119TH CONGRESS
2D SESSION

S. _____

To require the Secretary of Defense to assess and report on the feasibility of incorporating open-architecture, unmanned system command and control frameworks into Department of Defense unmanned system operations across all unmanned system tiers and domains, drawing on lessons from allied and partner country systems, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. MCCORMICK introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To require the Secretary of Defense to assess and report on the feasibility of incorporating open-architecture, unmanned system command and control frameworks into Department of Defense unmanned system operations across all unmanned system tiers and domains, drawing on lessons from allied and partner country systems, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Unmanned System Command and Control Integration Assessment Act of 2026''.

SEC. 2. ASSESSMENT OF UNMANNED SYSTEM COMMAND AND CONTROL FRAMEWORKS.

(a) ASSESSMENT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall, in coordination with the Chairman of the Joint Chiefs of Staff, the Under Secretary of Defense for Acquisition and Sustainment, the Secretary of Defense for Research and Engineering, the Chief Information Officer, Joint Interagency Task Force 401, the Director of the Defense Information Systems Agency, the Commander of Joint Interoperability Test Command, and the Secretaries of the military departments, commence a comprehensive assessment of open-architecture, unmanned system command and control frameworks with demonstrated operational effectiveness.

(b) SCOPE OF ALLIED AND PARTNER SYSTEM REVIEW.—The assessment commenced under subsection (a) shall review each of the following allied and partner country unmanned systems command and control frameworks and may include such additional frameworks as the Secretary determines appropriate:

(1) Ukraine's Delta battlefield management and unmanned aircraft systems coordination system, including an analysis of its technical architecture, its operational effectiveness in contested environments, the interoperability and integration lessons learned from its deployment that are applicable to United States Armed Forces unmanned aircraft systems command and control operations, and its cybersecurity resilience under active electronic warfare and cyber attack.

(2) Israel's Multiple Drone Operating System, including an analysis of its technical architecture, its demonstrated operational effectiveness in managing simultaneous civilian, commercial, and military unmanned aircraft systems operations, the interoperability and integration lessons learned from its deployment that are applicable to United States Armed Forces unmanned aircraft systems command and control operations, and its cybersecurity and emergency prioritization mechanisms.

(c) ELEMENTS OF ASSESSMENT.—The assessment commenced under subsection (a) shall address, at a minimum, each of the following elements:

(1) Architectural analysis, including—

(A) a comparative analysis of the technical architectures of the unmanned systems command and control frameworks reviewed, including data formats, communication protocols, interface standards, and software design approaches;

(B) an evaluation of the degree to which each framework employs open-architecture and modular open-systems architecture principles; and

(C) an identification of the architectural characteristics most associated with operational effectiveness, adaptability, and resilience in contested environments.

(2) Unmanned systems tier compatibility, including—

(A) an evaluation of each framework's capacity to manage all unmanned systems within a single integrated command and control environment;

(B) an identification of the technical and doctrinal barriers to command and control interoperability across unmanned systems s within a single framework; and

(C) a recommendation for the minimum capability requirements a Department unmanned systems command and control framework must meet to support effective employment of unmanned systems across all in a joint operational environment.

(3) Interoperability with existing Department systems, including—

(A) a detailed assessment of the compatibility and interoperability requirements for integrating an open-architecture unmanned system command and control framework with current and future Department command and control modernization, as designated by the Secretary at the time of the assessment;

(B) an identification of the interface standards, data translation requirements, and technical integration pathways that would be necessary to achieve such interoperability; and

(C) an assessment of the risks associated with integration, including cybersecurity risks arising from connecting an open-architecture system to existing classified networks.

(4) Cybersecurity and future-proofing, including—

(A) an assessment of the cybersecurity posture of each framework reviewed, including its resilience to electronic warfare, Global Positioning System denial, communications jamming, and software-based cyber attack in active contested environments;

(B) a recommendation for a cybersecurity standards framework or updates to the Risk Management Framework of the National Institute of Standards and Technology applicable to a Department unmanned system command and control system that—

(i) is based on the Cybersecurity Framework 2.0, published by the National Institute of Standards and Technology, and applicable special publications of the Institute, and is designed to incorporate updated guidance from the Institute without requiring legislative action;

(ii) incorporates a comprehensive supply chain risk management strategy;

(iii) implements robust data-centric security controls, including end-to-end data encryption, data tagging for automated policy enforcement, and accredited cross-

domain solutions to prevent compromise between classification levels and to enable secure data interoperability with mission partners;

