LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
5748	1	DesJarlais, Scott	CIT	DRL on Turbine Based Combine Cycle facilities at AFB	EB 1
5755	1	Crank, Jeff	CIT	Directs DoD to submit a modernization roadmap for the Commercial Solutions for Classified (CSfC) program	EB 1
5769	1	Finstad, Brad	CIT	The proposal supports inclusion of report language recognizing growing sophistication, scale, and velocity of malicious cyber activity directed against Department of Defense networks, systems, operational technology, and critical defense infrastructure.	EB 1
5776	1	Scott, Austin	CIT	This amendment would require a strategy to strengthen domestic production of advanced military prosthetic technologies critical to wounded service member recovery.	EB 1
5786	1	McCormick, Richard	CIT	Directs the Army to establish a three-year pilot program on the use of automated data security posture management technologies to protect the Army's artificial intelligence systems.	EB 1
5804	1	Gooden, Lance	CIT	Spectrum Sharing with Adaptive and Reconfigurable Technology	EB 1
5817	2	Carbajal, Salud O.	CIT	This DRL directs DoD to assess how it will securely deploy code and modernize vulnerable legacy software amid growing AI-enabled cyber threats.	EB 1
5906	1	Kiggans, Jennifer A.	CIT	This DRL directs the Under Secretary of Defense for Research and Engineering to submit a report to HASC/SASC not later than December 1, 2026, on opportunities to expand or adapt existing Department STEM initiatives to better identify and accelerate top-tier K-12 STEM talent.	EB 1
5911	1	Turner, Michael	CIT	Directs the Assistant SecDef for Mission Capabilitis to provide briefing by 1 December 2026 on the applicability of NITRO and required funding/authorities for NITRO.	EB 1
5958	1	Jackson, Ronny	CIT	Directs a briefing on the Department’s plan to evaluate, transition, and adopt AI-enabled assistive technologies for air crew.	EB 1
5965	0	Tokuda, Jill N.	CIT	Briefing on Air Force cyber defense pilot program, including options to scale the program and identification of additional authorities and agreements needed to improve cyber defense on U.S. and foreign territory and on and off installations.	EB 1
5973	1	Jackson, Ronny	CIT	Authorizes a pilot program to evaluate commercially available technologies that strengthen authentication and attribution of human authorization for consequential actions in order to improve the cybersecurity and physical security posture of the Department.	EB 1
5980	1	Crank, Jeff	CIT	Directs the CIO to brief on the status of the ongoing CMMC program review	EB 1

LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
6022	1	Kelly, Trent	CIT	Directs a briefing on efforts to improve digital hygiene training and cybersecurity readiness for National Guard and Reserve personnel.	EB 1
6028	1	Kelly, Trent	CIT	Directs a briefing on expanding classified software delivery using commercial development practices, cleared engineering teams, and streamlined acquisition pathways.	EB 1
6031	1	Wittman, Robert	CIT	Requires a report on scaling adoption of bring-your-own-device remote access capabilities across the National Guard Bureau.	EB 1
6062	2	Gooden, Lance	CIT	Communications Systems Electronic Warfare Resiliency Standards	EB 1
6070	1	Houlahan, Chrissy	CIT	Leveraging Emerging Biotechnology to Improve Resilience through Biomonitoring	EB 1
6094	2	Stefanik, Elise	CIT	Deployment and Scaling of Quantum Network: Directs the Department of Defense to report on efforts to deploy and scale quantum networking infrastructure to support post-quantum cybersecurity, and future quantum computing capabilities across Department networks.	EB 1
6099	2	Gooden, Lance	CIT	Report on the Adoption of AI-enabled VTOL Platforms	EB 1
6104	1	Davis, Donald G.	CIT	This provision directs the Air Force to deploy AI-enabled maintenance data cleansing and correction tools across Air Education and Training Command to improve the quality and usability of maintenance and logistics data. Request adapted from Leg Proposal#27221.	EB 1
6106	3	Kiggans, Jennifer A.	CIT	This DRL directs DoD to evaluate advanced thermo-conventional warhead effects for Blackbeard-GL and MACE missile programs, including reactive materials, AI-enabled modeling, affordability, and production scalability, with a briefing to Congress by December 1, 2026.	EB 1
6118	0	McCormick, Richard	CIT	Directs the Secretary of Defense in coordination with CDAO to provide a briefing to the committee on its use of open-weight AI models, plans for further adoption, and its views on open-weight models' relevance to military applications.	EB 1
6135	2	Vindman, Eugene Simon	CIT	Inclusion of critical infrastructure and operational technology in combatant command planning exercises.	EB 1
6158	1	Kiggans, Jennifer A.	CIT	This DRL directs SecDef, DirNSA, and DirNIST to submit a report to HASC/SASC by March 1, 2027, containing a roadmap for reducing memory management vulnerabilities across Department of Defense software systems.	EB 1
6176	2	Bacon, Don	CIT	Assessment of location assurance technologies, including those leveraging independent local physical evidence and environmental sensors to verify and authenticate a device’s claimed location	EB 1

LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
6179	0	Fallon, Pat	CIT	Would require the Secretary of Defense to report to the congressional defense committees on Department of Defense readiness to transition to quantum-resistant cryptographic standards, including a migration plan for all National Security Systems.	EB 1
6187	0	Messmer, Mark B.	CIT	Require a report on the organizational modernization of Electromagnetic Spectrum Operations (EMSO).	EB 1
6223	1	McGuire, John J.	CIT	Directs OSW to brief HASC on the security of DoW telecommunications networks and risks from partner security forces using high-risk telecommunications equipment.	EB 1
6238	1	McGuire, John J.	CIT	Directs CDAO to provide HASC with a brief on the state of commercial weather and environmental data acquisition across the DoD. The brief will cover unmet data requirements, acquisition timelines, and government data ownership challenges.	EB 1
6243	0	McGuire, John J.	CIT	Directs a report to HASC detailing plans for institutionalizing digital engineering and product lifecycle management throughout all current and future defense programs and platforms.	EB 1
6264	0	Jackson, Ronny	CIT	Directs a report on the Department's plan to establish a National Security and Defense Artificial Intelligence Institute consistent with Section 224 of P.L. 119-60.	EB 1
6267	1	Vasquez, Gabe	CIT	This direct report language would ask for a briefing from the Test Resource Management Center on weapon system survivability in combined environments	EB 1
6292	1	Khanna, Ro	CIT	Would direct the CDAO to submit a report to Congress detailing mechanisms for gathering workforce input during and after AI systems deployment.	EB 1
6322	0	Sorensen, Eric	CIT	Requires a briefing on the foreign weather modifications capabilities of our adversaries and allies, as well as recommendations on how DoD could bolster our own capabilities.	EB 1
6374	0	Whitesides, George	CIT	Directs the Air Force and Defense Intelligence Agency to evaluate the feasibility of establishing a program to detect and assess activities that may modify natural atmospheric processes.	EB 1
6379	0	Wittman, Robert	CIT	Requires a report on Department activities to develop and scale software sustainment best practices.	EB 1
6439	1	Elfreth, Sarah	CIT	A report on the Department of Defense's efforts to develop, evaluate, and transition biochemical sensing technologies to detect physiological biomarkers and external environmental threats.	EB 1
6443	0	Jackson, Ronny	CIT	Requires a biannual report on the adaptation cycles of the DAWG.	EB 1

LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
6449	2	Vindman, Eugene Simon	CIT	Asset Visibility and Discovery in the United States Indo-Pacific Command Area of Responsibility	EB 1
6452	0	Bacon, Don	CIT	Secretary of Defense shall issue Department of Defense-wide guidance for the identification of covered artificial intelligence companies and processes for the exclusion and removal of artificial intelligence developed by such companies from systems and devices	EB 1
6470	1	Jackson, Ronny	CIT	Directs a briefing on expanding and modernizing the Navy's SHARKCAGE program to bridge the visibility gap between shipboard enterprise networks and mission-essential industrial control systems through a unified IT and OT defense architecture.	EB 1
6473	0	Wittman, Robert	CIT	Amends how product support managers develop, update, and implement life-cycle sustainment plans by adding software sustainment frameworks and directing them to leverage software-enabled solutions.	EB 1
6496	1	Fallon, Pat	CIT	Would require the Commander of United States Cyber Command to brief HASC on the implementation plan, timeline, and resource requirements necessary to achieve full deployment of the IOM program's security automation capabilities and enterprise-wide coverage of the DODIN.	EB 1
6498	2	Vindman, Eugene Simon	CIT	Integrating AI-Enabled Advanced Manufacturing to Expand Missile Production	EB 1
6503	1	Bacon, Don	CIT	Develop and implement a streamlined, risk-informed, controlled evaluation framework to enable faster assessment of emerging cryptographic approaches	EB 1
6520	1	Fallon, Pat	CIT	Requires the Secretary of Defense, via the DoD CIO and the Commander of the Defense Cyber Defense Command, to submit semiannual reports on the implementation and findings of the Cyber Operational Readiness Assessment (CORA) program. Terminates after 3 years.	EB 1
6541	5	Vindman, Eugene Simon	CIT	Report on Efforts to Counter Transnational Cyber Fraud	EB 1
6555	2	Bergman, Jack	CIT	Artificial Intelligence–Enabled Systems for Software-Defined Hardware and Phased Array Systems	EB 1
6567	1	Wilson, Joe	CIT	Quantum-Enabled Radar Synchronization	EB 1
6595	1	Jacobs, Sara	CIT	Preserves existing human command responsibility for the use of force involving autonomous systems or AI-enabled systems, including procedures to identify responsible human commanders or operators.	EB 1
6600	1	Jacobs, Sara	CIT	Promotes effective use of AI-enabled systems by requiring human training to reduce overconfidence in such systems as part of operational testing, evaluation, and training under Sec. 1513.	EB 1

LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
6602	1	Wittman, Robert	CIT	Requires a briefing from the Navy on its compliance with the cybersecurity requirements for telecommunications systems established in section 1511 of the FY26 NDAA.	EB 1
6657	1	Jacobs, Sara	CIT	Clarifies that the incident and vulnerability reporting program should capture human-AI interface failures, including inappropriate reliance on AI outputs.	EB 1
6663	1	Jacobs, Sara	CIT	Requires common definitions or categories for AI systems deployed on Department enterprise AI platforms, including systems with agentic capabilities, to support acquisition clarity, testing, authorization, and operational adoption.	EB 1
6665	2	Khanna, Ro	CIT	Amends Artificial Intelligence (AI) incident and vulnerability reporting program to include concerning behavior related to AI control.	EB 1
6696	1	Elfreth, Sarah	CIT	Navy Digital Engineering Interoperability. Briefing on the Navy's strategy to establish an interoperable digital engineering infrastructure capable of supporting secure collaboration, data exchange, and vendor-neutral modeling.	EB 1
6703	1	Khanna, Ro	CIT	Directs the Secretary of Defense to carry out a pilot program to support the establishment of cloud laboratories at the Department of Defense.	EB 1
6742	0	Khanna, Ro	CIT	Directs the Secretary of Defense to submit a report on the feasibility of requiring bills of materials for defense acquisition.	EB 1
6755	1	DesJarlais, Scott	CIT	Amends Section 211 to include developmental test and evaluation	EB 1
6773	1	Conaway, Herb	CIT	Directs a briefing on the Department's strategy for mission partner identity verification	EB 1
6782	0	Bacon, Don	CIT	Establish a central dashboard to monitor and track Research, Development, Test, and Evaluation facility data related to military construction planning, design, and execution metrics across the military departments	EB 1
6821	0	Whitesides, George	CIT	Amends Sec. 1501 to add a requirement in annual reporting to provide detail about any covered AI incident resulting in the loss of life or bodily harm to members of the armed services and to add to the definition of covered AI incident.	EB 1
6850	0	Fallon, Pat	CIT	Directs the Secretary of Defense to report to congressional defense committees by June 1, 2027, on DoD's ability to identify and reduce its internet-accessible attack surface.	EB 1
6851	0	Kelly, Trent	CIT	This directive would require the Secretary of Defense to brief the House Committee on Armed Services on the Department’s strategy to improve data readiness, interoperability, governance, and secure data sharing in support of artificial intelligence and advanced analytics.	EB 1

LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT

Amendment to H.R. 8800

Offered by: Mr. DesJarlais

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Report On Assessment of Turbine Based Combine Cycle Facilities at Arnold Air Force Base

The committee recognizes the importance of ensuring adequate testing facilities are available for the development and evaluation of Turbine Based Combine Cycle (TBCC) technologies as part of hypersonic air vehicle development activities. The committee recognizes the importance of dedicated facilities and personnel, such as those at Arnold Air Force Base, to ensuring the success of such activities. Therefore, the committee directs the Secretary of Defense to submit a report to the congressional defense committees no later than December 1, 2026, describing the hosting plan for TBCC test and evaluation capabilities. The report shall include:

(1) a description of infrastructure and testing constraints and efficiencies, human capital resources and limitations, and other risks and/or optimizations to the program;

(2) an assessment of the ability of Arnold Air Force Base and other testing centers to modernize facilities to meet the needs of a full-scale TBCC operational capability;

(3) estimates for required power and industrial utility usage, as well as risks associated with development of secured access, networks, and grids; and

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

Amendment to H.R. 8800

Offered by: Mr. Crank

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Modernization of Commercial Solutions for Classified Program

The committee believes that modernization of the Commercial Solutions for Classified (CSfC) program could enable more rapid adoption of secure commercial technologies, improve scalability and interoperability across National Security Systems, and better align the program with the Department's ongoing efforts to accelerate acquisition and fielding of systems handling classified data. The Committee further recognizes the importance of ensuring that CSfC policies support joint and coalition operations and are responsive to emerging technologies.

