SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS EN BLOC #1

LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
1586	0	Bacon, Don	CIT	Directs DHS to provide a report on the federal cyber incident response.	EB 1
1622	1	Crow, Jason	CIT	Report Language for a briefing on defense biosecurity molecular cryptography	EB 1
1674	1	Bacon, Don	CIT	Directs SECDEF to provide a briefing on the Electromagnetic Battle Management (EMBM) program	EB 1
1704	0	Fallon, Pat	CIT	Requires the Secretary of Defense to submit a report on commercial 5G deployment on military installations	EB 1
1721	0	Johnson, Mike	CIT	Standardizes the process and software platform for requesting an authority to operate for an IT system on DoD Networks; requires the issuance of a reciprocity policy by the DOD - CIO	EB 1
1784	2	McClain, Lisa C.	CIT	Directs a briefing by the Army on plans for partnership with HBCUs and non-profit organizations in order to build the next generation of STEM leaders.	EB 1
1805	2	Brown, Anthony G.	CIT	Requires a cost estimate for the relocation of the offices of the Joint Spectrum Center	EB 1
1811	2	Moore, Blake D.	CIT	A report on the Department's Commercial Solutions for Classified (CSfC) Program, to include information about engagement with the private sector accessibility of related information by the public.	EB 1
1820	3	Moore, Blake D.	CIT	Directive Report Language on actions being taken to address IoT security of endpoint devices and how the DIU is working with non-traditional software development locations on these innovative technologies.	EB 1
1849	1	Jackson, Ronny	CIT	Directs the U.S. Army Research Labs to continue working with academic partners when developing stronger and lighter soldier protection materials	EB 1
1892	0	Waltz, Michael	CIT	National research and development strategy for distributed ledger technology	EB 1
1903	1	Wittman, Robert	CIT	Requests a report on opportunities the visible light spectrum might offer for secure communications for the Department of Defense	EB 1
1911	0	Speier, Jackie	CIT	Establishes an electric battery research pilot	EB 1

LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
1943	1	Fallon, Pat	CIT	Requires the Secretary of Defense to establish a target date to deploy 5G wireless infrastructure on all military installations	EB 1
1947	0	Banks, Jim	CIT	Establishes an Innovation Fellowship program at DARPA to expand opportunities for early career scientists.	EB 1
1948	0	Banks, Jim	CIT	Directs a report on options to support graduate students working on DARPA projects.	EB 1
2049	1	Bice, Stephanie I.	CIT	This DRL amendment tasks the USD(A&S) to provide a report that includes options to streamline the Information Assurance and Cyber Security approval processes for software acquisitions	EB 1
2089	1	Scott, Austin	CIT	This DRL directs the Secretary of Defense to provide a briefing on Cybersecurity activities with the country of Georgia.	EB 1
2097	1	Moulton, Seth	CIT	Clarifies the ability of the Under Secretary of Defense for Policy to delegate roles and responsibilities related to Information Operations.	EB 1
2100	1	Bice, Stephanie I.	CIT	Requires a briefing on efforts to identify and mitigate software supply chain threats and vulnerabilities.	EB 1
2107	0	Rogers, Mike	CIT	Allow the Secretary of DHS to select regional consortia	EB 1
2115	1	Bice, Stephanie I.	CIT	A report on DoD's strategy for future multi-cloud projects.	EB 1
2167	1	Horsford, Steven	CIT	Requires GAO to examine the impacts of restrictive enterprise software licenses.	EB 1
2204	2	Panetta, Jimmy	CIT	Requests that the Secretary of Defense, in coordination with the Principal Information Operations Advisor, conduct an assessment concerning the policymaking process for information operations across the defense enterprise	EB 1
2206	0	Panetta, Jimmy	CIT	Requests that the Secretary of Defense, in coordination with the Under Secretary for Research and Engineering, produce an Intellectual Property Strategy and report back to the Armed Services Committees regarding its implementation.	EB 1
2208	0	Panetta, Jimmy	CIT	Adds specificity to Sec. 1521 of the FY 2021 NDAA related to cybersecurity products	EB 1

LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
2232	2	DesJarlais, Scott	CIT	Directs the Under Secretary of Defense for Research and Engineering to undertake a review of the resources, budget, needs and opportunities to expand S&T research participant appointments.	EB 1
2234	1	Golden, Jared F.	CIT	DRL to examine large scale additive manufacturing potential to enhance expeditionary capability across a range of operational environments	EB 1
2247	0	Morelle, Joseph D.	CIT	Directive Report Language mandating a briefing on the Department of the Army's data infrastructure modernization efforts	EB 1
2251	2	Moore, Blake D.	CIT	Requires a briefing identifying identifying opportunity areas for further collaboration between military leadership at the installation level and non-traditional small businesses, startups, and venture-backed startups and scaleups.	EB 1
2328	1	Bice, Stephanie I.	CIT	Expresses support for Army Research Lab partnerships with academia and private industry to develop commercially available CUAS technologies	EB 1
2350	1	Golden, Jared F.	CIT	Requirement for SECDEF to provide a report on implementing uniform standards and requirements regarding the deployment of gesture control technology.	EB 1
2388	0	Moore, Blake D.	CIT	Requires a report on how the DoD can improve the Small Business Innovation Research program	EB 1
2394	0	Crow, Jason	CIT	Requires an assessment and optimization plan for DoD operations within the cyber domain	EB 1
2396	0	Crow, Jason	CIT	Requires a comprehensive assessment of cybersecurity vulnerabilities to Department of Defense weapons systems	EB 1
2433	0	Garcia, Sylvia	CIT	Requires the Sec. of the Treasury to submit an annual report to the Financial Services Committee on the state of its cybersecurity measures to protect the financial sector	EB 1
2437	0	Banks, Jim	CIT	Directs a report on plans to integrate advanced combustion technologies into Navy systems.	EB 1

AMENDMENT TO H.R. 7900

OFFERED BY MR. BACON OF NEBRASKA

At the appropriate place in the bill, insert the following:

SEC. ___. REPORT ON CYBERSECURITY ROLES AND RESPONSIBILITIES OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the roles and responsibilities of the Department and its components relating to cyber incident response.

(b) CONTENTS.—The report required under subsection (a) shall include the following:

(1) A review of how the cyber incident response plans under section 2210(c) of the Homeland Security Act of 2002 (6 U.S.C. 660(c)) are utilized in

the Federal Government's response to a cyber incident.

(2) An explanation of the roles and responsibilities of the Department of Homeland Security and its components with responsibility for, or in support of, the Federal Government's response to a cyber incident, including primary responsibility for working with impacted private sector entities.

(3) An explanation of which and how authorities of the Department and its components are utilized in the Federal Government's response to a cyber incident.

(4) Recommendations to provide further clarity for roles and responsibilities of the Department and its components relating to cyber incident response.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Crow

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Defense Biosecurity Molecular Cryptography Research

The committee recognizes the importance of biosecurity and the potential threats posed by the proliferation of advanced gene editing technologies by state and non-state actors. As biotechnology capabilities have become more democratized and globally accessible, the strategic importance of securing servicemembers genetic data has become more critical. The committee notes the continued importance of investing in research and development to mature technologies that provide protection of sensitive genetic information, including the utilization of Small Business Innovation Research contracts to engage small businesses and non-traditional defense contractors for leading edge commercial technologies. The committee is aware of ongoing research that applies novel cryptography directly to DNA molecules, significantly enhancing the protection provided for genetic information, reducing the risk of incidental data breaches, supply chain vulnerabilities, and malicious cyber actors. The committee directs the Under Secretary of Defense for Research and Engineering to provide a briefing by March 1, 2023 to the House Armed Services Committee on biosecurity molecular cryptography research within the Department.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by Mr. Bacon of Nebraska

As appropriate in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Electromagnetic Battle Management Machine Learning Integration

The committee supports the efforts of the Defense Information Systems Agency (DISA) to rapidly prototype and develop a Joint Electromagnetic Battle Management (EMBM) system. The committee anticipates that the EMBM Minimum Viable Capability Release 1 (MVCR1) will provide capabilities that are critical to countering the efforts of near peer competitors who seek to degrade our operational capabilities in the electromagnetic spectrum.

