

119TH CONGRESS
2D SESSION

S. 4930

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

JUNE 24, 2026

Mr. McCORMICK (for himself and Ms. ROSEN) introduced the following bill;
which was read twice and referred to the Committee on Armed Services

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Unmanned System
3 Command and Control Integration Assessment Act of
4 2026”.

5 **SEC. 2. ASSESSMENT OF UNMANNED SYSTEM COMMAND**
6 **AND CONTROL FRAMEWORKS.**

7 (a) **ASSESSMENT REQUIRED.**—Not later than 180
8 days after the date of the enactment of this Act, the Sec-
9 retary shall, in coordination with the Chairman of the
10 Joint Chiefs of Staff, the Under Secretary of Defense for
11 Acquisition and Sustainment, the Secretary of Defense for
12 Research and Engineering, the Chief Information Officer,
13 Joint Interagency Task Force 401, the Director of the De-
14 fense Information Systems Agency, the Commander of
15 Joint Interoperability Test Command, and the Secretaries
16 of the military departments, commence a comprehensive
17 assessment of open-architecture, unmanned system com-
18 mand and control frameworks with demonstrated oper-
19 ational effectiveness.

20 (b) **SCOPE OF ALLIED AND PARTNER SYSTEM RE-**
21 **VIEW.**—The assessment commenced under subsection (a)
22 shall review each of the following allied and partner coun-
23 try unmanned systems command and control frameworks
24 and may include such additional frameworks as the Sec-
25 retary determines appropriate:

1 (1) Ukraine’s Delta battlefield management and
2 unmanned aircraft systems coordination system, in-
3 cluding an analysis of its technical architecture, its
4 operational effectiveness in contested environments,
5 the interoperability and integration lessons learned
6 from its deployment that are applicable to United
7 States Armed Forces unmanned aircraft systems
8 command and control operations, and its cybersecu-
9 rity resilience under active electronic warfare and
10 cyber attack.

11 (2) Israel’s Multiple Drone Operating System,
12 including an analysis of its technical architecture, its
13 demonstrated operational effectiveness in managing
14 simultaneous civilian, commercial, and military un-
15 manned aircraft systems operations, the interoper-
16 ability and integration lessons learned from its de-
17 ployment that are applicable to United States Armed
18 Forces unmanned aircraft systems command and
19 control operations, and its cybersecurity and emer-
20 gency prioritization mechanisms.

21 (c) ELEMENTS OF ASSESSMENT.—The assessment
22 commenced under subsection (a) shall address, at a min-
23 imum, each of the following elements:

24 (1) Architectural analysis, including—

1 (A) a comparative analysis of the technical
2 architectures of the unmanned systems com-
3 mand and control frameworks reviewed, includ-
4 ing data formats, communication protocols,
5 interface standards, and software design ap-
6 proaches;

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

11 (C) an identification of the architectural
12 characteristics most associated with operational
13 effectiveness, adaptability, and resilience in con-
14 tested environments.

15 (2) Unmanned systems tier compatibility, in-
16 cluding—

17 (A) an evaluation of each framework's ca-
18 pacity to manage all unmanned systems within
19 a single integrated command and control envi-
20 ronment;

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

1 (C) a recommendation for the minimum
2 capability requirements a Department un-
3 manned systems command and control frame-
4 work must meet to support effective employ-
5 ment of unmanned systems across all in a joint
6 operational environment.

7 (3) Interoperability with existing Department
8 systems, including—

9 (A) a detailed assessment of the compat-
10 ibility and interoperability requirements for in-
11 tegrating an open-architecture unmanned sys-
12 tem command and control framework with cur-
13 rent and future Department command and con-
14 trol modernization, as designated by the Sec-
15 retary at the time of the assessment;

16 (B) an identification of the interface stand-
17 ards, data translation requirements, and tech-
18 nical integration pathways that would be nec-
19 essary to achieve such interoperability; and

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

24 (4) Cybersecurity and future-proofing, includ-
25 ing—

1 (A) an assessment of the cybersecurity
2 posture of each framework reviewed, including
3 its resilience to electronic warfare, Global Posi-
4 tioning System denial, communications jam-
5 ming, and software-based cyber attack in active
6 contested environments;

7 (B) a recommendation for a cybersecurity
8 standards framework or updates to the Risk
9 Management Framework of the National Insti-
10 tute of Standards and Technology applicable to
11 a Department unmanned system command and
12 control system that—

13 (i) is based on the Cybersecurity
14 Framework 2.0, published by the National
15 Institute of Standards and Technology,
16 and applicable special publications of the
17 Institute, and is designed to incorporate
18 updated guidance from the Institute with-
19 out requiring legislative action;