Therefore, the committee directs the Secretary of Defense, in coordination with the Director of the National Security Agency, to submit a briefing to the House Committee on Armed Services that details a modernization roadmap for the CSfC program not later than March 1, 2027, that includes the following:

(1) an assessment of the existing CsfC framework, including any structural and operational limitations within certification and validation processes;
(2) a plan to modernize CSfC governance, certification, and compliance mechanisms, including consideration of adoption of performance-based security criteria;
(3) a representative sample of mission areas in which CSfC-approved solutions have been deployed, including operational value provided; and
(4) an evaluation of NSA–DoD coordination mechanisms to ensure synchronization of CSfC policy.

Amendment to H.R. 8800

Offered by: MR. Finstad

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

AI-Enabled Defense Cyber Operations

The committee recognizes the growing sophistication and scale of malicious cyber activity directed against Department of Defense networks, systems, operational technology, and critical defense infrastructure. The committee further recognizes that advances in artificial intelligence, predictive analytics, adaptive cyber defense, and defensive deception technologies may enhance the Department's ability to identify, deter, and neutralize cyber threats before compromise or exfiltration occurs.

Accordingly, the committee directs the Under Secretary of Defense for Policy, in coordination with the Commander of United States Cyber Command, to provide a briefing to the House Committee on Armed Services not later than February 4, 2027, on the extent to which artificial intelligence-enabled, preemptive cybersecurity technologies have been or are planned to be incorporated into defensive cyber operations. The briefing should include:

(1) the types of artificial intelligence-enabled defensive cyber capabilities currently employed or under evaluation;

(2) the extent to which preemptive and adaptive defense mechanisms and defensive deception technologies are or will be utilized in operational environments;

(3) a description of the additive capability provided by such technologies;

(4) an assessment of the operational utility of technologies designed to mislead, detect, monitor, and disrupt malicious cyber actors prior to successful network compromise;

(5) any operational, legal, policy, acquisition, or workforce challenges associated with the deployment of such technologies; and

(6) recommendations for additional authorities, resources, or policy changes necessary to accelerate the secure adoption of preemptive cybersecurity capabilities across the Department.

Amendment to H.R. 8800

Offered by: Mr. Austin Scott of Georgia

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Advanced Military Prosthetic Technologies

The committee recognizes the importance of advanced prosthetic technologies in supporting wounded servicemembers, improving rehabilitation outcomes, and enhancing military medical readiness. The committee further notes the growing importance of domestic manufacturing capabilities for emerging technologies, including microprocessor-controlled prosthetics, neural-interface systems, advanced prosthetic manufacturing, and modular prosthetic systems.

Therefore, the committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Director of the Defense Health Agency, to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the Department's efforts to advance and field next-generation military prosthetic technologies.

The briefing shall include, at a minimum, the following:

(1) an assessment of current and future requirements for advanced military prosthetic technologies;

(2) an assessment of domestic industrial base capacity and supply chain risks associated with such technologies;

(3) opportunities to accelerate research, development, testing, and fielding of advanced prosthetic systems;

(4) the status of emerging technologies, including neural-interface and human-machine interface capabilities; and

(5) any recommendations for legislative action to strengthen domestic production and innovation in advanced military prosthetic technologies.

AMENDMENT TO H.R. 8800

OFFERED BY MR. MCCORMICK OF GEORGIA

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

SEC. 2___. PILOT PROGRAM ON THE USE OF AUTOMATED DATA SECURITY POSTURE MANAGEMENT TECHNOLOGIES FOR ARTIFICIAL INTELLIGENCE SYSTEMS.

(a) ESTABLSIHIMENT.—Not later than 90 days after the date of the enactment of this Act, the Secretary of the Army shall establish and commence implementation of a pilot program to evaluate the use of commercially available automated data security posture management technologies to enhance the cybersecurity, effectiveness, and reliability of artificial intelligence systems.

(b) ELEMENTS.—In carrying out pilot program under subsection (a) the Secretary of the Army shall—

(1) identify, select, and deploy at least one commercially available data security posture management technology platform that is capable of continuous, automated monitoring and assessment of artificial intelligence systems for security threats specific to such systems;

(2) designate at least one artificial intelligence system currently deployed by the Army to demonstrate the data security posture managed technology platform selected under paragraph (1);

(3) complete the demonstration described in paragraph (2);

(4) train relevant personnel on the deployment, maintenance, and data interpretation of the demonstrated data security posture management technology platform;

(5) evaluate the demonstrated data security posture management technologies—

(A) across the different tasks involved in development, deployment, storage, or hosting of components of such artificial intelligence system;

(B) to determine the ability of such technoogies to identify, mitigate and restore any corruption or malicious manipulation of the applications or data of such artificial intelligence system; and

(C) for compatibility and ease of adoption into the value chains of existing artificial intelligence systems of the Army;

(6) assess the feasibility of broader deployment of commercially available automated data security posture management technologies to improve the trustworthiness, resilience and integrity of artificial intelligence systems maintained by the Army.

(c) REPORTS.—

(1) PROGRESS REPORT.—Not later than 120 days after the date on which the Secretary of the Army commences the pilot program under subsection (a), and annually thereafter until the termination date specified un subsection (d), the Secretary of the Army shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the status of implementation and preliminary findings of the pilot program, including with respect to each element described in subsection (b).

(2) FINAL REPORT.—Not later than 180 days after the termination date specified in subsection (d), the Secretary of the Army shall submit to the Committees on Armed Services of the Senate and the House of Representatives a final report on the results of the pilot program. The report shall include—

(A) any recommendations of the Secretary with respect to the broader implementation commercially available automated data security posture management technologies to support artificial intelligence systems of the Army; and

(B) an assessment of the costs and benefits of such technologies.

(d) TERMINATION.—The pilot program under subsection (a) shall terminate on the date that is three years after the date on which the Secretary of the Army commences the pilot program.

☒

Amendment to H.R. 8800

Offered by: Mr. Gooden

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Spectrum Sharing with Adaptive and Reconfigurable Technology

The Committee understands that the many Department of Defense systems dependent upon access to the electromagnetic spectrum (EMS), including sensors and communications, face an ever-growing challenge from both increasing EMS congestion and the continuing evolution of electronic warfare technologies and techniques. The committee believes that EMS-dependent systems will need to be resilient against such challenges in order to prevent degraded or denied capabilities. The committee therefore notes the importance of the development of technologies and procedures to mitigate EMS challenges, including but not limited to advanced spectrum sharing and management technologies.

The committee report accompanying the National Defense Authorization Act for Fiscal Year 2024 (H. Rept. 118-125) required information be provided on Department efforts to advance spectrum use research, management, and sharing, as well as on planned investments in spectrum management tools and capabilities that are essential to the development and deployment of future spectrum capabilities. The Committee is thus concerned that, despite this effort, the Department has yet to make investments sufficient to yield and maintain improvements in EMS resiliency and management. The Committee therefore directs the Secretary of Defense to provide a report to the House Committee on Armed Services not later than February 1, 2027, on the Department's strategy, schedule, and estimated resource requirements for development and adoption of adaptable and reconfigurable spectrum sharing and management technologies. Such report shall include and, where appropriate, differentiate between the various users, use cases, and employed spectrum bands across the Department.

Amendment to H.R. 8800

Offered by: Mr. Carbajal

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

AI Code Assurance and Legacy Software Refactoring

The committee notes that advances in artificial intelligence (AI) are rapidly increasing the speed at which software vulnerabilities can be identified and exploited. The committee is encouraged by ongoing Department of Defense efforts related to software assurance, cyber resilience, and automated code modernization, but remains concerned that verification and assurance capabilities may not be scaling at the pace required to support rapid adoption of AI-enabled software development tools or to bring code assurance capabilities into operational use.

Therefore, the committee directs the Secretary of Defense to submit a report to the House Committee on Armed Services not later than March 1, 2027, on the Department's efforts to ensure the secure deployment of code and accelerate remediation of legacy software vulnerabilities. The report shall include:

(1) a review of software verification policies intended to ensure that code performs intended functions and does not introduce unintended vulnerabilities or behavioral changes;

(2) a representative review of testing, verification, and runtime monitoring tools used before and after deployment of code in operational systems;

(3) plans to accelerate refactoring of legacy software written in memory-unsafe programming languages, including efforts to validate the reliability of refactored code;

(4) recommendations on resources, authorities, acquisition policies, workforce needs, or industrial base constraints that could affect the Department's ability to address these challenges.

Amendment to H.R. 8800
Offered by: Mrs. KIGGANS OF VIRGINIA

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

National Security Science, Technology, Engineering, and Mathematics Talent Development

The committee is concerned that, at a time when technological superiority is increasingly central to national security, the United States appears to be underinvesting in the early identification and acceleration of high-potential science, technology, engineering, and mathematics (STEM) talent, including among gifted students in rural, underserved, military-connected, and economically disadvantaged communities. The committee is aware that many exceptionally capable students with strong aptitude in mathematics and science, including military dependents and students from Gold Star families, lack consistent access to advanced coursework, research opportunities, mentorship, competitions, and specialized enrichment programs due to geographic isolation, frequent relocations, limited school resources, or socioeconomic barriers, and as a result, the country risks excluding a significant portion of its domestic STEM talent base. The committee notes that a relatively small cohort of highly capable individuals disproportionately drives innovation in critical fields such as artificial intelligence, autonomy, advanced computing, biotechnology, and other emerging technologies relevant to the Department of Defense. The committee is concerned that the lack of a systematic approach to identifying and accelerating these students through advanced academic pathways beginning at the K-12 level could create a long-term talent gap and increase reliance on foreign-born expertise in critical technology areas.

The committee recognizes and supports the Department's recently established Joint K-12 STEM Education Initiative, which is intended to unify and coordinate the Department's STEM education and talent development efforts across the military departments and defense agencies. The committee believes this effort can strengthen the national security STEM talent pipeline, improve efficiency and performance tracking, and better align existing programs, including STARBASE, the Science, Mathematics, and Research for Transformation (SMART) Scholarship-for-Service Program, the Defense STEM Education Consortium (DSEC), and Department of Defense Education Activity (DoDEA) schools, to identify and accelerate high ability students. However, the committee notes that no existing Department program is currently designed with the primary mission of systematically identifying and accelerating the country's top K-12 STEM talent into elite STEM pathways. The committee emphasizes that expanded Department investment should focus not only on broad STEM outreach, but also on identifying and accelerating students performing at the highest levels in mathematics and science through rigorous coursework, enrichment, mentorship, and direct pathways into the national security workforce.

The committee directs the Under Secretary of Defense for Research and Engineering to submit a report to the congressional defense committees not later than December 1, 2026, on opportunities to expand or adapt existing Department STEM initiatives to better identify and accelerate top-tier K-12 STEM talent. The report should include the following:

(1) an evaluation of existing Department STEM education programs, including STARBASE, the SMART Scholarship-for-Service Program, DSEC, DoDEA schools, and the Joint K-12 STEM Education Initiative, with specific attention to their effectiveness in identifying and accelerating the highest-potential students, and an assessment of gaps in current programming for students in the top 1 percent of mathematical and scientific ability;
(2) a plan to refresh or expand Department programs to support early identification, acceleration, and enrichment of high-ability STEM students, including adoption of existing scalable models for nationwide implementation;
(3) an estimate of the funding, personnel, infrastructure, and partnership resources required to support expanded programming, including potential public-private partnerships with proven providers of K-12 advanced coursework, industry, national laboratories, and higher education institutions;
(4) recommendations to ensure that expanded programs effectively reach high-potential students from all backgrounds and communities through systematic universal identification and screening mechanisms designed to reduce barriers to participation;
(5) an analysis of how Department investment in early STEM talent development programs for top K-12 STEM students would strengthen the defense industrial base, reduce reliance on foreign talent in critical technology areas, and support long-term United States competitiveness in emerging technologies; and
(6) an assessment of the feasibility of the Department co-sponsoring and co-funding, in coordination with the National Science Foundation and other relevant agencies, initiatives beyond existing Department programs, including nationwide scholarship programs for top K-12 STEM students and accelerated high school-to-bachelor-to-STEM doctorate pathways and fellowships.

