

119TH CONGRESS
2D SESSION

S. 4697

To provide for design and safety requirements for autonomous and semi-autonomous weapon systems, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 8, 2026

Mr. SCHIFF introduced the following bill; which was read twice and referred to the Committee on Armed Services

A BILL

To provide for design and safety requirements for autonomous and semi-autonomous weapon 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,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Human Authority in
5 Lethal Operations Act of 2026” or the “HALO Act of
6 2026”.

7 **SEC. 2. DEFINITIONS.**

8 In this Act:

1 (1) APPROPRIATE COMMITTEES OF CON-
2 GRESS.—The term “appropriate committees of Con-
3 gress” means—

4 (A) the Select Committee on Intelligence,
5 the Committee on Armed Services, and the
6 Committee on the Judiciary of the Senate; and

7 (B) the Permanent Select Committee on
8 Intelligence, the Committee on Armed Services,
9 and the Committee on the Judiciary of the
10 House of Representatives.

11 (2) ARTIFICIAL INTELLIGENCE.—The term “ar-
12 tificial intelligence” has the meaning given such
13 term in section 5002 of the National Artificial Intel-
14 ligence Initiative Act of 2020 (15 U.S.C. 9401).

15 (3) AUTONOMOUS WEAPON SYSTEM.—

16 (A) IN GENERAL.—The term “autonomous
17 weapon system” means a weapon system that,
18 once activated, can identify, select, or engage
19 targets without further intervention by or com-
20 munication with a human operator.

21 (B) INCLUDES.—The term defined in sub-
22 paragraph (A) includes weapon systems that
23 have human-operated supervision with the abil-
24 ity to override complete operation of the system,
25 but can select and engage targets without fur-

1 ther human operator input, recalibration, or
2 communication after activation.

3 (4) COVERED ARTIFICIAL INTELLIGENCE CAPA-
4 BILITY.—The term “covered artificial intelligence ca-
5 pability” means an artificial intelligence designed,
6 tested, developed, procured, deployed, or used by, on
7 behalf of, or shared with the Department.

8 (5) DESIGNATED COMMANDER.—The term
9 “designated commander” means the highest ranking
10 commissioned officer within the chain of command
11 who exercises operational or administrative com-
12 mand authority over an autonomous or semi-autono-
13 mous weapons system.

14 (6) DEPARTMENT.—The term “Department”
15 means Department of Defense.

16 (7) ETHICAL PRINCIPLES FOR ARTIFICIAL IN-
17 TELLIGENCE.—The term “Ethical Principles for Ar-
18 tificial Intelligence” means the Ethical Principles for
19 Artificial Intelligence adopted by the Department on
20 February 24, 2020, as in effect on January 1, 2025.

21 (8) MILITARY DEPARTMENTS.—The term “mili-
22 tary departments” has the meaning given such term
23 in section 101(a) of title 10, United States Code.

24 (9) RESPONSIBLE ARTIFICIAL INTELLIGENCE
25 STRATEGY AND IMPLEMENTATION PATHWAY.—The

1 term “Responsible Artificial Intelligence Strategy
2 and Implementation Pathway” means the Respon-
3 sible Artificial Intelligence Strategy and Implemen-
4 tation Pathway dated June 2022 and prepared by
5 the Department of Defense Responsible Artificial In-
6 telligence Working Council in accordance with the
7 memorandum issued by Deputy Secretary of Defense
8 Kathleen Hicks on May 26, 2021, Implementing Re-
9 sponsible Artificial Intelligence in the Department of
10 Defense, as in effect on January 1, 2025.

11 (10) SECRETARY.—The term “Secretary”
12 means the Secretary of Defense.

13 (11) SEMI-AUTONOMOUS WEAPON SYSTEM.—

14 (A) IN GENERAL.—The term “semi-auton-
15 omous weapon system” means a weapon system
16 that, once activated, is intended to only engage
17 individual targets or specific target groups that
18 have been previously selected by a human oper-
19 ator.

20 (B) INCLUDED.—The term defined in sub-
21 paragraph (A) includes weapon systems that
22 autonomously conduct engagement-related func-
23 tions, including the following:

24 (i) Acquiring, tracking, and identi-
25 fying potential targets.

1 (ii) Cuing potential targets to human
2 operators.

3 (iii) Prioritizing selected targets.

4 (iv) Providing input on timing of
5 when to fire.

6 (v) Providing terminal guidance on
7 how to narrowly categorize selected tar-
8 gets, only if human operator control is re-
9 tained for the purpose of selecting indi-
10 vidual targets and specific target groups
11 for engagement.

12 (12) SPECIFIC TARGET GROUP.—

13 (A) IN GENERAL.—The term “specific tar-
14 get group” means a discrete group of potential
15 targets, such as a particular flight of enemy
16 aircraft, a particular formation of enemy tanks,
17 or a particular flotilla of enemy vessels.

18 (B) EXCLUDED.—The term defined in sub-
19 paragraph (A) does not include a general class
20 of targets or a specific type of target, such as
21 a particular model of tank or aircraft.

22 (13) UNINTENDED ENGAGEMENT.—The term
23 “unintended engagement” means the use of force
24 outcomes resulting in damage to persons or objects
25 that human operators did not intend to be the tar-

gets of United States military operations, including levels of collateral damage beyond those consistent with the Law of Armed Conflict and relevant laws of the United States and international laws, applicable rules of engagement, and commander's intent.

SEC. 3. DESIGN AND SAFETY REQUIREMENTS FOR AUTONOMOUS AND SEMI-AUTONOMOUS WEAPON SYSTEMS.

(a) GENERAL REQUIREMENT.—

(1) IN GENERAL.—The Secretary shall, acting through each of the Secretaries of the military departments, ensure that whenever the Department designs, tests, develops, procures, deploys, or uses a system described in paragraph (2), the system meets the requirements of this section.