The committee also supports DISA's use of an agile acquisition methodology for EMBM, and agrees that future iterations of EMBM will need to add and refine functionality in order to provide a mature solution that is capable of enabling long term electromagnetic superiority. Furthermore, the committee believes that achieving superiority in electromagnetic spectrum operations will require the rapid integration of machine learning technologies into programs that support this critical mission area. Some machine learning capabilities will be included in MVCR1, however, additional resourcing will be required to provide a mature solution capable of incorporating machine learning that implements EMBM tasks within the DoD's Electromagnetic Spectrum Superiority Strategy Implementation plan and enables long term electromagnetic superiority.

Therefore, the committee directs the Director of the Defense Information Systems Agency to provide a briefing to the House Committee on Armed Services by March 31, 2023, on DISA's plan to incorporate machine learning capabilities into the EMBM MVCR1 program.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Fallon

In the portion of the report to accompany H.R. 7900 titled "Report on commercial 5G deployment on military installations", strike the following text:

"The committee believes that robust information technology and wireless infrastructure contribute to readiness, safety, and quality of life for service members and their families.

Therefore, the committee directs the Secretary of Defense to provide a report to the House Committee on Armed Services not later than May 1, 2023, that includes the following:

(1) an assessment of the number of military installations with access to commercial 5G infrastructure;

(2) a review of barriers to broader commercial 5G deployment on military installations;

(3) a review of the funding and approval process for commercial 5G deployment on military installations; and

(4) a plan, to include funding and a timeline, on the feasibility of ensuring commercial 5G is available at all military installations."

and insert the following new text:

"The committee is concerned about the pace at which the Department of Defense is facilitating commercial 5G infrastructure deployment on military installations. Maintaining parity between the development of civilian coverage outside an installation and coverage on an installation is both a readiness and quality of life issue for servicemembers. Despite the establishment of a common form for siting a communications facility installation on federal lands in Public Law 115-141, each Military Department appears to be establishing its own process which is slowing wireless broadband deployment. The lack of designation of a singular official responsible for the oversight of this process for each Military Department is also hampering execution.

With this in mind, the committee directs the Secretary of Defense to submit a report to the House Committees on Armed Services by May 1, 2023 on the Department of Defense's plan to reduce barriers to siting communications facilities necessary for commercial 5G on military installations. At a minimum, the report should include:

(1) An assessment of the number of military installations with access to commercial 5G infrastructure
(2) A description of the Department of Defense's current process for reviewing an application for communications facilities necessary for commercial 5G deployment on military installations within each Military Department, and the role each Military Department and Installation plays in that process.
(3) How the Department of Defense is utilizing the Standard Form 299 process as required by Public Law 115-141, Division P, Title VI, Sec. 606.
    a. This should include compliance with the 270 day "shot clock" requirement.
(4) The number of applications each Military Department has received for the communications facilities necessary for commercial 5G deployment on installations over the last 6 years.
(5) The number of applications each Military Department has approved for communications facilities necessary for commercial 5G deployment on installations over the last 6 years.
(6) The average response time to each of these applications.
(7) Whether each Military Department has an online portal for processing the Standard Form 299. In the case of a Military Department that does not utilize an online portal, what the plan of the Military Department is to implement an online portal for reviewing the Standard Form 299.
(8) A plan, to include funding and a timeline, on the feasibility of ensuring commercial 5G is available at all military installations."

AMENDMENT TO H.R. 7900

OFFERED BY MR. JOHNSON OF LOUISIANA

At the appropriate place in title XV, insert the following new section:

SEC. 15___. STANDARDIZATION OF AUTHORITY TO OPERATE APPLICATIONS IN THE DEPARTMENT OF DEFENSE.

(a) POLICY.—

(1) REQUIREMENT.—Not later than 270 days after the date of the enactment of this Act, the Chief Information Officer of the Department of Defense shall establish a policy with criteria for the reciprocity of authority to operate for software and hardware between all networks of the Department of Defense.

(2) CONTENTS.—The policy under paragraph (1) shall contain the following:

(A) Procedures for requesting an authority to operate that applies to all networks of the Department.

(B) Guidance on when authorizing officials should grant an information technology platform that has already received an authority to

operate on another network of the Federal Government a reciprocal authority to operate on a network of the Department of Defense.

(C) A standardized format for documentation to support the evaluation of a request for an authority to operate.

(b) SINGLE PLATFORM.—Not later than one year after the date of the enactment of this Act, the Chief Information Officer shall implement a single software tool or platform for the submission and review of requests for an authority to operate applications. The tool or platform shall—

(1) be used by all authorizing officials of the Department for the receipt, review, and adjudication of all such requests; and

(2) authorize persons who submit such requests to see the progress of the request at all steps in the review process.

(c) REPORT.—Not later than one year after the date of the enactment of this Act, the Chief Information Officer shall submit to the congressional defense committees a report on the following:

(1) The operational status of the software tool or platform implemented under subsection (b).

(2) A list of all networks and authorizing officials of the Department that are using the software tool or platform.

(3) A list of all networks and authorizing officials of the Department that are not using the software tool or platform.

(d) AUTHORITY TO OPERATE DEFINED.—In this section, the term ''authority to operate'' means the official management decision given by a senior organizational official to authorize operation of an information system and accept the risk to organizational operations.

☒

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mrs. McClain

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Support for STEM Education in Historically Black Colleges and Universities

The Department of Defense faces challenges recruiting and retaining a workforce skilled in science, technology, engineering, and mathematics (STEM). While this is a nationwide concern, the Committee supports the efforts of the Department of Defense to grow the STEM workforce pipeline, particularly for women and under-represented minorities in the areas of additive metals manufacturing, modeling and simulation, renewable energies, and skilled trades.