20 (ii) incorporates a comprehensive sup-
21 ply chain risk management strategy;

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

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

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

9 (v) specifies a recurring review cycle
10 of not less than once every 18 months to
11 update cybersecurity standards as the Na-
12 tional Institute of Standards and Tech-
13 nology and other relevant standards bodies
14 publish new guidance, without requiring
15 legislative action; and

16 (vi) mandates alignment with Zero
17 Trust Architecture (ZTA), ensuring all
18 data, applications, assets, and services are
19 managed with the assumption that the net-
20 work is already compromised;

21 (C) an assessment of how the architecture
22 of the framework can accommodate future un-
23 manned systems technologies, including autono-
24 mous systems, artificial intelligence-enabled tar-
25 geting and deconfliction, swarming capabilities,

1 and beyond-visual-line-of-sight operations, with-
2 out requiring full system replacement; and

3 (D) a recommended technology refresh
4 cycle and associated governance process for
5 keeping a Department unmanned system com-
6 mand and control framework current with ad-
7 vancing technology and evolving threats.

8 (5) Tactical adaptability and field-level flexi-
9 bility, including—

10 (A) an assessment of the mechanisms with-
11 in each framework reviewed that enable tac-
12 tical-level operators and commanders to modify,
13 adapt, or extend command and control
14 functionality without depending on centralized
15 software updates or acquisition processes, draw-
16 ing on documented examples from the conflict
17 in Ukraine where unmanned aircraft systems
18 tactics evolved within weeks in response to ad-
19 versary countermeasures;

20 (B) a recommended design approach for a
21 Department framework that preserves appro-
22 priate security and safety controls while ena-
23 bling tactical-level customization, including
24 through the use of application programming

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

3 (C) an assessment of the doctrinal, train-
4 ing, and organizational changes required to en-
5 able and sustain field-level innovation within a
6 structured command and control architecture.

7 (6) Classification and technology transfer, in-
8 cluding—

9 (A) an assessment of the classification im-
10 plications of a Department unmanned system
11 command and control framework, including rec-
12 ommendations for which components may oper-
13 ate at unclassified levels to maximize interoper-
14 ability with allied and commercial systems, and
15 which must be classified;

16 (B) an assessment of the technology trans-
17 fer and foreign military sales implications of the
18 frameworks reviewed, including intellectual
19 property and national security considerations
20 associated with adopting or adapting systems
21 developed by or with foreign partners; and

22 (C) recommendations for information-shar-
23 ing arrangements with other United States
24 Government organizations, allies, and partner
25 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

1 and technical guidance to the assessment required under
2 section 2.

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

6 (1) not fewer than two individuals who have di-
7 rect operational experience in unmanned aircraft
8 systems employment in a joint or combined military
9 environment;

10 (2) not fewer than two individuals who have
11 technical expertise in open-architecture software sys-
12 tems, modular systems design, or command and con-
13 trol software architecture;

14 (3) not fewer than two individuals who have ex-
15 pertise in cybersecurity, including experience with
16 operational technology cybersecurity in contested en-
17 vironments;

18 (4) at least three individuals who have expertise
19 in unmanned aircraft systems command and control
20 operations, doctrine, or command and control from
21 an allied or partner country with significant un-
22 manned aircraft systems operational experience, ap-
23 pointed in coordination with relevant allied or part-
24 ner country authorities;

1 (5) at least one individual with experience in
2 unmanned aircraft system (UAS) traffic manage-
3 ment in the National Airspace System; and

4 (6) such additional members as the Secretary
5 determines appropriate, which may include rep-
6 resentatives from the defense industrial base, feder-
7 ally funded research and development centers, aca-
8 demic institutions with relevant expertise, and the
9 Department of Defense test and evaluation commu-
10 nity to ensure early consideration to interoperability,
11 testability, and certification requirements.

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

16 (d) DUTIES.—The Panel shall provide written assess-
17 ments and recommendations on each element of the as-
18 sessment described in section 2(c) and shall have the op-
19 portunity to review and comment on draft findings before
20 finalization.

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

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

1 Government shall be compensated at a daily rate equal
2 to the daily equivalent of the annual rate of basic pay for
3 level IV of the Executive Schedule under section 5315 of
4 title 5, United States Code, for each day they are engaged
5 in the performance of Panel duties and shall be allowed
6 travel expenses as authorized under section 5703 of title
7 5, United States Code.

8 **SEC. 4. REPORTS TO CONGRESS.**

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

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

17 (2) a summary of findings from the architec-
18 tural analysis required under section 2(c)(1);

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

21 (4) any significant findings or challenges identi-
22 fied to date.