Amendment to H.R. 8800

Offered by: MR. TURNER

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Nationwide Integration of Time Resiliency for Operations (NITRO)

The committee is encouraged by ongoing efforts of the Air Force Research Laboratory in developing position, navigating and timing (PNT) capabilities. The committee notes the joint program with the National Guard, the Nationwide Integration of Time Resiliency for Operations (NITRO), provides an alternative to the global positioning system for operations of critical infrastructure supporting military operations.

Therefore, the committee directs the Assistant Secretary of Defense for Mission Capabilities to provide a briefing to the House Committee on Armed Services not later than December 1, 2026, on the applicability of NITRO as well as costs to fund ongoing operations, maintenance, and sustainment of the system.

Amendment to H.R. 8800

Offered by: Mr. Jackson of Texas

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

AI-Enabled Assistive Technology for Air Crews

The committee recognizes recent advancements in artificial intelligence (AI)-enabled assistive technologies for pilots, and notes the potential for such technologies to improve flight safety, operational effectiveness, and aircrew performance. The committee also notes that recent efforts by the Department of the Air Force and U.S. Special Operations Command demonstrated the potential for advisory and pilot-assist technologies to enhance situational awareness and decision-making without exercising direct aircraft control.

The committee believes such technologies could assist air crews without modifying certified flight-critical systems or requiring replacement of existing avionics, flight controls, or actuators. However, the committee is concerned that the Department of Defense has not established consistent, Department-wide approaches to requirements development, airworthiness coordination, cybersecurity, and acquisition pathways for such software-centric technologies.

Therefore, the committee directs the Secretary of Defense, in coordination with the Secretary of the Army, Secretary of the Navy, Secretary of the Air Force, and the Commander, U.S. Special Operations Command, to provide a briefing to the House Committee on Armed Services not later than February 1, 2027, on the Department's plan to evaluate, transition, and adopt AI-enabled assistive technologies for air crew. The briefing shall include, but is not limited to:

(1) identification of a senior official or organization designated to coordinate Department-wide policy, requirements development, airworthiness alignment, cybersecurity considerations, and governance such technologies;
(2) a description of the Department's current airworthiness approval processes applicable to these capabilities;
(3) a description of plans for evaluation, experimentation, or limited operational use of such technologies during fiscal years 2027 and 2028, a listing of the specific platforms and mission sets, and the criteria used to assess operational benefit, safety, and readiness impacts; and
(4) an overview of the Department's planned approach to sequencing and scaling such capabilities, including an analysis of the operational and cost benefits of software-centric solutions relative to more hardware-intensive direct aircraft control solutions.

Amendment to H.R. 8800

Offered by: Ms. Tokuda

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Air Force Infrastructure Cyber Defense Pilot Program

The committee is encouraged by the work of Pacific Air Forces through the Mission-Relevant Terrain – Cyber pilot program to improve the cyber defense of the infrastructure upon which military installations rely in the Indo-Pacific. To build upon the experience of the pilot program, the committee directs the Secretary of the Air Force, in consultation with Commander, U.S. Indo-Pacific Command, to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the following:

(1) options to scale the Pacific Air Forces pilot to the Department of the Air Force and to the combatant commands, beginning with U.S. Indo-Pacific Command, including required funding and support;

(2) identification of additional authorities and agreements necessary to improve the cyber defense and information sharing related to the infrastructure, such as water, power, and logistics, on both U.S. and foreign territory, on which military platforms rely in the Indo-Pacific; and

(3) identification of needed authorities for on-base cyber defense risk mitigation and for off-base cyber defense risk mitigation in foreign countries, in U.S. territories and states outside the continental United States, and within the continental United States.

AMENDMENT TO H.R. 8800

OFFERED BY MR. JACKSON OF TEXAS

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

SEC. 2___. PILOT PROGRAM ON TECHNOLOGIES TO STRENGTHEN AUTHENTICATION AND ATTRIBUTION OF HUMAN AUTHORIZATION FOR CONSEQUENTIAL ACTIONS.

(a) PILOT PROGRAM AUTHORIZED.—The Secretary of Defense may carry out a pilot program to evaluate commercially available technologies that strengthen authentication and attribution of human authorization for consequential actions in order to improve the cybersecurity and physical security posture of the Department of Defense.

(b) OBJECTIVES.—Under the pilot program, the Secretary of Defense shall evaluate technologies that—

(1) strengthen access controls for systems and physical areas of the Department of Defense; and

(2) can be integrated across various environments of the Department without requiring specialized hardware.

(c) COMENCEMENT AND DURATION.—If the Secretary of Defense exercises the authority to carry out the pilot program under subsection (a), the program shall—

(1) commence not later than 180 days after the date of the enactment of this Act; and

(2) terminate not later than one year after the date on which the program is commenced.

(d) REPORT.—Not later than March 1, 2028, the Secretary of Defense shall submit to the congressional defense committees a report that includes—

(1) a summary of the results of the pilot program under subsection (a); and

(2) recommendations regarding adoption the technologies evaluated under the program at a wider scale across the Department of Defense.

☒

Amendment to H.R. 8800

Offered by: Mr. Crank

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Cybersecurity Maturity Model Certification Program Reform

The committee recognizes the importance of the Cybersecurity Maturity Model Certification (CMMC) program in protecting sensitive defense information across the defense industrial base and notes the shift from self-attestation to third-party assessments was a meaningful step toward ensuring the integrity of cybersecurity standards.

However, the committee is concerned that the current structure of the CMMC program imposes excessive regulatory burdens that drive up costs for smaller defense contractors and deter new entrants into the defense industrial base. The committee is also concerned about the transparency of cost within the CMMC ecosystem, including fees charged by the Cyber AB and CMMC Third-Party Assessment Organizations (C3PAOs).

The committee is aware that the Department of Defense Chief Information Officer is conducting an ongoing review of the CMMC program. The committee is concerned that, without reform, the current program disproportionately disadvantages small businesses.

The committee directs the Chief Information Officer of the Department of Defense to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the following:

(1) planned efforts to reduce the compliance burden on small businesses, including whether small applicants require the same assessor team size or certification pathway as larger applicants;
(2) an assessment of whether the Department should develop standardized architectures or implementation templates to reduce CMMC compliance costs for defense contractors, particularly small and medium-sized businesses;
(3) planned efforts to increase assessor capacity, including barriers to entry for new assessors and C3PAOs, and whether assessors of limited or software-only environments could be exempted from Tier 3 background check requirements;
(4) a representative survey of the costs incurred by small, medium, and large companies to implement CMMC, disaggregated, to the extent

practicable, by assessment costs, Cyber AB fees, and the costs incurred to meet security requirements;

(5) an assessment of existing Department oversight and legal authorities applicable to the Cyber AB and C3PAOs, including any gaps;

(6) an overview of the fee structures and revenue sources associated with Cyber AB, including charges to entities participating in the CMMC ecosystem; and

(7) a summary of current and planned efforts to incorporate automation and artificial intelligence-enabled workflows to improve continuous cybersecurity compliance and reduce administrative burden.

Amendment to H.R. 8800

Offered by: Mr. Kelly

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

DIGITAL HYGIENE TRAINING AND CYBERSECURITY POSTURE OF NATIONAL GUARD AND RESERVE PERSONNEL

The committee recognizes the critical role National Guard and Reserve personnel play in supporting Department of Defense missions across the homeland and abroad. The committee further recognizes that the continued prevalence of credential theft, phishing, and related cyber threats requires sustained efforts to strengthen cybersecurity awareness and digital resilience across the total force.

The committee believes it is important to ensure that National Guard and Reserve personnel have access to effective digital hygiene training and cybersecurity resources consistent with the Department's broader zero trust and identity management efforts.

Accordingly, the committee directs the Secretary of Defense, in coordination with the Department of Defense Chief Information Officer and the Chief of the National Guard Bureau, to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on existing and planned efforts to strengthen digital hygiene training and cybersecurity posture across the National Guard and Reserve components. The briefing shall include the following:

(1) an assessment of the current state and effectiveness of digital hygiene training available to National Guard and Reserve personnel;

(2) an assessment of cyber risks to National Guard and Reserve personnel associated with credential compromise, phishing, and related threats;

(3) an evaluation of the feasibility and cost of expanding access to cybersecurity tools and services across the National Guard and Reserve Components; and

(4) recommendations to improve digital hygiene training and cybersecurity readiness across the Reserve Components, consistent with zero trust principles.

Amendment to H.R. 8800

Offered by: Mr. Kelly

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Rapid Classified Software Development Capabilities

The committee recognizes that the Department of Defense continues to face delays in developing and deploying operational software capabilities within classified environments due to lengthy acquisition timelines, clearance requirements, and limited access to experienced cleared software engineers. The committee notes the growing operational importance of commercially available software development models that leverage embedded and cleared engineering teams, sprint-based delivery methodologies, fixed-price task structures, and development conducted directly within existing classified environments.

The committee encourages the Department to prioritize acquisition pathways consistent with Executive Order 14265 and the Adaptive Acquisition Framework, including commercial solutions offerings, Other Transaction Authority agreements, and Software Acquisition Pathway authorities.

The committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on:

(1) the Department's implementation of Executive Order 14265 and software acquisition reform guidance as applied to classified software delivery and operational AI integration;

(2) remaining barriers associated with software acquisition timelines and cleared workforce constraints; and

(3) opportunities to leverage non-traditional defense contractors and commercially available software development practices.

Amendment to H.R. 8800
National Defense Authorization Act for Fiscal Year 2027

Offered by: Mr. Wittman

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Secure Bring-Your-Own-Device Access for the National Guard Bureau

The committee recognizes potential for improved mobile access solutions to enhance cybersecurity, reduce costs, and improve operational flexibility across geographically distributed units. The committee notes that the Department of the Army has transitioned to a software-based bring-your-own-device (BYOD) capability that enables remote access to enterprise resources from personal devices without storing or transmitting any government data on the device, thereby eliminating data-at-rest and data-in-transit outside the enterprise boundary. Such solutions have demonstrated significant cost savings by reducing reliance on government-furnished equipment (GFE) while protecting servicemember privacy and improving secure mobile access across the force. The committee believes that other elements of the Department of Defense, including the National Guard Bureau (NGB), should similarly consider the adoption of an enterprise-wide BYOD solution meeting these characteristics.

Therefore, the committee directs the Secretary of Defense, in coordination with the Chief of the National Guard Bureau, to provide a briefing to the House Committee on Armed Services not later than February 1, 2027, containing the following:

(1) a description of current NGB mobile access practices, including an analysis of compliance with Department-wide cybersecurity requirements and personal privacy standards;
(2) where applicable, an analysis of whether waivers for any existing non-compliant mobile access solutions should be restricted or phased out; and
(3) the feasibility, cost, operational, cybersecurity, and personal privacy impacts related to adoption of an enterprise wide, virtualized BYOD capability meeting the characteristics described above, including a cost comparison between procurement and subscription-based secure BYOD solutions.

Amendment to H.R. 8800

Offered by: Mr. Gooden

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Communications Systems Electronic Warfare Resiliency Standards

The committee remains concerned that, while Section 168 of the Fiscal Year 2020 National Defense Authorization Act (Public Law 116-92) restricted the obligation of funds for communications systems that do not incorporate specified resiliency features, the Department of Defense has not established clear definitions, performance criteria, or measurable thresholds for communications resiliency against electronic warfare threats, including jamming and geolocation, on a Department-wide basis. The committee notes that without independent evaluations of performance in contested electromagnetic environments, programs can assert capability despite limited effectiveness against these threats.

Therefore, the committee directs the Secretary of Defense to submit a report to the congressional defense committees not later than January 15, 2027, detailing standards, certification processes, and enforcement mechanisms as they relate specifically to the performance of communication systems in denied or degraded environments. This report shall include, at a minimum:

(1) the data and metrics used to assess system availability under specified jamming conditions;

(2) the methods used to verify and independently certify reductions in electromagnetic signature; and

(3) the testing standards applied by accredited Department of Defense testing facilities to evaluate performance against near-peer adversary electronic warfare threats.