The Committee directs the Secretary of the Army to provide a briefing to the House Armed Services Committee by December 30, 2022 on how it plans to partner with HBCUs and non-profit organizations to leverage their expertise in the aforementioned areas of research to inform future requirements while building the next generation of STEM leaders.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: MR. BROWN OF MARYLAND

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Joint Spectrum Center Relocation

The committee directs the Secretary of Defense to provide the House and Senate Armed Services Committees, not later than December 23, 2022, with a report containing a cost estimate for the relocation of the offices of the Joint Spectrum Center to Fort Meade, Maryland . The cost estimate shall include, but not be limited to, the costs associated with moving the Joint Spectrum Center to its current designated building at Fort Meade, Maryland, as well as the cost and mission efficiencies that could be achieved by consolidating some or all Joint Spectrum Center personnel and mission with the Defense Spectrum Organization and other existing missions located at the Defense Information Systems Agency headquarter building at Fort Meade, Maryland. The committee also directs the Secretary of Defense to provide the committees with the results of a full Balanced Survivability Assessment of the Joint Spectrum Center's current leased facility at the former David Taylor Research Center site in Annapolis, MD as part of the report directed above.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Moore

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Commercial Solutions for Classified Program Architecture Review

The committee recognizes the success of the National Security Agency's Commercial Solutions for Classified (CSfC) Program, which enables commercial products to be used in layered solutions to protect classified National Security System data. However, the committee is aware that some stakeholders from industry have made claims that the CSfC Architecture is not reviewed or updated in a timely manner, and may not incorporate feedback from the private sector. While the committee is aware of recent and upcoming updates of CSfC Capability and Annexes, the committee believes that greater clarity on the issue is required. Therefore the committee directs the Secretary of Defense to submit a report to the House Committees on Armed Services of the Senate and the House of Representatives by March 1, 2023, on the Department's efforts to date for CSfC, to include communication with the private sector, public accessibility of information, and existing forums or mechanism for public engagement.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Moore

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Internet of Things Security

Cyber competition with Russia and China is heightening the sense of urgency with which the nation must reform our acquisition approach to maintain our military and technological superiority. The committee is concerned that near peer adversaries are challenging the U.S. across several cyber dimensions, including the threat to Internet of Things (IoT) and end point devices. The committee believes this new era of competition requires technological superiority to ensure the security of IoT devices from enhanced cyberattacks. Therefore, the committee directs the Chief Information Officer of the Department of Defense to provide a briefing to the House Committee on Armed Services by March 1, 2023, on the Department's actions to address IoT security of end point devices.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Jackson of Texas

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Material Development for Personal Protection Systems

The committee recognizes the importance of developing enhanced technologies such as lightweight armors, protective structures, kinetic energy active protection, ballistic shock protection, and helmet technologies to meet the current threats posed by adversaries. The committee understands that utilizing computational modeling and simulation allows for greater cost savings to the Department of Defense. Methods such as computational research allow for the development of models that predict the mechanical response of materials that are used in research and development at the U.S. Army Research Laboratory.

Therefore, the committee directs the Commander, U.S. Army Futures Command, to provide a briefing to the House Committee on Armed Services not later than March 1, 2023, that identifies efforts to collaborate with academic partners and to utilize computational modeling to develop new soldier protection materials that are lighter and stronger than current materials while providing greater protection.

AMENDMENT TO H.R. 7900

OFFERED BY MR. WALTZ OF FLORIDA

At the appropriate place in division E, insert the following:

SEC. ___. NATIONAL RESEARCH AND DEVELOPMENT STRATEGY FOR DISTRIBUTED LEDGER TECHNOLOGY.

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—Except as otherwise expressly provided, the term ''Director'' means the Director of the Office of Science and Technology Policy.

(2) DISTRIBUTED LEDGER.—The term ''distributed ledger'' means a ledger that—

(A) is shared across a set of distributed nodes, which are devices or processes, that participate in a network and store a complete or partial replica of the ledger;

(B) is synchronized between the nodes;

(C) has data appended to it by following the ledger's specified consensus mechanism;

(D) may be accessible to anyone (public) or restricted to a subset of participants (private); and

(E) may require participants to have authorization to perform certain actions (permissioned) or require no authorization (permissionless).

(3) DISTRIBUTED LEDGER TECHNOLOGY.—The term ''distributed ledger technology'' means technology that enables the operation and use of distributed ledgers.

(4) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

(5) RELEVANT CONGRESSIONAL COMMITTEES.—The term ''relevant congressional committees'' means—

(A) the Committee on Commerce, Science, and Transportation of the Senate; and

(B) the Committee on Science, Space, and Technology of the House of Representatives.

(6) SMART CONTRACT.—The term ''smart contract'' means a computer program stored in a distributed ledger system that is executed when certain predefined conditions are satisfied and wherein the outcome of any execution of the program may be recorded on the distributed ledger.

(b) NATIONAL DISTRIBUTED LEDGER TECHNOLOGY R&D STRATEGY.—

(1) IN GENERAL.—The Director, or a designee of the Director, shall, in coordination with the National Science and Technology Council, and the heads of such other relevant Federal agencies and entities as the Director considers appropriate, which may include the National Academies, and in consultation with such nongovernmental entities as the Director considers appropriate, develop a national strategy for the research and development of distributed ledger technologies and their applications, including applications of public and permissionless distributed ledgers. In developing the national strategy, the Director shall consider the following:

(A) Current efforts and coordination by Federal agencies to invest in the research and development of distributed ledger technologies and their applications, including through programs like the Small Business Innovation Research program, the Small Business Technology Transfer program, and the National Science Foundation's Innovation Corps programs.

(B)(i) The potential benefits and risks of applications of distributed ledger technologies

across different industry sectors, including their potential to—

(I) lower transactions costs and facilitate new types of commercial transactions;

(II) protect privacy and increase individuals' data sovereignty;

(III) reduce friction to the interoperability of digital systems;

(IV) increase the accessibility, auditability, security, efficiency, and transparency of digital services;

(V) increase market competition in the provision of digital services;

(VI) enable dynamic contracting and contract execution through smart contracts;

(VII) enable participants to collaborate in trustless and disintermediated environments;

(VIII) enable the operations and governance of distributed organizations;

(IX) create new ownership models for digital items; and

(X) increase participation of populations historically underrepresented in the technology, business, and financial sectors.

(ii) In consideration of the potential risks of applications of distributed ledger technologies under clause (i), the Director shall take into account, where applicable—

(I) additional risks that may emerge from distributed ledger technologies, as identified in reports submitted to the President pursuant to Executive Order 14067, that may be addressed by research and development;

(II) software vulnerabilities in distributed ledger technologies and smart contracts;

(III) limited consumer literacy on engaging with applications of distributed ledger technologies in a secure way;

(IV) the use of distributed ledger technologies in illicit finance and their use in combating illicit finance;

(V) manipulative, deceptive, and fraudulent practices that harm consumers

engaging with applications of distributed ledger technologies;

(VI) the implications of different consensus mechanisms for digital ledgers and governance and accountability mechanisms for applications of distributed ledger technologies, which may include decentralized networks;

(VII) foreign activities in the development and deployment of distributed ledger technologies and their associated tools and infrastructure; and

(VIII) environmental, sustainability, and economic impacts of the computational resources required for distributed ledger technologies.

(C) Potential uses for distributed ledger technologies that could improve the operations and delivery of services by Federal agencies, taking into account the potential of digital ledger technologies to—

(i) improve the efficiency and effectiveness of privacy-preserving data sharing among Federal agencies and with State, local, territorial, and Tribal governments;

(ii) promote government transparency by improving data sharing with the public;

(iii) introduce or mitigate risks that may threaten individuals' rights or broad access to Federal services;

(iv) automate and modernize processes for assessing and ensuring regulatory compliance; and

(v) facilitate broad access to financial services for underserved and underbanked populations.

(D) Ways to support public and private sector dialogue on areas of research that could enhance the efficiency, scalability, interoperability, security, and privacy of applications using distributed ledger technologies.

(E) The need for increased coordination of the public and private sectors on the development of voluntary standards in order to promote research and development, including standards regarding security, smart contracts, cryptographic protocols, virtual routing and forwarding, interoperability, zero-knowledge proofs, and privacy, for distributed ledger technologies and their applications.

(F) Applications of distributed ledger technologies that could positively benefit society but that receive relatively little private sector investment.

(G) The United States position in global leadership and competitiveness across research, development, and deployment of distributed ledger technologies.