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

1 port containing the complete findings and recommenda-
2 tions of the Secretary with respect to the assessment re-
3 quired under section 2. The final report shall include—

4 (1) a determination as to whether the develop-
5 ment of a Department unmanned system command
6 and control framework based on open-architecture
7 principles is feasible, operationally necessary, and
8 cost-effective;

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

13 (3) if the determination under paragraph (1) is
14 negative or qualified, a description of the specific
15 barriers identified and recommendations for address-
16 ing them; and

17 (4) a classified annex, as appropriate, con-
18 taining any elements that the Secretary determines
19 must be protected from public disclosure for national
20 security reasons.

21 (c) FORM.—Reports required under this section shall
22 be submitted in unclassified form, but may include a clas-
23 sified annex. Unclassified portions shall be made publicly
24 available on the Department public website not later than
25 30 days after submission.

1 (d) ANNUAL UPDATE.—For a period of five years fol-
2 lowing submission of the final report under subsection (b),
3 the Secretary shall submit to the congressional defense
4 committees, as part of the annual budget justification ma-
5 terials submitted to Congress in support of the budget of
6 the Department (as submitted with the budget of the
7 President under section 1105(a) of title 31, United States
8 Code), an update describing—

9 (1) actions taken by the Department in re-
10 sponse to the recommendations of the Secretary con-
11 tained in the final report;

12 (2) material changes in allied or partner coun-
13 try unmanned systems command and control frame-
14 works or practices relevant to the assessment’s con-
15 clusions;

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

19 (4) the status of any pilot programs, exercises,
20 or acquisition activities initiated pursuant to the rec-
21 ommendations of the Secretary contained in the
22 final report.

1 **SEC. 5. CYBERSECURITY STANDARDS FOR ANY REC-**
2 **OMMENDED FRAMEWORK.**

3 (a) REQUIREMENTS.—Any unmanned system com-
4 mand and control framework recommended in the final re-
5 port required under section 4(b), and any system devel-
6 oped or procured pursuant to such a recommendation,
7 shall—

8 (1) employ a modular open systems architecture
9 that permits individual software and hardware com-
10 ponents to be updated, replaced, or patched in re-
11 sponse to identified cybersecurity vulnerabilities
12 without requiring redesign of the system as a whole;

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

16 (3) comply with the most current version of the
17 Cybersecurity Framework 2.0 published by the Na-
18 tional Institute of Standards and Technology and
19 applicable special publications of the Institute, as
20 updated from time to time, without requiring
21 amendment of this Act to conform to new guidance;

22 (4) include a documented vulnerability disclo-
23 sure policy and a process for receiving, triaging, and
24 patching reported vulnerabilities within defined re-
25 sponse time standards established by the Secretary;
26 and

1 (5) undergo penetration testing by a National
2 Security Agency-certified red team not less fre-
3 quently than once every two years following initial
4 fielding, with findings reported to the Principal
5 Cyber Advisor and, in summary form, to the con-
6 gressional defense committees.

7 (b) EXCLUSION OF COVERED FOREIGN ENTITIES.—
8 No software, hardware, or service produced, provided, or
9 operated by an entity on the Federal Communications
10 Commission Covered List established under section 2 of
11 the Secure and Trusted Communications Networks Act of
12 2019 (47 U.S.C. 1601), or on the Department of Defense
13 Covered Foreign Entity list maintained pursuant to sec-
14 tion 4872 of title 10, United States Code, may be incor-
15 porated into any unmanned system command and control
16 framework developed, procured, or fielded pursuant to this
17 Act.

18 (c) LIVING STANDARDS PROCESS.—The Secretary
19 shall, in coordination with the Director of the National
20 Security Agency, the Director of the Cybersecurity and In-
21 frastructure Security Agency, and the Chief Information
22 Officer of the Department, establish a process for review-
23 ing and updating the cybersecurity standards applicable
24 to a framework developed pursuant to this Act on a recur-
25 ring basis of not less than once every 18 months, to ensure

1 such standards remain current with the evolving threat en-
2 vironment and applicable Federal standards without re-
3 quiring legislative action.

4 **SEC. 6. COORDINATION WITH EXISTING DEPARTMENT OF**
5 **DEFENSE PROGRAMS.**

6 (a) **REQUIRED COORDINATION.**—In conducting the
7 assessment required under section 2, the Secretary shall
8 ensure that the unmanned system command and control
9 framework under consideration is assessed for compat-
10 ibility with all current Department command and control
11 modernization programs of record, as designated by the
12 Secretary at the time of the assessment. The Secretary
13 shall update this assessment as the portfolio of such pro-
14 grams evolves, ensuring that recommendations remain
15 current with the Department’s command and control mod-
16 ernization activities regardless of changes in program
17 names, structures, or priorities.