AMENDMENT TO H.R. 8800

OFFERED BY MS. HOULAHAN OF PENNSYLVANIA

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

SEC. 28___. PILOT PROGRAM ON WASTEWATER MONITORING AND PATHOGEN-AGNOSTIC MONITORING SYSTEM OF CERTAIN MILITARY INSTALLATIONS.

(a) PILOT PROGRAM REQUIRED.—Not later than 180 days after the date of the enactment of this section, the Secretary of Defense shall carry out a pilot program under which the Secretary shall develop and implement a comprehensive wastewater monitoring system at not fewer than four military installations at which the Secretary seeks to identify the prevalence of infectious diseases among members of the Armed Forces at the installation (in this section referred to as the ''pilot program'').

(b) PATHOGEN-AGNOSTIC PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the Secretary shall carry out a second pilot program under which the Secretary shall develop and implement a pathogen-agnostic monitoring system that leverages

emerging biotechnologies for early detection of novel pathogens (in this section referred to as the ''pathogen-agnostic pilot program'').

(2) PURPOSES.—The purpose of the pathogen-agnostic pilot program shall aim be to—

(A) improve detection, identification, and analysis of infectious disease prevalence among members of the Armed Forces and other relevant Department of Defense personnel; and

(B) strengthen early-warning capabilities for novel pathogens.

(c) TECHNOLOGIES AND DATA SYSTEM USED.—In carrying out the pilot program under subsection (a), the Secretary shall ensure all systems developed and implemented under such subsection is comprised of appropriate technologies, standardized analytical tools, and a uniform data system.

(d) DURATION.—The pilot program shall be carried out during a two-year period beginning on the date of the commencement of the pilot program and the pathogen-agnostic pilot program, respectively.

(e) REPORT.—Not later than 90 days after the termination of the pilot program and the pathogen-agnostic pilot program, respectively, the Secretary shall submit to

the congressional defense committees a report that includes the following:

(1) A summary of the findings from all monitoring systems under the pilot program and pathogen-agnostic pilot program.

(2) Recommendations for interventions or policy changes based on trends observed under the pilot program.

(3) An assessment of the effectiveness of the pilot program in enhancing force health protection, readiness, and early pathogen detection.

(f) STRATEGIC PLAN.—Not later than one year after the date of the enactment of this section, the Secretary shall submit to Congress a strategic plan that—

(1) defines requirements for implementing a scalable, pathogen-agnostic monitoring capability;

(2) identifies technologies and risk-based methodologies to achieve mission requirements; and

(3) demonstrates coordination with the Biodefense Council ensuring compliance with Privacy Act and Department regulations.

☒

Amendment to H.R. 8800

Offered by: Ms. Stefanik

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Deployment and Scaling of Quantum Network Infrastructure

The committee notes that as the Department of Defense considers its transition to post-quantum cryptography, it must consider current weaknesses on its networks, including the threat posed by "Harvest Now, Decrypt Later" attacks. The committee is aware of quantum technology's potential to enable additional capabilities of telecommunications networks. The committee is also aware of additional benefits provided by quantum networking technologies, including facilitating infrastructure that will be a critical enabler to scaling future quantum compute.

As such, the committee recognizes the potential for the deployment and scaling of quantum networking technologies, both to protect current datasets and to scale future quantum infrastructure. Therefore, the committee directs the Chief Information Officer of the Department of Defense, in coordination with the Under Secretary of Defense for Research and Engineering and the Director of the Defense Advanced Research Projects Agency, to submit not later than June 1, 2027 a report to the House Armed Services Committee detailing its efforts to support the deployment of quantum networking technologies. At a minimum, the report shall include:

1. An assessment of entities that specialize in quantum networking technologies that currently exist in the commercial market;
2. A summary of the Department's participation, if any, in multiagency consortia to build and experiment with quantum network testbeds; and
3. Current plans and efforts to deploy and scale quantum networking technology across the Department's networks.

Amendment to H.R. 8800

Offered by: Mr. Gooden

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Report on the Adoption of Autonomous Vertical Takeoff and Landing Platforms

The committee supports efforts by the Navy and Marine Corps to pursue the Distributed Maritime Operations and Expeditionary Advanced Base Operations operational doctrines, supported by the Next Generation Air Dominance and Collaborative Combat Aircraft programs, to preserve combat power while increasing survivability and operational tempo in the Indo-Pacific. The committee understands that, in support of these operational doctrines, the Navy is developing autonomous vertical takeoff and landing (VTOL) platforms capable of operating in the Indo-Pacific. However, the committee is concerned that the absence of validated tactics, concepts of employment, and integration pathways may limit the operational utility and delay fielding of these systems.

Therefore, the committee directs the Secretary of the Navy, in coordination with the Commandant of the U.S. Marine Corps, to provide a briefing to the House Committee on Armed Services not later than December 1, 2026, on options for integration, operationalization, and sustainment of autonomous VTOL platforms. The briefing should include:

(1) a description of the force structure, logistics, training, operational concept, and sustainment trade space for autonomous VTOL platforms;
(2) a description of roles suitable for autonomous VTOL platforms, and for which such platforms would provide additional capability or efficiency;
(3) projected resource requirements and transition timelines; and
(4) an evaluation of the feasibility and advisability of the integration of such systems into Naval and Marine aviation units.

AMENDMENT TO H.R. 8800

OFFERED BY MR. DAVIS OF NORTH CAROLINA

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

SEC. 15___. EXPANSION OF AI-ENABLED MAINTENANCE INTELLIGENCE PLATFORMS ACROSS AIR EDUCATION AND TRAINING COMMAND.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, and subject to the availability of appropriations, the Secretary of the Air Force shall establish a pilot program to operationalize and expand artificial intelligence (AI)-enabled maintenance data cleansing and correction capabilities across the Air Force. This program will prioritize the improvement of aircraft availability and pilot production capacity by modernizing maintenance data quality, increasing the effectiveness of sustainment operations, and maximizing readiness of existing training aircraft fleets through enhanced data fidelity and decision support.

(b) SCOPE.—The program under subsection (a) shall apply across the full portfolio of aircraft operating within Air Education and Training Command.

(c) OBJECTIVES.—The objectives of the program are to leverage AI-enabled software solutions to—

(1) cleanse and correct structured and unstructured maintenance and logistics data;

(2) establish validated, high-fidelity ground-truth maintenance datasets to improve the performance and reliability of existing Air Force readiness, logistics, and decision-support systems;

(3) reduce manual data correction burdens and improve interoperability with legacy maintenance information systems;

(4) enhance sustainment efficiency, sortie generation, and scheduling accuracy through improved maintenance visibility;

(5) increase situational awareness for tactical-level maintainers and operational leadership;

(6) establish standardized, reusable maintenance data cleansing, correction, and integration frameworks designed to interoperate with and enhance existing Air Force maintenance, logistics, and readiness systems; and

(7) enable scalable, repeatable integration of AI-enabled maintenance capabilities across the Air Force.

(d) PARTNERSHIPS.—In carrying out the program under subsection (a), the Secretary of the Air Force may partner with a federally funded research and development center, a University Affiliated Research Center, a center of excellence, a military service laboratory, or one or more private-sector entities with experience in deploying AI-powered maintenance intelligence capabilities that support data cleansing, parts forecasting, and sustainment modernization within the Air Force, as well as any other partners the Secretary deems necessary.

(e) BRIEFING.—At least 30 days before the date on which the authority expires under subsection (f), the Secretary of the Air Force shall provide to the congressional defense committees a briefing that includes—

(1) a description of the data cleansing and correction challenges addressed through the program;

(2) an assessment of any improvements in data accuracy, aircraft availability, and maintenance efficiency resulting from the program; and

(3) an evaluation of the feasibility and advisability of expanding these capabilities to additional Air Force units operating the same aircraft types.

(f) EXPIRATION.—The authority to carry out the program under subsection (a) shall expire on the date that is one year after the date of the enactment of this Act.

☒

Amendment to H.R. 8800

Offered by: MRS. KIGGANS OF VIRGINA

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Advanced Warhead Effects

The committee notes that while the commercial sector and academic institutions are developing novel energetics, the Department of Defense has lagged in its adoption and is still primarily relying on legacy energetic materials. The committee is concerned that current development efforts may overemphasize delivery vehicles, launch, and propulsion while underinvesting in modern warhead lethality and advanced reactive materials.

The committee believes the Department should adequately prioritize advanced effects and lethality solutions to maintain technological superiority and improve production scalability. The committee notes that the Blackbeard-Ground Launched Missile and Multi-Mission Affordable Capacity Effector programs, among others, could provide opportunities adopt advanced reactive materials, with the potential to improve operational characteristics, affordability, and lethality.

The committee directs the Secretary of the Navy, in coordination with the Secretary of the Army and the Director of the Joint Energetics Transition Office, to provide a briefing to the House Committee on Armed Services not later than December 1, 2026, on the Department's plan to evaluate and integrate advanced warhead energetics into the Blackbeard-Ground Launched Missile and Multi-Mission Affordable Capacity Effector programs.

The briefing should include the following:
(1) an analysis of how funding provided in the One Big Beautiful Bill Act (Public Law 119-21) will support research and testing of advanced reactive materials;
(2) a description of how such materials can be integrated into system architectures early enough in the development cycle to enable scalable production and avoid costly recertification requirements;
(3) a description of any additional investments required to incorporate advanced energetics, including the use of advanced modeling approaches to accelerate development cycles; and
(4) an analysis of the feasibility and advisability of proposed actions to enable the adoption of advanced reactive materials while maintaining munition affordability.

Amendment to H.R. 8800

Offered by: Mr. McCormick

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Open-Weight Artificial Intelligence Models for Military Applications

The committee notes the existence of open-weight artificial intelligence (AI) models that allow for a significant degree of customization through users' ability to alter the numerical parameters that govern the model's output. The committee further understands that open-weight AI models are capable of on-premises deployment, which could make them suitable for use in secure settings.

The committee therefore directs the Secretary of Defense, in coordination with the Chief Digital and Artificial Intelligence Officer, to provide a briefing to the House Committee on Armed Services by March 15, 2027, summarizing the existing use of open-weight AI models by the Department, any plans for further adoption and deployment, and the Department's views on the relevance of these models to military applications.

AMENDMENT TO H.R. 8800

OFFERED BY MR. VINDMAN OF VIRGINIA

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

SEC. 15___. INCLUSION OF CRITICAL INFRASTRUCTURE AND OPERATIONAL TECHNOLOGY SECURITY IN COMBATANT COMMAND PLANNING AND READINESS EXERCISES.

(a) REQUIREMENT.—The Secretary of Defense shall direct the commanders of the combatant commands, consistent with the authorities provided under sections 164 and 167b of title 10, United States Code, to incorporate critical infrastructure security and operational technology security considerations into—

(1) planning activities conducted to execute national defense strategies; and

(2) joint and combined planning, training, and readiness exercises.

(b) SCOPE OF ACTIVITIES.—The activities described in subsection (a) shall, at a minimum, include—

(1) assessment of vulnerabilities and resilience of critical infrastructure and operational technology systems that support military operations, defense

support to civil authorities, and homeland defense missions;

(2) coordination with relevant Federal departments and agencies, State, local, Tribal, and territorial authorities, and private sector owners and operators, as appropriate; and

(3) integration of cyber, operational technology, and physical effects relevant to disruption, degradation, or compromise of such systems.

AMENDMENT TO H.R. 8800

OFFERED BY MRS. KIGGANS OF VIRGINIA

At the appropriate place in the report to accompany H.R. 8800, insert the following new directive report language:

Memory Safe Programming Languages and Software Security Roadmap

The committee recognizes that memory management vulnerabilities continue to represent a significant source of exploitable software weaknesses across commercial and defense systems. The committee further recognizes the importance of memory safe programming languages, formal methods, and commercial technologies that improve software assurance and reduce cybersecurity risk across Department of Defense systems.

The committee directs the Secretary of Defense, in coordination with the Director of the National Security Agency and the Director of the National Institute of Standards and Technology, to submit a report to the congressional defense committees by March 1, 2027, containing a roadmap for reducing memory management vulnerabilities across Department of Defense software systems. The report shall examine:

(1) technologies for preventing the exploitation of memory management vulnerabilities and other mitigation techniques;
(2) approaches for re-writing critical legacy code bases composed in unsafe memory management programming languages using memory safe programming languages or formal methods, either manually or with the assistance of artificial intelligence technologies;
(3) recommendations regarding when and under what circumstances the use of memory safe programming languages for new programs and major system upgrades should be required;
(4) options for establishing preferences in the acquisition of commercial systems and products developed using memory safe programming languages;
(5) methods for encouraging the Defense Industrial Base to accelerate the hiring and training of software developers proficient in memory safe programming languages; and
(6) technologies capable of generating software bills of material identify risks posed by memory management vulnerabilities.

