology. Metrics may include, but are not limited to:

(1) definition of technology transition, including the various types of technology transition;

(2) amount of time taken to transition from the research and development phase to the acquisition and fielding phase;

(3) cost required to transition from the research and development phase to the acquisition and fielding phase; and

(4) manhours used to transition from the research and development phase to the acquisition and fielding phase.

# TITLE XV—CYBERSPACE-RELATED MATTERS

## ITEMS OF SPECIAL INTEREST

### Authority to Operate

The committee recognizes that enterprise-wide adoption of bring your own device (BYOD) policies will bring secure communications to a broader section of Department of Defense personnel while simultaneously reducing costs and enabling a more mobile workforce. However, the committee is aware of gaps in Department of Defense policies preventing applications granted provisional authority to operate (P-ATO) on government-furnished equipment from being given P-ATO on personal devices currently enrolled in a BYOD program.

While the committee applauds the Department of Defense's efforts to establish BYOD programs that allow personnel to continue their critical work using BYOD-eligible devices, the committee is concerned that enduring gaps in the Department of Defense's policies will continue to impact personnel's ability to

connect to critical back-end systems up to Impact Level 5/Controlled Unclassified Information.

The committee believes that the Department of Defense must create policies that enable secure, reliable connection of BYOD-eligible devices to necessary Department of Defense systems.

Therefore, the committee directs the Chief Information Officer, Department of Defense to provide a briefing to the House Committee on Armed Services not later than January 1, 2024, on existing gaps in Department of Defense policy governing the issuance of P-ATO on BYOD-eligible devices and the Department of Defense's efforts to ensure its personnel can access those systems critical to executing their missions.

### Data Literacy in Artificial Intelligence

The committee recognizes the increasing complexities of artificial intelligence (AI) and machine learning capabilities available within the Department of Defense. To ensure the proper implementation of these new technologies, there must be a focus on data literacy across a broader population within the Department. Section 256 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92) required the Department of Defense to develop an AI education strategy, with the stated objective to educate "servicemembers in relevant occupational fields on matters relating to artificial intelligence."

Given the continued centrality of AI to warfighting, the committee directs the Chief Digital and Artificial Intelligence Officer of the Department of Defense to provide a briefing to the House Committee on Armed Services not later than March 31, 2024, on the implementation status of the AI education strategy, with emphasis on current efforts underway, such as the AI Primer course within the Army's Intelligence Center of Excellence.

### Data Repositories, Access, and Utilization

The committee commends the Department of Defense and the Chief Digital and Artificial Intelligence Office (CDAO) focus on building the scaffolding, or infrastructure, to produce the high-quality data required to support artificial intelligence and machine learning capabilities developed across the Department. The committee encourages the CDAO to continue to ensure requirements for the procurement of data repositories and the infrastructure for artificial intelligence and machine learning operations are clear to both government and industry stakeholders, particularly in regard to functions to be performed, performance required, and essential physical characteristics. As the CDAO continues to mature, the committee seeks additional information about how requirements for data repositories, access, and scaffolding are both developed and communicated to the totality of stakeholders involved.

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 December 1, 2023, about how requirements for data services are developed and socialized and how market research is performed as part of the acquisition process. Additionally, the briefing should include information about how the CDAO will develop policy and enforce compliance to the maximum extent possible.

### Evaluation of National Centers of Academic Excellence in Cybersecurity

The committee believes that promoting education and developing expertise in cybersecurity is vital to protecting United States critical infrastructure and growing the national cybersecurity workforce. The committee supports the efforts of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program to advance cybersecurity education in colleges and universities but is concerned that challenges in oversight and implementation may hinder the program's success.