(2) CONSULTATION.—

(A) IN GENERAL.—In carrying out the Director's duties under this subsection, the Director shall consult with the following:

(i) Private industry.

(ii) Institutions of higher education, including minority-serving institutions.

(iii) Nonprofit organizations, including foundations dedicated to supporting distributed ledger technologies and their applications.

(iv) State governments.

(v) Such other persons as the Director considers appropriate.

(B) REPRESENTATION.—The Director shall ensure consultations with the following:

(i) Rural and urban stakeholders from across the Nation.

(ii) Small, medium, and large businesses.

(iii) Subject matter experts representing multiple industrial sectors.

(iv) A demographically diverse set of stakeholders.

(3) COORDINATION.—In carrying out this subsection, the Director shall, for purposes of avoiding duplication of activities, consult, cooperate, and coordinate with the programs and policies of other relevant Federal agencies, including the interagency process outlined in section 3 of Executive Order 14067 (87 Fed. Reg. 14143; relating ensuring responsible development of digital assets).

(4) NATIONAL STRATEGY.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the relevant congressional committees and the President a national strategy that includes the following:

(A) Priorities for the research and development of distributed ledger technologies and their applications.

(B) Plans to support public and private sector investment and partnerships in research and technology development for societally beneficial applications of distributed ledger technologies.

(C) Plans to mitigate the risks of distributed ledger technologies and their applications.

(D) An identification of additional resources, administrative action, or legislative action recommended to assist with the implementation of such strategy.

(5) RESEARCH AND DEVELOPMENT FUNDING.—The Director shall, as the Director considers necessary, consult with the Director of the Office of Management and Budget and with the heads of such other elements of the Executive Office of the President as the Director considers appropriate, to ensure that the recommendations and priorities with respect to research and development funding, as expressed in the national strategy developed under this subsection, are incorporated in the development of annual budget requests for Federal research agencies.

(c) DISTRIBUTED LEDGER TECHNOLOGY RESEARCH.—

(1) IN GENERAL.—The Director of the National Science Foundation shall make awards, on a competitive basis, to institutions of higher education, including minority-serving institutions, or nonprofit organizations (or consortia of such institutions or organizations) to support research, including interdisciplinary research, on distributed ledger technologies, their applications, and other issues that impact or are caused by distributed ledger technologies, which may include research on—

(A) the implications on trust, transparency, privacy, accessibility, accountability, and energy consumption of different consensus mechanisms and hardware choices, and approaches for addressing these implications;

(B) approaches for improving the security, privacy, resiliency, interoperability, performance, and scalability of distributed ledger technologies and their applications, which may include decentralized networks;

(C) approaches for identifying and addressing vulnerabilities and improving the performance and expressive power of smart contracts;

(D) the implications of quantum computing on applications of distributed ledger technologies, including long-term protection of sensitive information (such as medical or digital property), and techniques to address them;

(E) game theory, mechanism design, and economics underpinning and facilitating the operations and governance of decentralized networks enabled by distributed ledger technologies;

(F) the social behaviors of participants in decentralized networks enabled by distributed ledger technologies;

(G) human-centric design approaches to make distributed ledger technologies and their applications more usable and accessible;

(H) use cases for distributed ledger technologies across various industry sectors and government, including applications pertaining to—

(i) digital identity, including trusted identity and identity management;

(ii) digital property rights;

(iii) delivery of public services;

(iv) supply chain transparency;

(v) medical information management;

(vi) inclusive financial services;

(vii) community governance;

(viii) charitable giving;

(ix) public goods funding;

(x) digital credentials;

(xi) regulatory compliance;

(xii) infrastructure resilience, including against natural disasters; and

(xiii) peer-to-peer transactions; and

(I) the social, behavioral, and economic implications associated with the growth of applications of distributed ledger technologies, including decentralization in business, financial, and economic systems.

(2) ACCELERATING INNOVATION.—The Director of the National Science Foundation shall consider continuing to support startups that are in need of funding, would develop in and contribute to the economy of the United States, leverage distributed ledger technologies, have the potential to positively benefit society, and have the potential for commercial viability, through programs like the Small Business Innovation Research program, the Small Business Technology Transfer program, and, as appro-

priate, other programs that promote broad and diverse participation.

(3) CONSIDERATION OF NATIONAL DISTRIBUTED LEDGER TECHNOLOGY RESEARCH AND DEVELOPMENT STRATEGY.—In making awards under paragraph (1), the Director of the National Science Foundation shall take into account the national strategy, as described in subsection (b)(4).

(4) FUNDAMENTAL RESEARCH.—The Director of the National Science Foundation shall consider continuing to make awards supporting fundamental research in areas related to distributed ledger technologies and their applications, such as applied cryptography and distributed systems.

(d) DISTRIBUTED LEDGER TECHNOLOGY APPLIED RESEARCH PROJECT.—

(1) APPLIED RESEARCH PROJECT.—Subject to the availability of appropriations, the Director of the National Institute of Standards and Technology, may carry out an applied research project to study and demonstrate the potential benefits and unique capabilities of distributed ledger technologies.

(2) ACTIVITIES.—In carrying out the applied research project, the Director of the National Institute of Standards and Technology shall—

(A) identify potential applications of distributed ledger technologies, including those that could benefit activities at the Department of Commerce or at other Federal agencies, considering applications that could—

(i) improve the privacy and interoperability of digital identity and access management solutions;

(ii) increase the integrity and transparency of supply chains through the secure and limited sharing of relevant supplier information;

(iii) facilitate increased interoperability across healthcare information systems and consumer control over the movement of their medical data;

(iv) facilitate broader participation in distributed ledger technologies of populations historically underrepresented in technology, business, and financial sectors; or

(v) be of benefit to the public or private sectors, as determined by the Director in consultation with relevant stakeholders;

(B) solicit and provide the opportunity for public comment relevant to potential projects;

(C) consider, in the selection of a project, whether the project addresses a pressing need not already addressed by another organization or Federal agency;

(D) establish plans to mitigate potential risks, including those outlined in subsection (b)(1)(B)(ii), if applicable, of potential projects;

(E) produce an example solution leveraging distributed ledger technologies for 1 of the applications identified in subparagraph (A);

(F) hold a competitive process to select private sector partners, if they are engaged, to support the implementation of the example solution;

(G) consider hosting the project at the National Cybersecurity Center of Excellence; and

(H) ensure that cybersecurity best practices consistent with the Cybersecurity Framework of the National Institute of Standards and Technology are demonstrated in the project.

(3) BRIEFINGS TO CONGRESS.—Not later than 1 year after the date of enactment of this Act, the Director of the National Institute of Standards and

Technology shall offer a briefing to the relevant congressional committees on the progress and current findings from the project under this subsection.

(4) PUBLIC REPORT.—Not later than 12 months after the completion of the project under this subsection, the Director of the National Institute of Standards and Technology shall make public a report on the results and findings from the project.

Amendment to H.R. 7900

National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Wittman

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Evaluating advances in secure communication technologies

The committee recognizes the need to take advantage of technologies that might strengthen secure communications for the United States military. As the management of the radio frequency portion of the electromagnetic spectrum becomes more complex, the committee notes the importance of the Department of Defense investigating alternative methods of communication. The committee encourages the Department to evaluate the utility of light fidelity technologies to improve the security of the Department's communications and achieve other related efficiencies. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services no later than March 1, 2023, on how the Department of Defense is considering the potential benefits of light fidelity technology.