Amendment to H.R. 8800

Offered by: Mr. Bacon of Nebraska

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Physics-Based Location Modeling

The committee remains concerned about the Department of Defense's ability to maintain reliable location services in Global Navigation Satellite Systems (GNSS)-denied environments. The committee notes that modern navigation and security systems often depend on broadcast signals and network connectivity, which can lead to systems operating with false confidence when these references degrade or are manipulated. The committee believes that utilizing advanced location assurance technologies could help mitigate this problem. Accordingly, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than April 1, 2027, describing the Department's assessment of location assurance technologies, including those leveraging independent local physical evidence and environmental sensors to verify and authenticate a device's claimed location. The briefing shall include but not be limited to:

1) An evaluation of technologies capable of operating independently from GNSS and capable of functioning effectively in GNSS denied, degraded, or contested environments, including indoor and subterranean terrain and contested electromagnetic spectrum environments;
2) The feasibility and utility of utilizing non-proprietary, commercially available sensors, including magnetic and gravimetric sensors, inertial measurement units, pressure transducers, and other measurable physical characteristics of the environment, combined with physics- based modeling, to detect and mitigate GNSS/GPS spoofing and jamming, identify radio frequency manipulation and falsified location data, and authenticate location claims using independently derived physical signatures of the environment;
3) An assessment of whether such capabilities can achieve location accuracy comparable to or exceeding GNSS; and
4) An evaluation of the scalability, interoperability, cybersecurity, and other operational factors related to the use of such technologies across a representative selection of Department of Defense mission sets.

Amendment to H.R. 8800

Offered by: Mr. Fallon

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Post-Quantum Cryptography Transition Readiness Assessment

The committee notes with concern that the Department of Defense has not yet established a comprehensive, system-level inventory of cryptographic assets vulnerable to quantum-enabled attacks. The National Institute of Standards and Technology (NIST) finalized post-quantum cryptography (PQC) standards in 2024, and the Committee on National Security Systems (CNSS) has issued binding guidance under the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) requiring migration of National Security Systems to quantum-resistant algorithms by specific deadlines. The committee is concerned that the pace of transition planning within the Department of Defense does not align with these timelines, particularly for legacy hardware and constrained network environments.

Accordingly, the committee directs the Secretary of Defense, in coordination with the Director of the National Security Agency, to submit a report to the congressional defense committees not later than March 31, 2027, on the Department of Defense's readiness to transition to quantum-resistant cryptographic standards. The report shall include:

(1) the current status of the Department of Defense's cryptographic inventory, including identification of systems operating on pre-quantum cryptographic standards;

(2) the Department of Defense's plan and timeline for migrating all National Security Systems to CNSA 2.0-compliant, quantum-resistant cryptographic algorithms, including systems operating on legacy hardware and bandwidth-constrained tactical networks;

(3) any interoperability challenges identified in transitioning to post-quantum cryptographic standards and the Department of Defense's strategy to address such challenges;

(4) an assessment of the Department of Defense's use of testbed infrastructure to validate PQC deployment on operational and legacy systems; and

(5) the extent to which the Department of Defense is leveraging existing cooperative research and development agreements (CRADAs) with standards bodies, including NIST, to accelerate PQC migration.

Amendment to H.R. 8800

Offered by: Mr. Messmer

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Electromagnetic Spectrum Operations Review

The coordination and modernization of Electromagnetic Spectrum Operations (EMSO) remains of vital importance to the committee. The committee is concerned, however, that the current EMSO governance structure has not fully realized the unity of effort envisioned by the 2020 EMS Superiority Strategy. With increasing complexity associated with cognitive electronic warfare and adaptive, autonomous capabilities, the committee is concerned that the United States is not prepared to maintain EMSO superiority against advanced near-peer adversaries.

The committee understands there are multiple potential organizational structures for EMSO, including, but not limited to, establishing a combat support agency or realigning the responsibilities associated with the EMSO Executive Committee and the EMSO lead for joint EMS operations, as established by sections 500 and 500e of title 10, United States Code, respectively. Therefore, the committee directs the Secretary of Defense to provide a report to the congressional defense committees not later than March 1, 2027 on the following:

(1) An update on the progress of the implementation of the 2020 EMS Superiority Strategy;
(2) An evaluation of potential governance structures for EMSO, including an analysis of alternatives using criteria such as operational effectiveness, manning, and resourcing; and
(3) Any legislative adjustments necessary to support the recommended governance structure identified pursuant to paragraph (2).

Amendment to H.R. 8800

Offered by: Mr. McGuire

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Partner Security Forces Operating High-Risk Telecommunications Equipment

The committee recognizes that the security of United States military operations, intelligence sharing, and defense cooperation depends in large part on the integrity and security of information and communications technology (ICT) networks used by security forces from partner nations. The committee highlighted these risks in the National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) by establishing government-wide restrictions related to the used of covered telecommunications equipment or services and in the National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283) by requiring the Secretary of Defense to identify risks to Department personnel, equipment, and operations prior to basing major weapons systems or permanently assigned forces in countries operating high-risk telecommunications infrastructure. The committee believes that such foreign security forces should be encouraged to eliminate reliance on high-risk ICT equipment or services that pose national security risks to the United States and its allies.

The committee also notes that under the telecommunications security program authorized in section 223 of Public Law 115-232, the Defense Information Systems Agency and the United States Cyber Command are responsible for monitoring government-transiting packet streams for 5G data for foreign adversarial threats on Department of Defense frequencies. Therefore, the committee directs the Secretary of Defense, in coordination with the Director of the Defense Information Systems Agency and the Commander of the United States Cyber Command, to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the integrity and security of ICT networks used by the Department of Defense and partner security forces. Such briefing shall include:

(1) an update on progress made in identifying foreign adversarial threats on Department of Defense networks through the telecommunications security program;

(2) an assessment of high-risk ICT equipment and services used in foreign security partners' information and communications technology networks.

(3) an evaluation of risk mitigation measures undertaken to address the risk of Department network traffic transiting through foreign, high-risk ICT infrastructure; and

(4) recommendations on whether further statutory measures may be necessary to discourage partner forces from relying on high-risk ICT equipment.

Amendment to H.R. 8800

Offered by: Mr. McGuire

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Weather and Environmental Data Acquisition Improvements

The committee is concerned that combatant commands may have unmet or partially met weather and environmental data requirements that support operations and that current Department practices for meeting such requirements may result in protracted timelines, duplicative acquisitions across components, and contract terms that limit government ownership and usability of the data.

The committee therefore directs the Chief Digital and Artificial Intelligence Officer, in coordination with the Under Secretary of Defense for Acquisition and Sustainment, to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on processes for and potential improvements to the acquisition of weather and environmental data. The briefing shall include the following:

(1) the process for identifying combatant command weather and environmental data requirements that could be met through commercial data, including the most common reasons requirements could be unmet or partially met;

(2) an identification of such purchased weather and environmental data over the preceding two fiscal years, including the average time from identification of requirements to delivery of appropriate data to appropriate data enclaves across components and identification of any duplicative acquisitions, disaggregated by method of acquisition, consumption model, and responsible program office;

(3) an identification of unmet or partially met weather and environmental data requirements for each combatant command during the preceding fiscal year, including the operational missions or functions affected;

(4) the extent to which Department of Defense components are using consumption-based acquisition approaches for weather and environmental data, including any enterprise-level vehicles, and an assessment of barriers to broader adoption;

(5) recommendations for administrative, regulatory, contract, or acquisition policy changes the Department can take without additional statutory authority to reduce acquisition timelines, eliminate duplicative acquisitions, and ensure government ownership of commercially acquired weather and environmental data without deployment restrictions.

Amendment to H.R. 8800

Offered by: Mr. McGuire

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Digital Engineering Integration and Governance Across the Department of Defense

The committee recognizes digital engineering as a foundational capability essential to improving acquisition outcomes, reducing lifecycle costs, and modernizing military systems across the Department of Defense. The committee believes digital engineering accelerates the delivery of mission-effective systems to the warfighter and, when combined with disciplined product lifecycle management, improves requirements development, enables earlier and better-informed programmatic decisions, and supports long-term sustainment and modernization.

The committee supports the scaling of digital engineering scaled across all Department programs and platforms and believes it must be resourced accordingly, including through the establishment of dedicated budget lines. The committee notes that the Department of the Air Force has demonstrated progress in integrating digital engineering and product lifecycle management into program execution and acquisition decision-making and strongly supports the continued maturation of lifecycle management across its programs. The committee further recognizes the Department's progress with the publication of Department of Defense Instruction 5000.97, which established department-wide direction for digital engineering. The committee encourages the Department to continue implementing the broad and deliberate training outlined in the Instruction, as well as organizing, equipping, and integrating efforts across development, acquisition and sustainment commands and organizations.

Therefore, the committee directs the Under Secretary of Defense for Acquisition and Sustainment to provide a briefing to the House Committee on Armed Services not later than March 1, 2027 on the Department's plan to institutionalize digital engineering across all current and future weapon system and platform programs. The report shall include the following information:

(1) an assessment of the Department's progress implementing Department of Defense Instruction 5000.97 throughout the design, acquisition, sustainment, and modernization lifecycle;

(2) an outline of digital engineering and product lifecycle management best practices for naval shipbuilding, aviation, unmanned aerial vehicles, and undersea warfare programs;

(3) a recommendation for the designation of an executive agent or office responsible for Department-wide digital engineering strategy, implementation, and oversight; and

(4) an assessment of currently available commercial digital engineering ecosystems and product lifecycle management capabilities that could serve as department-wide solutions, including their ability to meet the Department's requirements for governance structures, data standards, cybersecurity, access controls, and interoperability with existing service- and program-level digital environments.

Amendment to H.R. 8800

Offered by: Mr. Jackson of Texas

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Establishment of National Security and Defense Artificial Intelligence Institute

The committee continues to support the authority provided in section 224 of the National Defense Authorization Act for Fiscal Year 2026 (P.L. 119-60) for the Secretary of Defense to establish one or more National Security and Defense Artificial Intelligence (AI) Institutes at eligible host institutions, including Senior Military Colleges. The Committee further supports the current Administration's AI Action Plan recommendations to grow Senior Military Colleges into hubs of artificial intelligence research, development, and talent building, including through AI-specific curriculum for AI use, development, and infrastructure management. However, the committee remains concerned that the Department has not articulated a clear implementation plan, timeline, governance structure, or resource requirement for carrying out this authority.

Therefore, the Committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Chief Digital and Artificial Intelligence Officer and any other official deemed relevant by the Secretary, to submit a report to the House Committee on Armed Services not later than February 1, 2027, on the Department's plan to establish a National Security and Defense Artificial Intelligence Institute consistent with Section 224 of P.L. 119-60. The report shall include:

(1) the Department's proposed timeline for establishment, responsible office or official, governance structure, and coordination plan with the military departments, defense agencies, combatant commands, Federal laboratories, industry, and institutions of higher education;
(2) identification of specific AI mission areas the Department anticipates such an Institute to prioritize, including secure data, AI testbeds, access to computing resources, AI assurance, workforce development, and transition of research into operational capability;
(3) the proposed criteria for selecting eligible host institutions, including how the Department will evaluate Senior Military College status, DoD-sponsored research experience, secure research infrastructure, talent pipelines, partnerships with the defense industrial base and startup companies, and demonstrated ability to transition research into defense applications;
(4) the estimated funding required across the Future-Years Defense Program for establishment, including any program element, solicitation vehicle, or schedule for a competitive award; and

(5) any legal, budgetary, acquisition, data access, compute access, classification, security, or personnel barriers to implementation, along with proposed congressional actions to address such barriers.

Amendment to H.R. 8800

Offered by: Mr. Vasquez

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Weapon System Survivability in Combined Environments

The committee notes the importance of comprehensive weapon system survivability testing, including testing of both single event and combined event radiation effects, and believes that such testing is and will be essential to maintaining operational relevance and deterring peer adversaries. However, the committee is concerned that current infrastructure and capabilities for combined event radiation testing may be insufficient to maintain the required confidence in system survivability characteristics. Therefore, the committee directs the Director of the Test Resource Management Center to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, describing the Department's efforts to ensure adequate test capabilities for combined event radiation effects. The briefing should describe the current coordination and communication structures among relevant stakeholders, identify current and planned testing requirements for combined events, describe current and planned infrastructure requirements in support of such testing, and identify investments required across the Future Years Defense Program to enable such testing.

Amendment to H.R. 8800

Offered by: Mr. Khanna

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Worker Feedback in Development of Department of Defense Artificial Intelligence Systems

The committee is aware that the Department of Defense is rapidly deploying artificial intelligence (AI) systems across the defense enterprise and wants to ensure workers who use or are affected by these systems are engaged before and during deployment and have a channel to provide feedback after deployment.