18 (b) **AVOIDANCE OF DUPLICATION.**—In developing
19 recommendations under section 2, the Secretary shall as-
20 sess whether existing programs of record identified under
21 subsection (a) can be extended or adapted to provide the
22 unmanned system command and control capability de-
23 scribed in this Act without developing a wholly new system
24 and shall include in the final report a determination as

1 to whether such extension or adaptation is technically fea-
 2 sible and operationally preferable.

3 (c) DOMESTIC UNMANNED AIRCRAFT SYSTEMS IN-
 4 DUSTRIAL BASE COMPATIBILITY.—The Secretary shall
 5 ensure that the assessment and any recommended frame-
 6 work account for the domestic small unmanned aircraft
 7 systems industrial base remediation efforts undertaken
 8 pursuant to section 914 of the National Defense Author-
 9 ization Act for Fiscal Year 2026 (10 U.S.C. 4811 note),
 10 including ensuring that unmanned aircraft systems plat-
 11 forms produced through those programs are compatible
 12 with any recommended command and control framework.

13 **SEC. 7. SHARING OF FINDINGS WITH THE FEDERAL AVIA-**
 14 **TION ADMINISTRATION.**

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

22 (1) open architecture and modular design prin-
 23 ciples applicable to unmanned system command and
 24 control systems;

1 (2) cybersecurity standards and frameworks
2 evaluated or recommended for Department un-
3 manned aircraft systems command and control sys-
4 tems that may have applicability to civil unmanned
5 aircraft systems traffic management infrastructure;

6 (3) technical standards and interface specifica-
7 tions that could support interoperability between
8 military and civil unmanned aircraft systems oper-
9 ations in shared airspace; and

10 (4) lessons learned from systems of allied and
11 partner countries of the United States, regarding
12 the integration of military, commercial, and civil un-
13 manned aircraft systems operations within a unified
14 airspace management framework.

15 (b) PURPOSE.—The purpose of subsection (a) is to
16 inform any Federal Aviation Administration planning,
17 rulemaking, or feasibility assessment related to civil un-
18 manned aircraft system traffic management, beyond visual
19 line of sight operations, or national airspace integration,
20 including any activities undertaken pursuant to a feasi-
21 bility assessment directed by Congress regarding a na-
22 tional unmanned aircraft systems traffic management sys-
23 tem. Nothing in this section shall be construed to require
24 the Secretary to disclose any classified information to the
25 Administrator.

1 (c) FEDERAL AVIATION ADMINISTRATION RE-
2 SPONSE.—Not later than the date that is 180 days after
3 the date on which the Administrator receives the summary
4 transmitted under subsection (a), the Administrator shall
5 submit to the congressional defense committees, the Com-
6 mittee on Commerce, Science, and Transportation of the
7 Senate, and the Committee on Transportation and Infra-
8 structure of the House of Representatives a written as-
9 sessment of the relevance of such findings to Federal Avia-
10 tion Administration civil unmanned aircraft systems air-
11 space integration activities and any actions the Federal
12 Aviation Administration intends to take in response.

13 **SEC. 8. FUNDING.**

14 Amounts obligated or expended by the Secretary to
15 carry out this Act shall be derived from amounts appro-
16 priated to the Department for research, development, test,
17 and evaluation.

18 **SEC. 9. DEFINITIONS.**

19 In this Act:

20 (1) **COMMAND AND CONTROL FRAMEWORK.**—

21 The term “command and control framework” means
22 the software architecture, communications protocols,
23 data standards, interface specifications, and associ-
24 ated hardware that together enable an operator or

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

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

7 (3) DEPARTMENT.—The term “Department”
8 means the Department of Defense.

9 (4) MODULAR OPEN SYSTEMS ARCHITEC-
10 TURE.—The term “modular open systems architec-
11 ture” has the meaning given to that term in section
12 4401(c) of title 10, United States Code, and means
13 a design approach in which key interfaces are de-
14 fined by widely supported and consensus-based
15 standards, enabling components to be added, modi-
16 fied, replaced, or removed with minimal impact to
17 the remainder of the system.

18 (5) OPEN ARCHITECTURE.—The term “open
19 architecture” means a system design based on pub-
20 lished, consensus-developed interface standards that
21 permit systems from multiple vendors to inter-
22 operate, and that permits components to be updated,
23 replaced, or added without redesign of the system as
24 a whole.

- 1 (6) SECRETARY.—The term “Secretary” means
2 the Secretary of Defense, unless otherwise specified.