(iv) establishes vulnerability disclosure and patch management standards enabling timely response to newly identified threats without requiring system-wide redesign; and

(v) specifies a recurring review cycle of not less than once every 18 months to update cybersecurity standards as the National Institute of Standards and Technology and other relevant standards bodies publish new guidance, without requiring legislative action; and

(vi) mandates alignment with Zero Trust Architecture (ZTA), ensuring all data, applications, assets, and services are managed with the assumption that the network is already compromised;

(C) an assessment of how the architecture of the framework can accommodate future unmanned systems technologies, including autonomous systems, artificial intelligence-enabled tar-

geting and deconfliction, swarming capabilities, and beyond-visual-line-of-sight operations, without requiring full system replacement; and

(D) a recommended technology refresh cycle and associated governance process for keeping a Department unmanned system command and control framework current with advancing technology and evolving threats.

(5) Tactical adaptability and field-level flexibility, including—

(A) an assessment of the mechanisms within each framework reviewed that enable tactical-level operators and commanders to modify, adapt, or extend command and control functionality without depending on centralized software updates or acquisition processes, drawing on documented examples from the conflict in Ukraine where unmanned aircraft systems tactics evolved within weeks in response to adversary countermeasures;

(B) a recommended design approach for a Department framework that preserves appropriate security and safety controls while enabling tactical-level customization, including through the use of application programming

interfaces, modular software components, and operator-accessible configuration tools; and

(C) an assessment of the doctrinal, training, and organizational changes required to enable and sustain field-level innovation within a structured command and control architecture.

(6) Classification and technology transfer, including—

(A) an assessment of the classification implications of a Department unmanned system command and control framework, including recommendations for which components may operate at unclassified levels to maximize interoperability with allied and commercial systems, and which must be classified;

(B) an assessment of the technology transfer and foreign military sales implications of the frameworks reviewed, including intellectual property and national security considerations associated with adopting or adapting systems developed by or with foreign partners; and

(C) recommendations for information-sharing arrangements with other United States Government organizations, allies, and partner nations that would facilitate ongoing exchange

of unmanned systems command and control lessons learned and technical standards.

(7) Implementation roadmap, including—

(A) a recommended phased implementation approach for developing and fielding a Department unmanned system command and control framework, including recommended near-term pilot programs or exercises that could demonstrate technical feasibility and operational utility;

(B) an estimate of the resources, including funding, personnel, and acquisition authorities, required to develop and field the recommended framework; and

(C) an identification of existing Department programs, platforms, and acquisition vehicles that could serve as the basis for or be accelerated by an unmanned system command and control capability.

SEC. 3. INDEPENDENT ADVISORY PANEL.

(a) ESTABLISHMENT.—Not later than 60 days after the date of the enactment of this Act, the Secretary shall establish an independent advisory panel (in this section referred to as the ''Panel'') to provide independent review

and technical guidance to the assessment required under section 2.

(b) COMPOSITION.—The Panel shall consist of not fewer than 10 and not more than 15 members appointed by the Secretary, including—

(1) not fewer than two individuals who have direct operational experience in unmanned aircraft systems employment in a joint or combined military environment;

(2) not fewer than two individuals who have technical expertise in open-architecture software systems, modular systems design, or command and control software architecture;

(3) not fewer than two individuals who have expertise in cybersecurity, including experience with operational technology cybersecurity in contested environments;

(4) at least three individuals who have expertise in unmanned aircraft systems command and control operations, doctrine, or command and control from an allied or partner country with significant unmanned aircraft systems operational experience, appointed in coordination with relevant allied or partner country authorities;

(5) at least one individual with experience in unmanned aircraft system (UAS) traffic management in the National Airspace System; and

(6) such additional members as the Secretary determines appropriate, which may include representatives from the defense industrial base, federally funded research and development centers, academic institutions with relevant expertise, and the Department of Defense test and evaluation community to ensure early consideration to interoperability, testability, and certification requirements.

(c) LIMIT ON ACTIVE GOVERNMENT EMPLOYEES.—Not more than two-thirds of the members of the Panel may be a full-time officer or employee of the United States Government.

(d) DUTIES.—The Panel shall provide written assessments and recommendations on each element of the assessment described in section 2(c) and shall have the opportunity to review and comment on draft findings before finalization.

(e) TERMINATION.—The Panel shall terminate on the date that is 90 days after the date of the submittal of the final report required under section 4(b).