The committee directs the Chief Digital and Artificial Intelligence Officer, in coordination with the Under Secretary of Defense for Personnel and Readiness and the Director of Operational Test and Evaluation, to provide a report to the congressional defense committees not later than February 1, 2027, on the Department of Defense's processes for gathering worker feedback before AI systems are deployed, during operations, and after fielding. The report shall include the following:

(1) an evaluation of the extent to which Department workforce is actively and systematically solicited for input on the design and deployment of AI systems before fielding, including impacts on work roles, workflows, decision transparency, changes to daily tasks, productivity, training requirements, and usability;

(2) an assessment of whether standing mechanisms exist for the workforce to report feedback after deployment;

(3) examples of whether such feedback resulted in modifications or corrective actions; and

(4) an assessment of gaps in the Department's processes for gathering worker feedback and any planned actions and associated timelines to address identified gaps.

The report should be submitted in an unclassified form but may include a classified annex.

Amendment to H.R. 8800

Offered by: Mr. Sorensen

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Foreign Weather Modification Capabilities

The committee notes increasing international investment in weather modification capabilities, particularly by the People's Republic of China, which has publicly described large-scale programs dedicated to precipitation enhancement and other forms of atmospheric intervention. The committee further notes that several other nations, including Japan, Russia, the United Arab Emirates, India, Thailand, the Philippines, and Indonesia, maintain active research, development, and operational programs related to weather modification technologies. The committee is concerned that the United States may lack a comprehensive understanding of the scope, objectives, and potential military implications of these activities, particularly by adversaries, including possible applications for operational weather shaping, civil disaster mitigation, and broader economic or geopolitical influence.

Accordingly, the committee directs the Secretary of Defense to brief the House Committee on Armed Services not later than March 1, 2027, assessing foreign weather modification activities and their implications for United States national security. The briefing shall include:

(1) an assessment of foreign objectives, programs, institutional sponsors, and estimated funding levels;
(2) relevant research and development activities, including atmospheric targeting methods, advanced modeling capabilities such as the Pangu-Weather system;
(3) machine-learning applications;
(4) operational capabilities including dispersion platforms, mechanisms, materials, and supporting sensing systems;
(5) potential benefits and risks associated with such activities;
(6) the strategic implications should foreign nations achieve technological or operational dominance in weather modification capabilities;
(7) any resources, including any staff funding, required for the Department to combat the threat and study or develop similar capabilities, as well which Department office is already tasked with this and the state of agency coordination; and
(8) recommendations, including an analysis of existing and dormant authorities, for actions the Department of Defense could take to improve understanding of foreign weather modification activities and re-establish American weather modification leadership to deter risk, bolster civil and defense capabilities, and maintain economic and national security.

AMENDMENT TO H.R. 8800

Offered by Mr. Whitesides of California

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Atmospheric Dominance Research and Monitoring

The committee recognizes the importance of the atmosphere and near-space environment to joint operations worldwide, as well as the complex environments that United States assets are likely to encounter.

The committee believes that additional research on atmospheric signatures and dynamics in the atmosphere and the development of predictive techniques to ensure observational and operational superiority would be beneficial for Air Force missions. The committee encourages the Air Force to conduct additional research in atmospheric phenomenology in order to develop monitoring systems that detect and analyze threats. Further, the committee directs the Secretary of the Air Force, in coordination with the Director of the Defense Intelligence Agency, to submit a report to the House Committee on Armed Services not later than January 1, 2027, on the path to establish a program that:

(1) expands global in-situ atmospheric monitoring and assimilation with satellite data across the troposphere and stratosphere to detect and attribute active modification of natural atmospheric processes;

(2) ensures sufficient atmospheric observation, modeling, and analytical capability to differentiate benign activities from those that could impact the national security of the United States; and

(3) leverages public-private partnerships, as appropriate, to efficiently scale in-situ atmospheric monitoring and analytic capabilities.

Amendment to H.R. 8800
National Defense Authorization Act for Fiscal Year 2027

Offered by: Mr. Wittman

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Software-Enabled Sustainment

The committee notes that the Department of Defense is increasingly deploying advanced software solutions and software-based capabilities across the organization, and encourages the Department to take steps to appropriately incorporate software sustainment into life-cycle planning. Managing software systems against readiness and cybersecurity risks will continue to drive mission capable rates across platforms.

Furthermore, the National Defense Authorization Act for Fiscal Year 2026 (Public Law 119-60) established portfolio acquisition executives and provided those officers with additional responsibilities to oversee life-cycle sustainment of programs under their purview. Public Law 119-60 also elevated product support managers to the same authority and program managers. These changes reflect the committee's intent to prioritize sustainment for the joint force and across the services, and the committee encourages the Department to further incorporate the maintenance of software into the duties and responsibilities of those positions.

Therefore, the committee directs the Deputy Secretary of Defense, in coordination with Under Secretary of Defense for Acquisition and Sustainment, to submit a report to the congressional defense committees, not later than February 1, 2027, detailing efforts to expand best practices and lessons learned in developing and scaling software-enabled sustainment practices. The report shall include, at a minimum, the following information:

(1) software sustainment metrics, including mission capable rate contribution, patch currency rates, and vulnerability remediation timelines;
(2) processes to assess costs and readiness outcomes;
(3) leading practices for replication across the Department; and
(4) and other information the Deputy Secretary deems relevant.

Amendment to H.R. 8800

Offered by: Ms. Elfreth of Maryland

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Biochemical Sensing Technologies for Warfighter Readiness

The committee recognizes the importance of real-time biochemical sensing technologies to support warfighter readiness, force protection, and operational decision-making. The committee is aware of ongoing U.S. Army Combat Capabilities Development Command efforts to develop forward deployable, wearable biochemical sensors.

The committee further notes that expanding sensing capabilities to additional biomarkers could improve the Department's ability to assess readiness, performance, brain health, and exposure to toxic industrial chemicals or chemical agents.

The committee directs the Secretary of Defense to submit a report to the congressional defense committees, not later than March 1, 2027, on Department efforts to develop, evaluate, and transition biochemical sensing technologies, including:

(1) an overview of relevant Department research and development activities;
(2) a description of potential applications for physiological monitoring and environmental threat detection;
(3) an identification of transition pathways;
(4) a description of relevant supply chain and manufacturing considerations, including foreign-sourced components and potential for transition to domestic production; and
(5) a summary of major milestones, testing, or demonstration activities.

AMENDMENT TO H.R. 8800

OFFERED BY MR. JACKSON OF TEXAS

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

SEC. 10___. BIANNUAL REPORTS ON OPERATIONAL ADAPTATION AND FIELDING OF DEFENSE AUTONOMOUS WARFARE GROUP.

(a) REPORTS REQUIRED.—Not later than 90 days after the date of the enactment of this Act, and every 180 days thereafter until the date that is two years after the date of the enactment of this Act, the Secretary of Defense, in coordination with the Commander of United States Special Operations Command, shall submit to the congressional defense committees a report on the adaptation cycles of the Defense Autonomous Warfare Group and associated autonomous warfare programs. Each such report shall include, for the period covered by the report, each of the following:

(1) A summary of operational lessons identified during such period regarding the employment, maintenance, and integration of autonomous and remotely piloted systems, including lessons derived

from combat observations, electronic warfare and cyber threat environments, and joint exercises.

(2) A description of the specific actions taken to incorporate the lessons identified under paragraph (1) into joint and service-level military doctrine, including the timeline from the identification of a lesson to the formal update of doctrinal publications.

(3) A description of modifications made to training pipelines, leader development programs, and personnel policies to reflect operational lessons.

(4) An analysis of how operational feedback has influenced current and future procurement strategies, including—

(A) changes made to existing contracts or performance requirements;

(B) the speed at which technical feedback from operators was translated into hardware or software updates;

(C) an analysis of the reliance on non-domestic supply chains for components altered during adaptation cycles; and

(D) a list of any procurement programs under which existing contractual requirements hindered the rapid adoption of operational lessons.

(5) A summary of the broad allocation of funds across major capability lines and the general distribution profile of resulting autonomous assets across the military departments and combatant commands.

(6) An assessment of the adaptation cycle speed for autonomous systems, defined as the duration between the identification of an operational deficiency or opportunity and the implementation of a corresponding change in doctrine, training, or procurement, including an assessment of the average time required to develop, test, and deploy software patches or technical countermeasures to fielded autonomous systems.

(7) To the extent practicable, a comparison of the adaptation cycle speed of the Department of Defense relative to the observed adaptation cycles of near-peer competitors in the field of autonomous warfare.

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

Amendment to H.R. 8800

Offered by: Mr. Vindman

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Asset Visibility and Discovery in the United States Indo-Pacific Command Area of Responsibility

The committee recognizes that effective cyber defense depends on maintaining visibility into assets connected to Department of Defense networks, including information technology, operational technology, and internet-of-things devices. The committee is concerned that limited visibility into assets operating on classified networks may hinder the ability to identify vulnerabilities, reduce attack surface risk, and support command and control of forces.

Therefore, the committee directs the Commander of United States Indo-Pacific Command, in coordination with the Department of Defense Chief Information Officer, to submit a report to the House Committee on Armed Services not later than June 1, 2027, on asset visibility and discovery across classified networks operated by the U.S. Indo-Pacific Command. The report shall be submitted in unclassified form but may include a classified annex. The report should include the following:

(1) an assessment of the current and planned ability to identify and maintain visibility into assets connected to classified networks;

(2) significant gaps in asset visibility and discovery across classified networks;

(3) current and planned efforts to address such gaps; and

(4) resource requirements and projected funding requirements across the Future Years Defense Program to improve asset visibility and discovery across classified networks.

AMENDMENT TO H.R. 8800

OFFERED BY MR. BACON OF NEBRASKA

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

SEC. 15___. REQUIREMENT FOR GUIDANCE AND PROHIBITION ON USE OF ARTIFICIAL INTELLIGENCE OF CERTAIN ARTIFICIAL INTELLIGENCE COMPANIES.

Section 1532 of the National Defense Authorization Act for Fiscal Year 2026 (10 U.S.C. 2224 note) is amended in subsection (a)—

(1) by amending paragraph (2) to read as follows:

''(2) GUIDANCE FOR DEPARTMENT SYSTEMS AND DEVICES.—Not later than 30 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2027, the Secretary of Defense shall issue Department of Defense-wide guidance for the identification of covered artificial intelligence companies and processes for the exclusion and removal of artificial intelligence developed by such companies from systems and devices of the Department.''; and

(2) in paragraph (3)(B), by striking ''if'' and inserting ''on and after the date that is 90 days after the date on which''.

☒

Amendment to H.R. 8800

Offered by: Mr. Jackson of Texas

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Shipboard Cyber-Physical Survivability and Artificial Intelligence-Enabled Anomaly Detection

The committee recognizes that increasing strategic competition in the maritime domain has expanded the cyber threat surface facing the U.S. Navy's information technology (IT) and operational technology (OT) systems, which could disrupt naval operations, degrade readiness, and threaten mission execution. The committee is encouraged by the efforts to improve visibility across shipboard IT and OT environments and notes the potential value of artificial intelligence and machine learning technologies to identify cyber anomalies, detect threats, reduce response times, and enhance the resilience of mission-critical systems.

Therefore, the committee directs the Secretary of the Navy to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the feasibility, effectiveness, and operational impact of expanding and modernizing the SHARKCAGE program to bridge the visibility gap between shipboard enterprise networks and mission-essential industrial control systems through a unified IT and OT defense architecture. The briefing shall include:

(1) an assessment of current cyber gaps in visibility across shipboard IT, OT, and mission-critical control systems, and the operational risks associated with such gaps;
(2) an evaluation of the current and potential use of artificial intelligence and machine learning technologies for detecting cyber anomalies and threats across shipboard IT and OT environments;
(3) an assessment of the operational feasibility of continuous monitoring and threat detection across shipboard IT and OT environments, including the ability to operate in contested, disconnected, intermittent, or degraded environments;
(4) an assessment of interoperability and integration of shipboard IT and OT monitoring and cyber defense capabilities with existing Navy cybersecurity, command-and-control, maintenance, and fleet readiness systems; and
(5) recommendations regarding the expansion or modernization of SHARKCAGE, including technical and resource considerations associated with scaling such capabilities.

AMENDMENT TO H.R. 8800

OFFERED BY MR. WITTMAN OF VIRGINIA

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

SEC. 8___. SOFTWARE ACCOUNTABILITY IMPROVEMENTS OVER LIFECYCLES.