AMENDMENT TO H.R. 7900

OFFERED BY MS. SPEIER OF CALIFORNIA

At the appropriate place in title II, insert the following new section:

SEC. 2___. PILOT PROGRAM TO FACILITATE THE RESEARCH, DEVELOPMENT, AND PRODUCTION OF ADVANCED BATTERY TECHNOLOGIES FOR WARFIGHTERS.

(a) ESTABLISHMENT.—The Secretary of Defense shall carry out a pilot program to be known as the ''American Sustainable Battery Production Technologies Program'' (referred to in this section as the ''Program''). Under the Program, the Secretary shall seek to award assistance to eligible entities to facilitate the research, development, and production of electric battery technologies that may be useful for defense-related purposes.

(b) COORDINATION WITH RELATED PROGRAMS.—The Secretary of Defense shall ensure that activities under the Program are coordinated with—

(1) the Strategic Environmental Research and Development Program under section 2901 of title 10, United States Code; and

(2) the Department of Energy.

(c) PROGRAM ACTIVITIES.—Under the Program, the Secretary of Defense shall seek to award assistance to eligible entities—

(1) to conduct research and development into electric battery technologies and any associated manufacturing and production needs;

(2) to expand the battery recycling capabilities of the Department of Defense;

(3) to reduce the reliance of the Department of Defense on foreign competitors for critical materials and technologies, including rare earth materials; and

(4) to transition battery technologies, including technologies developed from other pilot programs, prototype projects, or other research and development programs, from the prototyping phase to production.

(d) FORM OF ASSISTANCE.—Assistance awarded to an eligible entity under the Program may consist of a grant, a contract, a cooperative agreement, other transaction, or such other form of assistance as the Secretary of Defense considers appropriate.

(e) PRIORITY CONSIDERATION.—In awarding assistance to eligible entities under the Program, the Secretary of Defense shall give priority to entities that—

(1) are located in and operate in the United States, including any manufacturing operations;

(2) are owned by a United States entity; and

(3) deploy North American-owned intellectual property and content.

(f) DATA COLLECTION.—The Secretary of Defense shall collect and analyze data on the Program for the purposes of—

(1) developing and sharing best practices for achieving the objectives of the Program;

(2) providing information to the Secretary on the implementation of the Program, and related policy issues; and

(3) reporting to the congressional defense committees in accordance with subsection (h).

(g) TERMINATION.—The Program shall terminate on the date that is six years after the date of the enactment of this Act.

(h) REPORTS.—

(1) ANNUAL REPORTS.—Not later than one year after the date of the enactment of this Act and annually thereafter until the date on which the Program terminates under subsection (g), the Secretary of Defense shall submit to the appropriate congressional committees a report on the use of funds under

the Program. Each report shall include the following:

(A) An explanation of whether and to what extent the assistance awarded to eligible entities under the Program met mission requirements during the period covered by the report, including—

(i) the value of the assistance awarded, including the value of each grant, contract, cooperative agreement, other transaction, or other form of assistance; and

(ii) a description of the research, technology, or capabilities funded with such assistance.

(B) A description of any research, technology, or capabilities being tested under the Program as of the date of the report together with an explanation of how the Secretary has applied, or expects to apply, such research, technology, or capabilities within the Department of Defense.

(2) FINAL REPORT.—Not later than one year after the date on which the Program terminates under subsection (g), the Secretary of Defense shall submit to the appropriate congressional committees

a final report on the results of the Program. Such report shall include—

(A) a summary of the objectives achieved by the Program; and

(B) recommendations regarding the steps that may be taken to promote battery technologies that are not dependent on foreign competitors to meet the needs of the Armed Forces.

(i) DEFINITIONS.—In this section:

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

(A) the congressional defense committees;

(B) the Committee on Energy and Commerce and the Committee on Science, Space, and Technology of the House of Representatives; and

(C) the Committee on Energy and Natural Resources and the Committee on Commerce, Science, and Transportation of the Senate.

(2) The term ''eligible entity'' means a battery producer or other entity involved in the battery production supply chain.

AMENDMENT TO H.R. 7900

OFFERED BY MR. FALLON OF TEXAS

At the appropriate place in title X, insert the following:

SEC. 10___. TARGET DATE FOR DEPLOYMENT OF 5G WIRELESS BROADBAND INFRASTRUCTURE AT ALL MILITARY INSTALLATIONS.

(a) TARGET REQUIRED.—The Secretary of Defense shall—

(1) establish a target date by which the Secretary plans to deploy 5G wireless broadband infrastructure at all military installations; and

(2) establish metrics, which shall be identical for each of the military departments, to measure progress toward reaching the target required by paragraph (1).

(b) ANNUAL REPORT.—The Secretary shall submit to the congressional defense committees and annual report that includes—

(1) the metrics in use pursuant to subsection (a)(2); and

(2) the progress of the Secretary in reaching the target required by subsection (a)(1).

(c) TERMINATION.—No report shall be required under subsection (b) after the date that is five years after the date of the enactment of this Act.

AMENDMENT TO H.R. 7900

OFFERED BY MR. BANKS OF INDIANA

At the appropriate place in title II, insert the following new section:

SEC. 2___. DEFENSE ADVANCED RESEARCH PROJECTS AGENCY INNOVATION FELLOWSHIP PROGRAM.

(a) IN GENERAL.—The Director of the Defense Advanced Research Projects Agency shall develop a plan for the establishment of a fellowship program (to be known as the ''Innovation Fellowship Program'') to expand opportunities for early career scientists to participate in the programs, projects, and other activities of the Agency.

(b) ELEMENTS.—In developing the plan under subsection (a), the Director of the Defense Advanced Research Projects Agency shall—

(1) review the programs, projects, and other activities of the Agency that are open to participation from early career scientists to identify opportunities for the expansion of such participation;

(2) conduct an assessment of the potential costs of the fellowship program described in subsection (a);

(3) establish detailed plans for the implementation of the fellowship program;

(4) define eligibility requirements for participants in the fellowship program;

(5) identify criteria for evaluating applicants to the fellowship program; and

(6) address such other matters as the Director determines appropriate.

(c) SUBMITTAL TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the Director of the Defense Advanced Research Projects Agency shall submit to the congressional defense committee a report that includes—

(1) the plan developed under subsection (a); and

(2) recommendations for expanding opportunities for early career scientists to participate in the programs, projects, and other activities of the Agency.

☒

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Banks

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

DARPA Graduate Student Funding

The committee recognizes that U.S. defense depends on the Department and the country having a vibrant, cutting-edge scientific and engineering enterprise. That, in turn, requires having a well-trained, innovative workforce that is regularly refreshed with diverse new talent. DARPA-funded research has many strengths, but DARPA projects are generally not well aligned with academic timelines with respect to graduate student funding. The committee believes that familiarizing graduate students with DARPA's unique approach to technology innovation will strengthen their talent pipeline.

The high-risk nature of DARPA work often requires failing programs to be terminated abruptly, which puts graduate student education at risk. DARPA has informal processes to support continued graduate student funding until alternate sources can be secured by the home university, but these are not legally binding and put students at significant risk, particularly when there are unexpected close out costs associated with a given program. DARPA's contracts office has a history of innovation in contracting, and there appear to be opportunities to codify student funding in contracts or grants, consistent with federal acquisition regulations, and thus stabilize student funding and minimize the burden on individual students.