Therefore, the committee directs the Secretary of Defense to submit a report to the House Committee on Armed Services not later than December 1, 2023, assessing the NCAE-C program. The report should include:

(1) an evaluation of challenges in administration and implementation, both at the program level and at individual institutions;

(2) a review of metrics used to evaluate the continued alignment of institutions with program requirements and objectives;

(3) participation metrics, including but not limited to the number of institutions currently designated or being considered for designation, geographical distribution of the institutions, and number of students receiving relevant degrees and certificates; and

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

### Innovation for Cybersecurity of the Defense Industrial Base

The committee recognizes the challenges faced by the Department of Defense in securing its own critical data, intellectual property, networks, and infrastructure, as well as that of its supporting defense industrial base (DIB), from cyberattack. Multiple offices within the Department of Defense, the military services, and the National Security Agency have programs focused upon various aspects of this massive problem. Over more than a decade, Congress has pursued many courses to address the substantial issue of cybersecurity for the DIB. This includes reviews, new authorities, and directed support for programs such as the Cybersecurity Maturity Model Certification and the National Cyber Security Operations Center. Unfortunately, the problem persists with seemingly little progress made. The committee remains unsatisfied and concerned that until the issue can be addressed holistically and is made a priority for the leadership of the Department of Defense, the United States will continue to see successful cyberattacks by nation states and non-state actors.

Therefore, the committee directs the Chief Information Officer of the Department of Defense, in coordination with the secretaries of the military

departments, the Under Secretary of Defense for Acquisition and Sustainment, and the Under Secretary of Defense for Policy, to provide a briefing to the House Committee on Armed Services not later than January 31, 2024, on DIB cybersecurity efforts, specifically those efforts performing in an exemplary or satisfactory manner, as well as those efforts being underutilized or which are underperforming.

### Internet Access Point Modernization

The committee commends the Defense Information Systems Agency and Joint Force Headquarters–Department of Defense Information Network on the actions taken to date on modernizing and monitoring the Department of Defense's network and information technology infrastructure. As part of this, the Department's internet access points (IAPs) play a critical, if often overlooked, part in the delivery of data to and across the enterprise. To this end, the Department requires that these IAPs be upgraded and modernized to keep abreast of adversaries.

Therefore, the committee directs the Director, Defense Information Systems Agency, serving concurrently as the Commander, Joint Force Headquarters–Department of Defense Information Network, to provide a briefing to the House Committee on Armed Services not later than March 1, 2024, on the efforts underway to modernize the IAP infrastructure of the Department.

### Internet Operations Management

The committee is encouraged by strides made by Joint Force Headquarters-Department of Defense Information Network (JFHQ–DODIN) to improve its enterprise-wide visibility of Department of Defense networks through internet operations management (IOM), a critical component of ongoing efforts to harden Department of Defense networks. The additional network visibility this capability provides can most meaningfully drive risk reduction if seamlessly integrated with state-of-the-art security orchestration and automation capability deployable in the military services and U.S. Cyber Command's Big Data Platforms.

Therefore, the committee directs the Commander, JFHQ-DODIN to provide a briefing to the House Committee on Armed Services not later than August 1, 2024, on future plans for IOM, to include consideration of enterprise-wide visibility for the Department's entire internet presence.

### Next Generation Cyber Red Teams

The Department of Defense uses military service-led cyber red teams (CRTs) to identify critical problems and improve defenders' capabilities and decision making for operational-level cyber operations. The committee is concerned that CRTs face many challenges, like high demand, lack of resources and personnel, as well as a need for automation capabilities to ease workload, that may decrease their

ability to effectively and efficiently do their job. Section 1660 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92) recognized the shortfalls in Department of Defense red team capability and required a joint assessment of Department of Defense CRT capabilities, capacity, demand, and requirements. Despite that required assessment, the Department continues to struggle with providing the red team capacity demanded by the the military services and components.

Therefore, the committee directs the Chief Information Officer, Department of Defense, in coordination with the Secretaries of the military services, to submit a report to the House Committee on Armed Services not later than December 31, 2023, which includes the following elements:

(1) actions taken as a direct result of the joint assessment directed in section 1660 of Public Law 116-92;

(2) a quantitative assessment and judgement on whether red team capacity has been properly funded since the delivery of the joint assessment directed in section 1660 of Public Law 116-92;

(3) a qualitative assessment of Department of Defense red team capacity at present and obstacles for addressing any shortfalls identified;

(4) efforts to modernize CRTs with a focus on utilizing cyber threat intelligence, threat modeling, automation, artificial intelligence/machine learning capabilities, and data collection and correlation;

(5) an inventory of all certified Department of Defense red teams and parent organizations;

(6) a determination by the Chief Information Officer, Department of Defense, the Assistant Secretary of Defense for Cyber Policy, and the Commander of United States Cyber Command as to whether all red teams shall be included within the Cyberspace Operations Forces; and

(7) a description of the methodology for the oversight of Department of Defense red team certification and compliance.