(f) COMPENSATION.—Members of the Panel who are not full-time officers or employees of the United States

Government shall be compensated at a daily rate equal to the daily equivalent of the annual rate of basic pay for level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day they are engaged in the performance of Panel duties and shall be allowed travel expenses as authorized under section 5703 of title 5, United States Code.

SEC. 4. REPORTS TO CONGRESS.

(a) INTERIM REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees an interim report on the status of the assessment required under section 2, which shall include—

(1) an identification of any additional allied and partner country frameworks selected for review and analysis beyond those specified in section 2(b);

(2) a summary of findings from the architectural analysis required under section 2(c)(1);

(3) a preliminary assessment of interoperability requirements under section 2(c)(3); and

(4) any significant findings or challenges identified to date.

(b) FINAL REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees a final re-

port containing the complete findings and recommendations of the Secretary with respect to the assessment required under section 2. The final report shall include—

(1) a determination as to whether the development of a Department unmanned system command and control framework based on open-architecture principles is feasible, operationally necessary, and cost-effective;

(2) if the determination under paragraph (1) is affirmative, a recommended framework architecture, phased implementation roadmap, and legislative or regulatory actions required to proceed;

(3) if the determination under paragraph (1) is negative or qualified, a description of the specific barriers identified and recommendations for addressing them; and

(4) a classified annex, as appropriate, containing any elements that the Secretary determines must be protected from public disclosure for national security reasons.

(c) FORM.—Reports required under this section shall be submitted in unclassified form, but may include a classified annex. Unclassified portions shall be made publicly available on the Department public website not later than 30 days after submission.

(d) ANNUAL UPDATE.—For a period of five years following submission of the final report under subsection (b), the Secretary shall submit to the congressional defense committees, as part of the annual budget justification materials submitted to Congress in support of the budget of the Department (as submitted with the budget of the President under section 1105(a) of title 31, United States Code), an update describing—

(1) actions taken by the Department in response to the recommendations of the Secretary contained in the final report;

(2) material changes in allied or partner country unmanned systems command and control frameworks or practices relevant to the assessment's conclusions;

(3) emerging unmanned systems technologies or cybersecurity threats that would materially affect the recommended framework architecture; and

(4) the status of any pilot programs, exercises, or acquisition activities initiated pursuant to the recommendations of the Secretary contained in the final report.

SEC. 5. CYBERSECURITY STANDARDS FOR ANY RECOMMENDED FRAMEWORK.

(a) REQUIREMENTS.—Any unmanned system command and control framework recommended in the final report required under section 4(b), and any system developed or procured pursuant to such a recommendation, shall—

(1) employ a modular open systems architecture that permits individual software and hardware components to be updated, replaced, or patched in response to identified cybersecurity vulnerabilities without requiring redesign of the system as a whole;

(2) apply a supply chain risk management framework throughout the asset's and component's lifecycles;

(3) comply with the most current version of the Cybersecurity Framework 2.0 published by the National Institute of Standards and Technology and applicable special publications of the Institute, as updated from time to time, without requiring amendment of this Act to conform to new guidance;

(4) include a documented vulnerability disclosure policy and a process for receiving, triaging, and patching reported vulnerabilities within defined response time standards established by the Secretary; and

(5) undergo penetration testing by a National Security Agency-certified red team not less frequently than once every two years following initial fielding, with findings reported to the Principal Cyber Advisor and, in summary form, to the congressional defense committees.

(b) EXCLUSION OF COVERED FOREIGN ENTITIES.—No software, hardware, or service produced, provided, or operated by an entity on the Federal Communications Commission Covered List established under section 2 of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601), or on the Department of Defense Covered Foreign Entity list maintained pursuant to section 4872 of title 10, United States Code, may be incorporated into any unmanned system command and control framework developed, procured, or fielded pursuant to this Act.

(c) LIVING STANDARDS PROCESS.—The Secretary shall, in coordination with the Director of the National Security Agency, the Director of the Cybersecurity and Infrastructure Security Agency, and the Chief Information Officer of the Department, establish a process for reviewing and updating the cybersecurity standards applicable to a framework developed pursuant to this Act on a recurring basis of not less than once every 18 months, to ensure

such standards remain current with the evolving threat environment and applicable Federal standards without requiring legislative action.

SEC. 6. COORDINATION WITH EXISTING DEPARTMENT OF DEFENSE PROGRAMS.