Therefore, the committee directs the Director of DARPA to study and report to the House Committee on Armed Services on options for stabilizing graduate student funding against termination of DARPA projects. The report should identify current efforts to do this, proposals to provide formal (contractual) obligation of partial funding for student support upon termination of a project, and any barriers to execution of these proposals. It should make clear whether any additional authorities would be needed and cost estimates. DARPA shall provide the report to the committee no later than February 1, 2023.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mrs. Stephanie Bice

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Streamlining of Information Assurance and Cybersecurity Protocols in Defense Software Acquisitions

Congress notes that existing Information Assurance and Cybersecurity processes within the Department of Defense acquisition process often cause delays in software acquisition programs.

Accordingly, the committee directs the Undersecretary for Acquisition and Sustainment to provide a report that includes options to streamline the Information Assurance and Cyber Security approval processes for software acquisitions and submit such report to the House Committee on Armed Services by March 1, 2023.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Scott of Georgia

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Cybersecurity Activities with Georgia

The Republic of Georgia faces major regional security challenges, including extensive challenges in cyberspace. The committee expects the defense relationship between the United States and Georgia to continue to mature. To that end, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services, no later than March 1, 2023, on the last two years of DOD activities with Georgia on cyber-related matters. This briefing should describe activities by any and all components of DOD as relates to cyberspace, to include United States Cyber Command and United States European Command. Additionally, this briefing shall include potential recommendations and plans for future engagement with Georgia on cyber-related matters.

AMENDMENT TO H.R. 7900

OFFERED BY MR. MOULTON OF MASSACHUSETTS

At the appropriate place in title XV insert the following new section:

SEC. 15___. CONSISTENCY IN DELEGATION OF CERTAIN AUTHORITIES RELATING TO INFORMATION OPERATIONS.

Except as otherwise provided specifically by law, if any roles or responsibilities relating to information operations are assigned pursuant to a provision of law or by the direction of the Secretary of Defense to the Under Secretary of Defense for Policy, the Under Secretary shall ensure that such roles or responsibilities are assigned or otherwise delegated to the same position within the Office of the Under Secretary of Defense of Policy.

☒

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mrs. Stephanie Bice

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Briefing on Department of Defense Software Supply Chain Vulnerabilities

The Committee recognizes the importance of protection our software supply chain from attacks. It understands that trends show software supply chain attacks are increasing at an exponential rate of 4-5 times per year, with several thousand attacks in 2021. The Committee understands that the Department of Defense with support of Congress continues to address supply chain vulnerabilities but is concerned that the focus has been on material and hardware vice the software supply chain. Accordingly, the Committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services no later than March 1, 2023, on its efforts to identify and mitigate supply chain threats and vulnerabilities throughout the software supply chain, to include software as well as procedures and controls to ensure the security of that software supply chain.

AMENDMENT TO H.R. 7900

OFFERED BY MR. ROGERS OF ALABAMA

At the appropriate place in division E, insert the following:

SEC. ___. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

The National Cybersecurity Preparedness Consortium Act of 2021 (Public Law 117–122; 6 U.S.C. 652 note) is amended—

(1) in subsections (a) and (b), by striking ''The Secretary may work with one or more consortia'' each place it appears and inserting ''The Secretary shall work with not fewer than three consortia'';

(2) in subsection (c)—

(A) in the matter preceding paragraph (1), by striking ''In selecting a consortium'' and inserting ''In selecting the consortia''; and

(B) in paragraph (2), by striking ''Geographic diversity of the members of any such consortium'' and inserting ''Regional diversity of such consortia, and geographic diversity of the members of such consortia,''; and

(3) in subsection (d), by striking ''If the Secretary works with a consortium'' and inserting ''In working with the consortia''.

☒

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mrs. Bice of Oklahoma

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Cloud management software technology

The Committee supports the Department's decision to deploy a multi-cloud architecture. A multi-cloud approach aligns better with the Department's mission and offers many benefits including allowing for more comprehensive future innovations, easier data portability, increased resilience and security, and decreased stove-piping. The Committee directs the Chief Information Officer of the Department of Defense to provide a briefing the House Committee on Armed Services not later than March 31, 2023 on the strategy for future multi-cloud projects.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Horsford

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Enterprise Software Licenses

The committee is aware that a portion of the Department of Defense's workloads are dependent upon on the use of enterprise software licenses from software providers. The committee has observed how restrictive licensing practices can have the effect of limiting customer choice and increasing cost when customers are procuring one or more cloud services. These restrictive software licensing practices often apply to software widely adopted by the Department of Defense, and the committee is concerned that the Department of Defense may not have an accurate approach to accounting for the costs associated with restrictive licensing practices.

Therefore, the committee directs the Comptroller General of the United States to submit a report to the congressional defense committees not later than August 1, 2023, on the impact that restrictive software licenses could have on the Department of Defense as it transitions to cloud services and leverages innovation across multiple CSPs. Considerations as part of the Comptroller General's examination should include:

(1) the relationship between restrictive software licenses and cloud costs and choice;
(2) how the restrictive software licenses could affect different cloud architecture;
(3) what efforts the Department is taking to mitigate the potential impact of restrictive software licenses; and
(4) any additional matters the Comptroller General determines appropriate.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Panetta

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Information Operations for Modern Warfare Strategy

The committee recognizes the growing importance of effectively leveraging information operations. The committee is concerned that fractured and siloed information operations doctrine across the Department of Defense could obstruct the United States' ability to effectively deter competition, particularly below the threshold of armed conflict.

The committee seeks to ensure efficient resourcing, funding, training, specialization, and utilization of scarce information operations resources. To that end, the committee requests additional information as to whether changes to doctrine governing information operations could clarify roles and responsibilities within the Department. The committee therefore directs the Secretary of Defense, in consultation with the Principal Information Operations Advisor, to brief the House Committee on Armed Services not later than December 23, 2022, regarding:

(1) The feasibility and utility of adjustments to doctrine, roles, and responsibilities in the area of information operations;
(2) The utility of recategorizing information operations into operations in the information environment, special information operations which enable the joint and interagency force to tackle operations that occur in the grey zone or competition between the threshold of armed conflict; and long term public diplomacy
(3) Such other potential doctrinal changes as the Secretary deems appropriate; and
(4) The applicability of other organizational and doctrinal models, such as the Key West Agreement and the Intelligence Community.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Panetta of California

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Developing an Intellectual Property Strategy and Advancing the Innovation Ecosystem

The committee is aware of efforts by adversarial states to advance technology-based innovation as a key driver for their geopolitical power. The committee is therefore concerned that failure to foster a strong and resilient domestic innovation base could jeopardize our military technological superiority and our economic competitiveness. Therefore, the committee directs the Secretary of Defense, in coordination with the Under Secretary for Research and Engineering, to provide a report to the Committees on Armed Services not later than March 1, 2023 outlining an intellectual property strategy for the Department of Defense. The report should include:

(1) means to promote a robust innovation ecosystem, to include talent management; research infrastructure; joint experimentation; and inter-service, intra-governmental, and public-private collaboration;
(2) a description of additional means to protect intellectual property;
(3) an examination of the utility of intellectual property as a tool for strategic competition, cost imposition, and counter-malign activity;
(4) recommendations for changes to statute, regulations, or policies that would support the achievement of the goals set forth elsewhere in the report;
(5) an examination of the ability of modified approaches to intellectual property to address near-term, mid-term, and long-term capability gaps, with an emphasis on spurring innovation and mitigating the gap between the research and development of and the procurement and fielding of emerging capabilities and technologies; and
(6) an assessment of the ability of military education institutions and science and technology reinvention laboratories to encourage innovation and raise awareness of intellectual property related matters.