(a) SOFTWARE SUSTAINMENT FRAMEWORK.—Section 4324(b)(1) of title 10, United States Code, is amended by adding at the end the following new subparagraph:

''(G) A software sustainment framework that—

''(i) defines metrics for software-enabled elements, including patch currency, vulnerability remediation timelines, and version lifecycle status; and

''(ii) provides for periodic review of such metrics.''.

(b) LIFE-CYCLE SUSTAINMENT PLANNING BY PRODUCT SUPPORT MANAGERS.—Section 4324(b)(2) of title 10, United States Code, is amended—

(1) in subparagraph (D), by striking ''and'' at the end;

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

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

''(F) maximize software-enabled solutions that reduce unanticipated growth work during maintenance cycles; and

''(G) maximize the use of consumption-based solutions as described in section 3605 of this title.''.

(c) RESPONSIBILITIES OF PORTFOLIO ACQUISITION EXECUTIVES.—Section 1732(c) of title 10, United States Code, is amended—

(1) in paragraph (7), by striking ''and'' at the end;

(2) in paragraph (8), by striking the period at the end and inserting ''; and''; and

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

''(9) establish incentives for effective use by contractors of software-enabled solutions that expand the collection of decision-quality data to reduce unanticipated growth work during maintenance cycles or expedite the construction or procurement of capabilities.''.

(d) RESPONSIBILITIES OF PRODUCT SUPPORT MANAGERS.—Section 1733(d) of title 10, United States Code, is amended—

(1) by redesignating paragraphs (4) through (9) as paragraphs (5) through (10), respectively;

(2) by redesignating the second paragraph (3) (relating to ''Adopting predictive analytics'') as paragraph (4); and

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

''(11) Maximizing the qualification, approval, integration, and adoption of advanced technologies and processes.''.

☒

Amendment to H.R. 8800

Offered by: Mr. Fallon

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Internet Operations Management Security Automation

The committee recognizes that the Department of Defense Cyber Defense Command (DCDC) has piloted security automation capabilities that operationalize the attack surface visibility and vulnerability discovery capabilities of its Internet Operations Management (IOM) program. The committee notes the potential for full deployment and scaling of security automation capable of mitigating new and emerging vulnerabilities at machine speed to enhance United States Cyber Command (USCYBERCOM)'s ability to keep pace with increasingly sophisticated cyber threats against the Department of Defense Information Network.

The committee is therefore concerned that without a clear implementation plan and dedicated resources, full deployment of advanced security orchestration and automation capabilities across the Department of Defense Information Network may not be achieved within operationally relevant timelines.

The committee directs the Commander of United States Cyber Command to provide a briefing to the House Committee on Armed Services not later than March 31, 2027, on the implementation plan, timeline, and resource requirements necessary to achieve full deployment of the IOM program, or equivalent security automation capabilities, across the Department of Defense Information Network.

Amendment to H.R. 8800

Offered by: Mr. Vindman

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Artificial Intelligence–Enabled Advanced Manufacturing for Missile and Munitions Production

The committee is encouraged by the progress made by the Department of Defense in understanding and addressing the critical shortage of missiles and other large munitions. While the committee recognizes ongoing efforts to modernize and expand depots throughout the United States, additional commercial manufacturing capacity will be needed now and well into the future. The committee is aware that artificial intelligence (AI)-enabled advanced manufacturing has proven particularly effective at optimizing and rapidly scaling production of missiles in privately funded facilities.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than February 1, 2027, on the integration of AI enabled advanced manufacturing into the defense industrial base. The briefing should include:

(1) how AI-enabled advanced manufacturing can be fully integrated into the defense industrial base for missile and large munitions production;

(2) actions the Department is taking or will take to encourage defense prime contractors to incorporate AI-enabled advanced manufacturing capabilities into their supply chains; and

(3) any statutory, regulatory, contractual, or workforce barriers that may impede adoption of AI-enabled advanced manufacturing across the defense industrial base.

Amendment to H.R. 8800

Offered by: Mr. Bacon of Nebraska

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

ACCELERATION AND MODERNIZATION OF CRYPTOGRAPHIC CERTIFICATION PROCESS

The committee is aware of the growing risks to the Department's cyber posture and ability to maintain mission assurance in modern, contested environments. To stay ahead of adversaries, the committee believes that the Department must continue to develop and implement a streamlined, risk-informed, controlled evaluation framework to enable faster assessment of emerging cryptographic approaches, including hardware-based solutions based on non general-purpose computing architectures. Therefore, the committee directs the Secretary of Defense to provide a report to the House Committee on Armed Services no later than June 1, 2027, on the following:

1. a detailed status update on modernization efforts of the certification process;
2. assessments of emerging cryptographic technologies, including hardware-centric approaches;
3. identified barriers or technical, operational, or bureaucratic gaps hampering acceleration;
4. an updated roadmap and timeline for completing modernization milestones, including benchmarks, resources allocated, and stakeholder engagement actions.

AMENDMENT TO H.R. 8800

OFFERED BY MR. FALLON OF TEXAS

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

SEC. 15___. SEMIANNUAL REPORTS ON CYBER OPERATIONAL READINESS ASSESSMENT PROGRAM.

(a) SEMIANNUAL REPORTS REQUIRED.—Not later than 180 days after the date of the enactment of this Act, and not less frequently than once every 180 days thereafter, the Secretary of Defense shall, acting through the Chief Information Officer of the Department of Defense and the Commander of the Department of Defense Cyber Defense Command (DCDC), submit to the congressional defense committees a semiannual report on the implementation of the Cyber Operational Readiness Assessment program of the Department of Defense Cyber Defense Command and the findings from such program.

(b) CONTENTS.—Each report required under subsection (a) shall include, for the period covered by the report, the following:

(1) An overview of the implementation status of the Cyber Operational Readiness Assessment pro-

gram, including scope, methodology, and assessment cadence across the military departments and the defense agencies and Department of Defense field activities.

(2) Aggregate and component-level findings on cyber operational readiness, including systemic risks, recurring deficiencies, and trends affecting mission assurance.

(3) An assessment of operational resilience, including the ability of the Department of Defense to maintain essential functions, contain adversary activity, and recover from cyber incidents during contested operations.

(4) A description of actions taken or planned to address material risks identified through the program, including timelines, responsible organizations, and any resource constraints.

(5) An initial plan, and subsequent progress reports, for incorporating operational technology (OT) environments into assessments carried out under the program to ensure a comprehensive operational readiness evaluation of mission-critical systems, weapon platforms, industrial control systems, and supporting infrastructure.

(6) An assessment of how assessments under the program will incorporate and operationalize Critical Infrastructure Discovery and Evaluation (CIDE) activities conducted by the Department of Defense Cyber Defense Command on operational technology networks, including alignment of scope, methodology, data collection, reporting, and resourcing to ensure unity of effort and avoid duplication.

(7) A description of any policy, authority, or resourcing gaps that inhibit full execution of the program as an operational readiness assessment.

(c) PURPOSE.—The purpose of subsection (a) is to ensure that cybersecurity is treated by the Department as an element of operational readiness across the Department and to support senior leader decisionmaking, risk acceptance, and resource prioritization related to the security and resilience of the Department of Defense Information Network (DoDIN).

(d) TERMINATION.—The requirements of this section shall terminate on the date that is three years after the date of the enactment of this Act.

Amendment to H.R. 8800

Offered by: Mr. Vindman

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Efforts to Counter Transnational Cyber Fraud

The committee recognizes the threat posed by transnational criminal organizations using cyberspace to conduct fraud and theft and compromise private data. The committee understands that countering such activities requires a whole-of-government approach and that the Department of Defense's expertise in countering malicious cyber activities is of great value.

The committee directs the Secretary of Defense to submit a report to the congressional defense committees not later than July 1, 2027, on the role of the Department of Defense in countering transnational criminal organizations conducting cyber-enabled fraud and related malicious cyber activities. The report should be submitted in unclassified form but may include a classified annex. The report should include:

(1) an assessment of the threat to Department of Defense objectives, operations, personnel, or property posed by transnational criminal organizations conducting cyber-enabled fraud;

(2) a description of current Department of Defense roles and activities to counter transnational criminal organizations conducting cyber-enabled fraud;

(4) identification of any statutory, regulatory, authority, or resource limitations affecting the Department's ability to conduct such activities; and

(5) actions the Department could take in cyberspace, consistent with current authorities and responsibilities, to contribute to efforts to counter transnational criminal organization threats to Department of Defense objectives, operations, personnel, or property.

Amendment to H.R. 8800

Offered by: Mr. Bergman

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Artificial Intelligence–Enabled Systems for Software-Defined Hardware

The committee notes the increasing role of software-defined hardware in Department of Defense systems and is concerned about the potential for resultant challenges with debugging, validation, and sustainment. The committee believes that systems engineering tools incorporating artificial intelligence that are capable of continuously monitoring, diagnosing, and conducting root cause analysis could improve readiness, performance, and system design for heavily software-defined systems, including phased array systems.

Therefore, the committee directs the Undersecretary of Defense for Research and Engineering, in coordination with the Chief Digital and AI Officer and the Chief Technology Officers of the military departments, to provide a report to the congressional defense committees not later than February 1, 2027, on the Department's plans to adopt AI–enabled systems engineering capabilities. The report shall include—

(1) an assessment of recurring challenges in debugging, validating, and repairing software-defined hardware systems;
(2) a description of existing and planned efforts to apply artificial intelligence to systems engineering, root cause analysis, and maintenance activities; and
(3) a strategy for integrating AI-enabled systems engineering capabilities into workforce training, test and evaluation, and operations.

Amendment to H.R. 8800

Offered by: MR. WILSON OF SOUTH CAROLINA

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Quantum-Enabled Radar Synchronization

The committee recognizes the importance of resilient positioning, navigation, and timing (PNT) and radar capabilities to military operations. The committee notes that advances in quantum technologies may enable improvements in timing precision, radar synchronization, and operational resilience for PNT-dependent capabilities in degraded GPS environments. The committee therefore directs the Under Secretary of Defense for Research and Engineering to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the potential applications of quantum-enabled radar synchronization technologies. The briefing shall include:

(1) an assessment of the technical maturity, feasibility, and operational relevance of such technologies in degraded GPS environments;

(2) an identification of research, development, testing, evaluation, and prototyping activities relevant to the maturation of such technologies; and

(3) recommendations for further development or integration of quantum-enabled radar synchronization technologies into applicable Department of Defense programs.

AMENDMENT TO H.R. 8800

OFFERED BY MS. JACOBS OF CALIFORNIA

In section 1513 [Log 85788], in subsection (b), redesignate paragraphs (4) through (8) as paragraphs (5) through (9), respectively, and insert after paragraph (3) the following new paragraph:

(4) requirements to preserve existing human command responsibility for the use of force involving autonomous systems or artificial intelligence-enabled systems, including procedures to identify the human commanders or operators responsible for authorizing, supervising, and terminating such use of force;

☒

AMENDMENT TO H.R. 8800

OFFERED BY MS. JACOBS OF CALIFORNIA

In section 1513 [Log 85788], in subsection (b)(7), insert after ''mission risk and operational consequence'' the following: '', including training to promote calibrated reliance on artificial intelligence-enabled systems''.

☒

Amendment to H.R. 8800
National Defense Authorization Act for Fiscal Year 2027

Offered by: Mr. Wittman

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Cybersecurity Protections in Telecommunications Systems

The committee remains concerned that the Department of the Navy, in its administration of Department of Defense wireless telecommunications contracts, is failing to prioritize cybersecurity protections in its telecommunications contracting and procurement processes. The committee believes that recent cyber intrusions and continued cyber threats, including Salt Typhoon and incidents involving the disclosure of the personal information of special operations personnel, highlight the urgency for the Department to strengthen cybersecurity capabilities to protect sensitive and classified information.

The committee notes that section 1511 of the National Defense Authorization Act for Fiscal Year 2026 (Public Law 119-60) requires the Department of Defense to ensure that each wireless mobile phone provided to senior officials or any other employee who performs sensitive national security functions have enhanced cybersecurity protections. The committee believes the Department should expand the deployment of these protections as broadly as possible.

Therefore, the committee directs the Chief Information Officer of the Navy to provide a briefing to the House Committee on Armed Services, not later than March 1, 2027, detailing steps the Navy is taking or plans to take to enhance cyber protections for wireless telecommunications devices and how the Navy is ensuring current and future telecommunications contracts are abiding by section 1511 of Public Law 119-60.

AMENDMENT TO H.R. 8800

OFFERED BY MS. JACOBS OF CALIFORNIA

In section 1501 [Log 85241], in the quoted matter adding a new section 2224b to title 10, United States Code, in subsection (b)(1), insert after ''systemic weaknesses in artificial intelligence systems'' the following: '', including risks or failure modes arising from human-machine teaming''.