(a) REQUIRED COORDINATION.—In conducting the assessment required under section 2, the Secretary shall ensure that the unmanned system command and control framework under consideration is assessed for compatibility with all current Department command and control modernization programs of record, as designated by the Secretary at the time of the assessment. The Secretary shall update this assessment as the portfolio of such programs evolves, ensuring that recommendations remain current with the Department's command and control modernization activities regardless of changes in program names, structures, or priorities.

(b) AVOIDANCE OF DUPLICATION.—In developing recommendations under section 2, the Secretary shall assess whether existing programs of record identified under subsection (a) can be extended or adapted to provide the unmanned system command and control capability described in this Act without developing a wholly new system and shall include in the final report a determination as

to whether such extension or adaptation is technically feasible and operationally preferable.

(c) DOMESTIC UNMANNED AIRCRAFT SYSTEMS INDUSTRIAL BASE COMPATIBILITY.—The Secretary shall ensure that the assessment and any recommended framework account for the domestic small unmanned aircraft systems industrial base remediation efforts undertaken pursuant to section 914 of the National Defense Authorization Act for Fiscal Year 2026 (10 U.S.C. 4811 note), including ensuring that unmanned aircraft systems platforms produced through those programs are compatible with any recommended command and control framework.

SEC. 7. SHARING OF FINDINGS WITH THE FEDERAL AVIATION ADMINISTRATION.

(a) TRANSMISSION OF FINDINGS.—Not later than the date that is 30 days after the date of the submittal of the final report under section 4(b), the Secretary shall transmit to the Administrator of the Federal Aviation Administration an unclassified summary of the findings and recommendations included in the report, with particular attention to findings regarding—

(1) open architecture and modular design principles applicable to unmanned system command and control systems;

(2) cybersecurity standards and frameworks evaluated or recommended for Department unmanned aircraft systems command and control systems that may have applicability to civil unmanned aircraft systems traffic management infrastructure;

(3) technical standards and interface specifications that could support interoperability between military and civil unmanned aircraft systems operations in shared airspace; and

(4) lessons learned from systems of allied and partner countries of the United States, regarding the integration of military, commercial, and civil unmanned aircraft systems operations within a unified airspace management framework.

(b) PURPOSE.—The purpose of subsection (a) is to inform any Federal Aviation Administration planning, rulemaking, or feasibility assessment related to civil unmanned aircraft system traffic management, beyond visual line of sight operations, or national airspace integration, including any activities undertaken pursuant to a feasibility assessment directed by Congress regarding a national unmanned aircraft systems traffic management system. Nothing in this section shall be construed to require the Secretary to disclose any classified information to the Administrator.

(c) FEDERAL AVIATION ADMINISTRATION RESPONSE.—Not later than the date that is 180 days after the date on which the Administrator receives the summary transmitted under subsection (a), the Administrator shall submit to the congressional defense committees, the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on Transportation and Infrastructure of the House of Representatives a written assessment of the relevance of such findings to Federal Aviation Administration civil unmanned aircraft systems airspace integration activities and any actions the Federal Aviation Administration intends to take in response.

SEC. 8. FUNDING.

Amounts obligated or expended by the Secretary to carry out this Act shall be derived from amounts appropriated to the Department for research, development, test, and evaluation.

SEC. 9. DEFINITIONS.

In this Act:

(1) COMMAND AND CONTROL FRAMEWORK.—The term ''command and control framework'' means the software architecture, communications protocols, data standards, interface specifications, and associated hardware that together enable an operator or

commander to task, direct, monitor, and receive data from one or more unmanned aircraft systems.

(2) CONGRESSIONAL DEFENSE COMMITTEES.—The term ''congressional defense committees'' has the meaning given that term in section 101(a) of title 10, United States Code.

(3) DEPARTMENT.—The term ''Department'' means the Department of Defense.

(4) MODULAR OPEN SYSTEMS ARCHITECTURE.—The term ''modular open systems architecture'' has the meaning given to that term in section 4401(c) of title 10, United States Code, and means a design approach in which key interfaces are defined by widely supported and consensus-based standards, enabling components to be added, modified, replaced, or removed with minimal impact to the remainder of the system.

(5) OPEN ARCHITECTURE.—The term ''open architecture'' means a system design based on published, consensus-developed interface standards that permit systems from multiple vendors to interoperate, and that permits components to be updated, replaced, or added without redesign of the system as a whole.

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Defense, unless otherwise specified.