The committee further directs the Secretary of Defense to provide an interim briefing to the committee not later than December 23, 2022 providing a status update on the creation of the strategy outlined above.

AMENDMENT TO H.R. 7900

OFFERED BY MR. PANETTA OF CALIFORNIA

At the appropriate place in title XV, insert the following:

SEC. 15___. DEPARTMENT OF DEFENSE ENTERPRISE-WIDE PROCUREMENT OF CYBER DATA PRODUCTS AND SERVICES.

Section 1521 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81; 10 U.S.C. 2224 note) is amended—

(1) in subsection (a)(5), by inserting ‘‘, including the use of artificial intelligence-based endpoint security that prevents cyber attacks and does not require constant internet connectivity to function,’’ after ‘‘services’’; and

(2) in subsection (b), by inserting ‘‘, including by enhancing the security of the software supply chain of the Department’’ after ‘‘best interests of the Department’’.

☒

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. DesJarlais

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

DOD S&T Workforce

The committee believes the expansion of undergraduate and post-graduate scientific research participant appointments within the Department Science and Technology (S&T) ecosystem is foundational for the future of the Department.

Therefore, the committee directs the Under Secretary of Defense for Research and Engineering to report to the House Committee on Armed Services no later than December 31, 2022, an assessment of the resources, budget, needs and opportunities to expand S&T research participant appointments. The report should include initial strategies, opportunities, and approaches to such appointments, including outlining how existing Strategic Partnership Programs with other departments can be utilized to achieve this goal.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Golden of Maine

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Additive Manufacturing

The committee supports efforts within the Department to study and develop additive manufacturing and identify opportunities for large scale deployment. The committee believes that additive manufacturing has the potential to address existing supply chain and material challenges, and it may enhance expeditionary capabilities across operational environments.

Therefore the committee directs the Under Secretary of Defense Research and Engineering to brief the House Committee on Armed Services no later than December 31, 2022 on deploying large scale additive manufacturing. The briefing, at minimum, should address potential benefits of forward-deployed capabilities; technology readiness, including potential to address metal or metallic alloy forging and casting needs for the Department of Defense; and actions needed to support the industrial base.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Morelle of New York

In the appropriate place in the report to accompany H.R. 7900 insert the following new Directive Report Language:

Infrastructure Modernization for the Department of Defense

The Committee remains concerned about the Department of Defense's ability to have adequate infrastructure that can meet current and future data demands. To succeed in modern warfare, the Department will require sufficient bandwidth and capacity, necessitating sustained investment for persistent modernization. To date, much of this work has occurred through the Army's Installation Information Infrastructure Modernization (I3MP) effort. The committee is encouraged that the Department is taking steps to enable new data architecture requirements into its facility criteria. The Committee recognizes that the current unified facilities criteria (UFC) for design and construction of facilities does not inhibit utilization of new data architecture requirements into facilities. The committee encourages the Department and the military services to continue prioritizing its infrastructure modernization program and ensure whole-of-department efforts are synchronized to the maximum extent practicable. To this end, the Committee directs the Secretary of the Army to provide a briefing to the House Committee on Armed Services by April 1, 2023, detailing the Department of the Army's data infrastructure modernization efforts.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Moore

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Military Installation Innovation Projects

The committee is aware of the need to accelerate adoption of emerging technology in order to strengthen the national defense innovation base and meet the demands of near-peer competition. The committee encourages collaboration with non-traditional small businesses, startups and venture-backed scaleups, and believes that such efforts can accelerate and strengthen innovation and adoption across the Department of Defense. To this end, the committee supports empowering military leaders with direct responsibility for mission outcomes that have the potential to be improved by rapidly development and deployment of innovative technologies.

Therefore, the committee directs the Secretary of Defense to submit a report to the House Committee on Armed Services, not later than March 1, 2023, identifying opportunity areas for further collaboration between military leadership at the installation level and non-traditional small businesses, startups, and venture-backed startups and scaleups. This briefing should include recommendations addressing the utility, feasibility, and cost of establishing a pilot program designed to enable military leadership at the installation level to adopt emerging technology.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mrs. Bice of Oklahoma

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Counter UAS Technology Research

The Committee supports the Army's investment in advanced technologies to mitigate threats from Unmanned Aircraft Systems (UAS), especially as these threats emerge and mature rapidly. The Committee encourages the Army Research Lab to partner with academic institutions and private industry to further develop commercially available counter UAS technology.

The Committee directs the Commander of U.S. Army Futures Command to provide a briefing to the House Armed Services Committee no later than December 31, 2022 on opportunities to partner with academia and industry in counter-UAS research.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Golden of Maine

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Gesture Control Technology Standards

The committee recognizes that advancements in gesture control technologies have a wide array of potential applications across Department of Defense activities.

The committee recognizes that the development and implementation of consistent standards and requirements for gesture control technology has the potential to reduce administrative redundancy and overlap, and may aid in advancing gesture control technology platforms to conventional forces more quickly and efficiently.

Therefore, the committee directs the Secretary of Defense to provide a report to the House Committee on Armed Services by December 31, 2022, on implementing uniform standards and requirements regarding the deployment of gesture control technology.

The report should include, at a minimum:

1. The department's projected timeline for the integration of wearable gesture control technology, the offices and agencies best suited to foster development, funding, and sustainment, and the scope of gesture control interoperability in military technology, namely unmanned systems, digital interfaces, and communications systems.

2. A potential acquisition strategy for wearable gesture control, including an estimate of the average production unit cost, and a schedule for full-rate production listed in paragraph one.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Moore

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Small Business Innovation Research Improvements

The committee recognizes the significant impact of the Small Business Innovation Research (SBIR) program and encourages the Department of Defense to continue stimulating technological innovation to meet the robust research and development needs of the warfighter. The committee recognizes the success of the SBIR program, and the notable contributions made through harnessing the creativity and innovation of small business owners in science, aerospace and defense. The committee acknowledges that in an era of rapidly developing and emergent technologies, fully utilizing the innovative might of American small businesses is central to maintaining superiority over peer competition. Therefore, the committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Office of Small Business Programs to provide a briefing to the House Committee on Armed Services, not later than March 1, 2023 on the utility, benefit and impact of increasing SBIR investment as part of the Department's research and development efforts. The briefing should include the impact of increasing SBIR funding as part of the Department's research and development budget, increases to the amount of Phase I and II awards, shortening the time from SBIR Phase 1 proposal submission to contract award, and setting a limit for the number of SBIR Phase 1 topics issued annually.

AMENDMENT TO H.R. 7900

OFFERED BY MR. CROW OF COLORADO

At the appropriate place in title XV, insert the following:

SEC. 15___. ASSESSMENT AND OPTIMIZATION OF DEPARTMENT OF DEFENSE INFORMATION OPERATIONS WITHIN THE CYBER DOMAIN.

(a) ASSESSMENT AND PLAN.—Not later than 90 days after the date of the enactment of this Act, the Principal Information Operations Advisor and the Principal Cyber Advisor to the Secretary of Defense, in coordination with the Commander of the United States Cyber Command, shall complete both an assessment and an optimization plan for integrating all information and influence operations within cyberspace across the Department of Defense.

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

(1) An inventory of the components of the Department of Defense conducting information and influence operations within cyberspace.

(2) An examination of sufficiency of resources allocated for information and influence operations within cyberspace.

(3) An evaluation of the command and control, oversight, and management of matters related to information and influence operations within cyberspace across the Office of the Secretary of Defense and the Joint Staff.