☒

AMENDMENT TO H.R. 8800

OFFERED BY MS. JACOBS OF CALIFORNIA

In section 1512 [Log 85276], in subsection (b), redesignate paragraphs (2) through (5) as paragraphs (3) through (6), respectively; and insert after paragraph (1) the following new paragraph:

(2) COMMON DEFINITIONS AND CATEGORIES.—Common definitions or categories for AI systems deployed on Department enterprise AI platforms, including systems with agentic capabilities, to support acquisition clarity, testing, authorization, and operational adoption.

☒

AMENDMENT TO H.R. 8800

OFFERED BY MR. KHANNA OF CALIFORNIA

In section 1501 [Log 85241], in the quoted matter adding a new section 2224b to title 10, United States Code, in subsection (j)(2), strike ''or'' at the end of subparagraph (C); strike the period at the end of subparagraph (D) and insert ''; or''; and add at the end the following new subparagraph:

(E) operates in a manner that raises concerns regarding system control and autonomy.

☒

Amendment to H.R. 8800
Offered by: Ms. Elfreth of Maryland

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Navy Digital Engineering Interoperability

The committee recognizes that engineering, modeling and simulation, testing, certification, and sustainment activities across the Department of the Navy continue to face challenges associated with fragmented digital environments, proprietary software ecosystems, disconnected data architectures, and limited interoperability across organizations, programs, and security domains. The committee further recognizes the importance of secure collaboration and authoritative data exchange between Naval Air Systems Command, Naval Sea Systems Command, and other naval acquisition and sustainment organizations as maritime and aviation platforms become increasingly software-defined and interconnected.

The committee directs the Secretary of the Navy to provide a briefing to the House Committee on Armed Services not later than February 1, 2027, on the Navy's strategy to establish decentralized, interoperable digital engineering infrastructure capable of supporting secure cross-network collaboration, authoritative data exchange, vendor-neutral modeling and simulation data, and continuous engineering and certification workflows without requiring replacement of existing engineering tools or centralization of authoritative data. The briefing should include the following:

(1) barriers to interoperability and data portability across Navy engineering, modeling, simulation, test, and sustainment environments;
(2) opportunities to support secure collaboration between Naval Sea Systems Command, Naval Air Systems Command, and other Department of Defense organizations through interoperable digital engineering environments;
(3) opportunities to improve interoperability, authoritative data exchange, and secure collaboration across engineering, modeling, simulation, testing, and sustainment environments while preserving organizational control, cybersecurity requirements, and data sovereignty protections; and
(4) opportunities to reduce recertification burdens, accelerate modernization timelines, improve software integration activities, and enhance mission readiness through continuous engineering and digital certification approaches.

AMENDMENT TO H.R. 8800

OFFERED BY MR. KHANNA OF CALIFORNIA

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

SEC. 2___. CLOUD LABORATORY PILOT PROGRAM.

(a) CLOUD LABORATORY PILOT PROGRAM.—

(1) PROGRAM REQUIRED.—

(A) IN GENERAL.—The Secretary of Defense shall carry out a pilot program to support the establishment of cloud laboratories at the Department of Defense.

(B) REQUIREMENTS.—Each cloud laboratory supported under the pilot program shall generate high-quality data that shall be collected for use and analysis by authorized researchers.

(2) IMPLEMENTATION.—

(A) INITIAL LABORATORY.—Not later than one year after the date of the enactment of this Act and subject to the availability of appropriations, the Secretary shall establish at least one fully operational cloud laboratory.

(B) ADDITIONAL LABORATORIES.—Not later than three years after the date of the enactment of this Act and subject to the availability of appropriations, the Secretary shall, on a competitive basis, establish not fewer than two additional fully operational cloud laboratories.

(C) BIOTECHNOLOGY-FOCUSED LABORATORY.—At least one of the cloud laboratories established under this paragraph shall be focused on advancing research and development of biotechnology.

(3) IMPLEMENTATION PLAN.—Not later than one year after the date of enactment of this Act, the Secretary shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report that includes the following:

(A) A plan to establish the cloud laboratories.

(B) A plan for building in considerations related to cybersecurity, biosecurity, and research security from the beginning of development for each cloud laboratory.

(b) DEFINITIONS.—In this section:

(1) The term ''artificial intelligence'' has the meaning given such term in section 5002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283;15 U.S.C. 9401).

(2) The term ''authorized researcher'' refers to an individual who has been appropriately authorized to access data generated by the cloud laboratories supported under the pilot program, as determined by the Secretary using an authorization process established by the Secretary for such purpose.

(3) The term ''cloud laboratory'' means a physical laboratory that is equipped with automation and data storage to conduct continuous experiments.

(4) The term ''Secretary'' means the Secretary of Defense.

☒

AMENDMENT TO H.R. 8800

OFFERED BY MR. KHANNA OF CALIFORNIA

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

SEC. 18___. REPORT ON THE FEASIBILITY OF REQUIRING BILLS OF MATERIALS FOR DEFENSE ACQUISITION.

(a) REPORT REQUIRED.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report on the following:

(1) The feasibility of including requirements for Bills of Materials, including software, hardware, artificial intelligence, and cryptography, within DoD Instruction 5000.87 and the Software Acquisition Pathway.

(2) The expected value of the information gained through Bills of Materials as it relates to risk management and supply chain integrity.

(3) The necessity of establishing a new system or consolidating existing systems to perform asset management within the Department to house the information in Bills of Materials as it relates to weap-

on system components currently in use across the Armed Forces.

(b) FORM.—The report required by subsection (a) shall be submitted in unclassified form and may include a classified annex.

☒

AMENDMENT TO H.R. 8800

OFFERED BY MR. DESJARLAIS OF TENNESSEE

In section 211 (Log 84890)—

(1) in the matter proposed to be inserted by paragraph (1)(C), insert ''and developmental test and evaluation'' after ''budget classification)''; and

(2) in the matter proposed to be inserted by paragraph (3), insert ''and developmental test and evaluation'' after ''budget classification)''.

☒

Amendment to H.R. 8800

Offered by: Mr. Conaway

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

MISSION PARTNER IDENTITY VERIFICATION

The committee notes the progress made by the Defense Manpower Data Center (DMDC) in implementing Identity, Credential, and Access Management (ICAM) solutions for non-Department personnel, including dependents, foreign military partners, and the defense industrial base. The committee believes that modernizing identity verification is essential to enhancing Department of Defense (DoD) security, interoperability, and governance.

Therefore, the committee directs the Director of the Defense Manpower Data Center, in coordination with the Department of Defense Chief Information Officer, to provide a briefing to the House Committee on Armed Services not later than June 1, 2027, on the Department's strategy for mission partner identity verification. The briefing shall include the following:

(1) a plan for developing standard security requirements to enable interoperability among identity management and identity verification capabilities; and

(2) an assessment of approaches to improve identity verification and credential management for mission partners, including methods for establishing trust in credentials issued by foreign mission partners.

AMENDMENT TO H.R. 8800

OFFERED BY MR. BACON OF NEBRASKA

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

SEC. 28___. ESTABLISHMENT OF A DASHBOARD FOR MILITARY CONSTRUCTION PROJECTS FOR RESEARCH, DEVELOPMENT, TEST, AND EVALUATION FACILITIES.

(a) IN GENERAL.—Not later than one year after the enactment of this section, the Under Secretary of Defense for Research and Engineering, in coordination with each Secretary of a military department, shall establish a central dashboard to monitor and track Research, Development, Test, and Evaluation facility data related to military construction planning, design, and execution metrics across the military departments.

(b) REQUIREMENTS.—The database shall—

(1) use existing financial management tools;

(2) display relevant data for Research, Development, Test, and Evaluation facilities including, at a minimum, facility location, manager of the facility, building number, plant replacement value, age, size, building condition index, mission dependency index,

civil engineering projects programmed for the facility, and value of each such projects;

(3) track unfunded facility requirements;

(4) summarize laboratory real property and non-real property data and metrics;

(5) use Real Property Unique Identifiers (or a similar identifier for real property or other assets authorized by the Secretary of Defense) for Equipment Replacement Value of equipment that is not real property; and

(6) display trends across any data included in the database.

(c) NOTIFICATION TO CONGRESS.—Not later than 30 days after the date on which the dashboard required by subsection (a) is established, the Under Secretary of Defense for Research and Engineering shall submit to the congressional defense committees a certification that the dashboard is operational and meets the requirements of subsection (b).

(d) RECOMMENDATION.—Not later than three years after the enactment of this section, the Under Secretary of Defense for Research and Engineering shall submit to the Secretary of Defense a recommendation on whether use of the dashboard should be continued. Not later than 15 days after making such submission, the Under Sec-

retary shall submit to the congressional defense committees a notice of such recommendation.

(e) TERMINATION.—The authority under this section terminates on December 30, 2030.

(f) DEFINITIONS.—In this section:

(1) The term ''Research, Development, Test, and Evaluation facility'' means a laboratory facility or a test and evaluation facility.

(2) The term ''Equipment Replacement Value'' means the estimated cost to replace the non-real property installed test equipment within a ground test infrastructure asset.

☒

AMENDMENT TO H.R. 8800

OFFERED BY MR. WHITESIDES OF CALIFORNIA

In section 1501 [Log 85241], in the quoted matter adding a new section 2224b to title 10, United States Code, in subsection (i)(1), strike ''and'' at the end of subparagraph (B); redesignate subparagraph (C) as subparagraph (D); and insert after subparagraph (B) the following new subparagraph:

(C) in the case of any covered AI incident resulting in the loss of life of, or in bodily harm to, a member of the Army, Navy, Marine Corps, Air Force, or Space Force—

(i) a description of the incident, including the system or systems involved and the operational context;

(ii) the date and time the incident occurred;

(iii) an assessment of the cause and operational consequence of the incident; and

(iv) any corrective actions taken; and

In such section, in such quoted matter, in subsection (j)(2)(B), insert after ''operates outside'' the following: ''authorized parameters or''.

In such section, in such quoted matter, in subsection (j)(2), strike ''or'' at the end of subparagraph (C); redesignate subparagraph (D) as subparagraph (E); and insert after subparagraph (C) the following new subparagraph:

(D) fails to respond to an operator disengage command; or

Amendment to H.R. 8800

Offered by: Mr. Fallon

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Department of Defense Attack Surface Visibility

The committee recognizes that recent exploitation of vulnerabilities in internet-accessible enterprise software demonstrated the importance of maintaining visibility into internet-accessible systems, services and applications. The committee recognizes that improved visibility into the Department's attack surface can support the rapid identification of vulnerable systems, misconfigurations, and unauthorized internet-facing assets.

Therefore, the committee directs the Secretary of Defense to provide a report to the congressional defense committees not later than June 1, 2027, on the Department's approach to maintain visibility into and reduce its internet-accessible attack surface. The report shall include:

(1) an assessment of the Department's ability to identify internet-accessible systems, services, and applications;

(2) significant gaps in visibility into internet-accessible systems, services, and applications; and

(3) planned actions to address such gaps.

Amendment to H.R. 8800

Offered by: Mr. Kelly

In the appropriate place in the report to accompany H.R. 8800, insert the following new Directive Report Language:

Data Strategy to Accelerate Artificial Intelligence and Analytics Across the Department of Defense

The committee recognizes that enterprise data readiness is essential to the Department of Defense's ability to scale artificial intelligence and advanced analytics capabilities in support of operational, business, and warfighting requirements. The committee is concerned that data silos, limited interoperability, inconsistent governance, and restrictive access practices continue to impede secure data sharing and reuse across the Department.

The committee is further concerned that the Department's ability to preserve Government control of data assets and avoid dependence on closed or proprietary architectures is critical to ensuring long-term flexibility, competition, and mission effectiveness. The committee believes that the use of open standards, interoperable architectures, open-source technologies, and multi-vendor approaches, where practicable, can improve the Department's ability to accelerate adoption of artificial intelligence and advanced analytics capabilities.

The committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than March 1, 2027, on the Department's strategy to improve data readiness in support of artificial intelligence and advanced analytics. The briefing should include:

(1) an assessment of efforts to reduce data silos and improve secure data sharing and reuse across the Department;

(2) an assessment of efforts to improve interoperability and governance across cloud, on-premises, and operational environments;

(3) a description of how the Department is preserving Government control of data assets and avoiding unnecessary dependence on closed or proprietary architectures;

(4) an assessment of the Department's use of open standards, interoperable architectures, open-source technologies, and multi-vendor approaches, where practicable;

(5) a description of the governance structure for implementing the Department's data readiness strategy, including roles and responsibilities across the Department;

(6) an assessment of barriers to implementation; and

(7) any recommendations for additional authorities or resources.