North Atlantic Treaty Organization and Cyberspace Operations

The committee asserts that there is robust potential for the North Atlantic Treaty Organization (NATO) to improve how it considers and incorporates cyberspace operations into its planning efforts. To date, despite previous calls and a recognition of cyberspace as an operational domain in 2016 at the NATO summit, the Department of Defense has not accounted for nor identified why this remains a persistent gap in alliance operations. It remains unclear whether expertise for cyberspace operations is provided by U.S. European Command's Joint Cyber Center or U.S. Cyber Command's Cyberspace Operations Integrated Planning Element collocated with U.S. European Command. Before achieving success operationally, the committee believes these questions will need answers.

Therefore, the committee directs the Assistant Secretary of Defense for Cyber Policy to submit a report to the House Committee on Armed Services not

later than March 31, 2024, which addresses precisely how the Department's cyber capabilities have been incorporated into NATO planning forums and obstacles that hinder more comprehensive efforts to leverage cyberspace operations in NATO activities. Additionally, this report should contain an inventory of prior legislative mandates concerning NATO and cyberspace activities and a list of changes enacted after these prior requirements were satisfied.

### Thunderdome and Other Zero Trust Initiatives in the Department of Defense

The committee is encouraged by the Department of Defense's efforts to implement zero trust principles and architecture within and across the Department of Defense information networks, best exemplified by the Thunderdome effort under the Department of Defense Chief Information Officer and the Defense Information Systems Agency (DISA). If executed properly, Thunderdome has the potential to operationalize zero trust in an enterprise fashion. However, there remain key questions about what Thunderdome requires to be successful.

Therefore, the committee directs the Chief Information Officer, Department of Defense, in coordination with the Director, Defense Information Systems Agency, to provide a briefing to the Senate Committee on Armed Services and the House Committee on Armed Services not later than March 1, 2024, on Thunderdome and other related zero trust efforts. This briefing should include deployment milestones and associated timelines, a discussion of progress made to date, and potential plans to promote the adoption of additional Thunderdome subtenants at Department of Defense components beyond DISA.

### U.S. Northern Command Employment of Technology in Homeland Defense

The committee believes that as the geographic combatant command-designated lead for homeland defense, U.S. Northern Command (USNORTHCOM) is well-postured to capitalize on the promise of artificial intelligence and machine learning for critical defensive missions, to include defense from airspace incursions. However, the Commander, USNORTHCOM is dependent in many cases on the military services for the provision of technology services.

Therefore, the committee directs the Commander, U.S. Northern Command, to provide a briefing to the House Committee on Armed Services not later than January 31, 2024, on efforts, programs, and initiatives either underway or planned to utilize new technologies in the furtherance of the USNORTHCOM mission set. The briefing should include a consideration for efforts at other combatant commands, such as U.S. Central Command, which has established a new Chief Technology Officer on the senior staff of the command.

### Utilization of National Guard and Reserve Forces in Cyberspace Operations

Over the last 10 years, Congress has expressed its position that the Department of Defense can bolster its operational capacity in cyberspace through

improved utilization of the National Guard. This has resulted in 10 legislative provisions over a decade's worth of National Defense Authorization Acts and is most pertinently expressed through sections 1729 and 1730 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283). Despite these calls for change, the Department of Defense and the military services appear not to have made any meaningful change in how the expertise resident within the National Guard and the Reserve Component can be better leveraged.

Therefore, the committee directs the Assistant Secretary of Defense for Cyber Policy, in coordination with the Commander, U.S. Cyber Command, to submit a report to the Senate Committee on Armed Services and the House Committee on Armed Services not later than May 31, 2024, on the specific actions and institutional obstacles that have prevented change from being instantiated after the requirements directed in the following legislative provisions:

(1) section 1651 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328);

(2) section 1653 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232); and

(3) section 1729 and 1730 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283).