(4) Any other matters determined relevant by the Principal Information Operations Advisor and the Principal Cyber Advisor to the Secretary of Defense, in coordination with the Commander of the United States Cyber Command.

(c) OPTIMIZATION PLAN.—The optimization plan under subsection (a) shall include the following:

(1) Actions that the Department will implement to integrate all Department information and influence operations within cyberspace in a manner that ensures the proper level of visibility, unity of effort, synchronization, and deconfliction.

(2) Coordination procedures within the Department to ensure that coordination with the Commander of the United States Cyber Command takes place with regard to unity of effort, synchronization,

deconfliction of information and influence operations within cyberspace.

(3) An evaluation of potential organizational changes required to optimize information and influence operations within cyberspace.

(4) Any other matters determined relevant by the Principal Information Operations Advisor and the Principal Cyber Advisor to the Secretary of Defense, in coordination with the Commander of the United States Cyber Command.

(d) BRIEFINGS.—Not later than 30 days after completing the assessment and optimization plan under subsection (a), the Principal Information Operations Advisor and the Principal Cyber Advisor to the Secretary of Defense, in coordination with the Commander of the United States Cyber Command, shall provide to the congressional defense committees a briefing on the assessment and plan.

(e) IMPLEMENTATION.—Not later than 180 days after the date on which the briefing is provided under subsection (d), the Secretary of Defense shall implement the optimization plan under subsection (a).

AMENDMENT TO H.R. 7900

OFFERED BY MR. CROW OF COLORADO

At the appropriate place in title XV, insert the following:

SEC. 15___. CYBERSECURITY OF MILITARY STANDARDS FOR DATA.

(a) IN GENERAL.—No later than 270 days after enactment of this act, the principal staff assistant designated with primary responsibility for the Strategic Cybersecurity Program of the Department of Defense pursuant to paragraph (2) of section 1640(c) of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2224 note), as amended by [section 1502] of this Act, shall conduct a comprehensive review of Military Standard 1553 (in this section referred to as ''MIL–STD–1553''). At the discretion of the Secretary of Defense, the review required under this subsection may include reviews of additional serial data standards beyond MIL–STD–1553.

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

(1) An identification of programs and weapon systems currently employing MIL–STD–1553 and

other serial data standards, as appropriate, across the Department of Defense, the military departments, and components, with notations for any programs previously assessed by the Strategic Cybersecurity Program.

(2) An evaluation of, and inventory for, the vulnerabilities to MIL–STD–1553 and other serial data standards, as appropriate.

(3) An inventory of potential commercial- and Government-sourced mitigations and solutions, either in use or available to program offices.

(4) An assessment of potential changes to address identified vulnerabilities to MIL–STD–1553 and other serial data standards, as appropriate.

(c) DETERMINATION.—Based on the findings of the review required under subsection (a), the Secretary of Defense shall determine whether to revise or update MIL–STD–1553 and other serial data standards, as appropriate.

(d) GUIDANCE.—Subsequent to the completion of the review required under subsection (a), the head of the Strategic Cybersecurity Program shall issue guidance across the Department for program managers involved in procuring weapon systems that use MIL–STD–1553 and other serial data standards, as appropriate. The guidance

shall include information related to the potential threats to MIL–STD–1553, available mitigations and solutions, and technical resources for program managers to use in addressing issues with MIL–STD–1553 and other data serial standards, as appropriate.

(e) COMPLIANCE CERTIFICATION.—Subject to the findings for the review required under subsection (a), the senior official identified pursuant to section 1647(j) of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92) for a military department and the service acquisition executive (as such term is defined in section 101(10) of title 10, United States Code) shall, if applicable, issue a certification that mitigations identified by the Strategic Cybersecurity Program for assessed weapons systems have been applied and corrected. Not later than one year after the date of the enactment of this Act, such senior official and the service acquisition executive shall submit to the congressional defense committees such assessment.

(f) TEST AND EVALUATION.—The Director of Operational Test and Evaluation may include evaluations of MIL–STD–1553 and other serial data standards, as appropriate, in reports required to be provided to the congressional defense committees pursuant to law.

(g) REPORT.—Not later than 45 days after completion of the review required under subsection (a), the head of the Strategic Cybersecurity Program shall submit to the congressional defense committees—

(1) a report on the review required under subsection (a); and

(2) a copy of the guidance required under subsection (d).

☒

AMENDMENT TO H.R. 7900

OFFERED BY MS. GARCIA OF TEXAS

At the appropriate place in division E, insert the following:

SEC. ___. REVIEW OF CYBER-RELATED MATTERS AT THE DEPARTMENT OF THE TREASURY.

(a) IN GENERAL.—No later than 270 days after the date of enactment of this Act, the Secretary of the Treasury shall complete a comprehensive review of the Department of the Treasury's efforts dedicated to enhancing cybersecurity capability, readiness, and resilience of the financial services sector, specifically as it relates to—

(1) Treasury's role as the sector risk management agency for the financial services sector, as defined by section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021; and

(2) integration of operational resilience and cybersecurity for the financial services sector across the Department of the Treasury.

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

(1) A comprehensive review of the components and offices within the Departmental Offices of the Department of the Treasury involved in efforts specified in subsection (a).

(2) A review of activities by the Department of the Treasury involved in efforts specified in subsection (a).

(3) An assessment of the how each activity identified in this subsection connects to the National Security Strategy and other related documents of the Executive Branch.

(4) An assessment of the Department of the Treasury's ability to discharge fully its duties specified in subsection (a) and identify any areas where it may need additional resources, legislation or authority.

(5) An evaluation of the partnerships with other executive branch departments and agencies to support efforts specified in subsection (a).

(6) An evaluation of support to and from the Financial and Banking Information Infrastructure Committee, and its member agencies to enhance efforts specified in subsection (a).

(7) A five-year plan for the Department of the Treasury that defines an objectives and goals related to the efforts specified in subsection (a).

(c) SUBMISSION TO CONGRESS.—No later than 30 days after the completion of the review specified under subsection (a), the Secretary of the Treasury shall transmit the review to Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate.

(d) ANNUAL UPDATE.—No later than February 1st of each year after the submission of the review until 2028, the Secretary shall provide an update on progress made in the preceding year in relation to the plan directed in subsection (b)(7) to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate.

Amendment to H.R. 7900
National Defense Authorization Act for Fiscal Year 2023

Offered by: Mr. Banks

In the appropriate place in the report to accompany H.R. 7900, insert the following new Directive Report Language:

Advanced Combustion Collaboration

The Committee is encouraged by the US Naval Research Laboratory's continued study and development of rotating detonation combustion technologies. This advanced form of combustion offers significant advantages in both fuel efficiency and system size compared with current gas turbine architectures. The Committee is also aware that the Department of Energy is currently undertaking activities to integrate a rotating detonation combustor with an existing Navy inventory T63 powerplant.

The Committee directs the US Naval Research Laboratory to collaborate with the Department of Energy, along with academic and industry participants, to inform the integration and demonstration of this system to optimize dual-use applicability of the resulting system for both civilian and defense applications. This effort should be accompanied by an assessment of Navy systems that could utilize a 500kw generator of this type—to include ship power, expeditionary power, directed energy systems and high Mach devices. The Committee directs the Assistant Secretary of the Navy for Research, Development to brief the House Committee on Armed Services by June 30, 2023 on the results of this assessment and plans to integrate rotating detonation technology more broadly into Navy systems.