(2) SYSTEMS.—A system described in this paragraph is an autonomous weapon system or semi-autonomous weapon system that uses artificial intelligence to create, generate, prioritize, recommend, or engage targets or courses of action in support of use of force decisions.

(b) HUMAN RESPONSIBILITY OVER USE OF FORCE.—

(1) ACCOUNTABLE INDIVIDUALS.—For each system described in subsection (a)(2)—

1 (A) not later than 90 days after the date
2 of the enactment of this Act, the Secretary shall
3 promulgate rules for clear chain of command
4 and command hierarchy for military operations
5 involving a system described in subsection
6 (a)(2) to mirror the chain of command and
7 command hierarchy for military operations that
8 do not involve such systems;

9 (B) the Secretary shall ensure that a des-
10 ignated commander is identified as accountable
11 under applicable military and international laws
12 for each engagement or class of engagements
13 involving a system described in subsection
14 (a)(2), regardless of the degree to which artifi-
15 cial intelligence contributed to the identifica-
16 tion, development, recommendation, selection,
17 or engagement of the target; and

18 (C) the designated commander identified
19 under subparagraph (B) shall exercise ultimate
20 discretion, judgment, and control over the use
21 of force.

22 (2) SYSTEM REQUIREMENTS.—Each system de-
23 scribed in subsection (a)(2) shall incorporate the fol-
24 lowing:

1 (A) A system design that incorporates ca-
2 pabilities and interfaces that require the des-
3 ignated commander to exercise ultimate discre-
4 tion, judgment and control in the envisioned de-
5 velopment, planning, deployment, and use proc-
6 esses for the weapon system, including con-
7 straints on each such system's authorized ac-
8 tions, targets, and geographic, temporal, and
9 contextual scope, which the system may not ex-
10 pand or modify without explicit human author-
11 ization.

12 (B) System capabilities, human-machine
13 interfaces, doctrine, tactics, techniques, proce-
14 dures, and human operator training must re-
15 quire commanders and human operators to use
16 the system with deference to their discretion re-
17 garding care, and to analyze the output, in ac-
18 cordance with the Law of Armed Conflict and
19 relevant laws of the United States and inter-
20 national laws, applicable treaties, weapon sys-
21 tem safety rules, and rules of engagement that
22 are applicable or reasonably expected to be ap-
23 plicable.

24 (C) The creation and ongoing maintenance
25 of records of target selection data, decision

1 logic, and human operator actions, including
2 the individual designated under subsection
3 (b)(1)(B), sufficiently detailed to enable post-
4 engagement review of compliance.

5 (D) The design, testing, development, pro-
6 curement, deployment, legal analysis and re-
7 view, and use of artificial intelligence capabili-
8 ties in autonomous and semi-autonomous weap-
9 on systems shall be consistent with, but not
10 limited to, the Ethical Principles for Artificial
11 Intelligence and the Responsible Artificial Intel-
12 ligence Strategy and Implementation Pathway.

13 (3) AVAILABILITY TO THE PUBLIC.—The Sec-
14 retary shall ensure that—

15 (A) the Ethical Principles for Artificial In-
16 telligence and the Responsible Artificial Intel-
17 ligence Strategy and Implementation Pathway
18 are available to the public; and

19 (B) any revision to the Ethical Principles
20 for Artificial Intelligence or the Responsible Ar-
21 tificial Intelligence Strategy and Implementa-
22 tion Pathway adopted by the Secretary is made
23 available to the public before the date that is 30
24 days before the date on which the revision goes
25 into effect.

1 (c) ENGAGEMENT CONSTRAINTS AND TERMI-
2 NATION.—

3 (1) IN GENERAL.—Each system described in
4 subsection (a)(2) shall be designed—

5 (A) to complete engagements within a des-
6 igned timeframe and designated geographic
7 area and against a designated set of potential
8 targets, as well as other relevant constraints,
9 consistent with commander and human operator
10 intentions;

11 (B) to require independent review and
12 analysis of a designated commander before
13 using force against previously unauthorized tar-
14 gets, materially expanding target sets or geo-
15 graphic scope, taking actions contravening ap-
16 plicable law, rules of engagement, other relevant
17 laws of the United States and international
18 laws, or taking actions likely to result in unin-
19 tended engagement; and

20 (C) if unable to complete an engagement
21 consistent with the parameters described in
22 paragraph (1), to terminate the engagement
23 until additional human operator and com-
24 mander evaluation is completed.

1 (2) EVALUATION CRITERIA.—The evaluation
2 criteria used under subparagraph (C) of paragraph
3 (1) shall consist of assessment of deficiencies and
4 recommendations for changes to be compliant with
5 subparagraph (A) of such paragraph before restart-
6 ing preparation for engagement.

7 (d) TRANSPARENCY, AUDITABILITY, AND
8 EXPLAINABILITY.—Consistent with the potential con-
9 sequences of an unintended engagement or unauthorized
10 interference with the operation of a system described in
11 subsection (a)(2), the physical hardware and software of
12 such system shall be designed with—

13 (1) technologies and data sources that are
14 available to, auditable by, and explainable to the
15 greatest extent possible by relevant personnel of the
16 Department with the necessary clearance level; and

17 (2) system safety, anti-tamper mechanisms, and
18 cybersecurity in accordance with Department in-
19 structions and military standards governing cyberse-
20 curity and system safety.

21 (e) ACTIVATION, TERMINATION, AND HUMAN OPER-
22 ATOR INTERFACE.—Each system described in subsection
23 (a)(2) shall be designed so that—

24 (1) system design and human-machine inter-
25 faces are readily understandable to trained human

1 operators, including by clearly disaggregating which
2 actions human operators need to perform and which
3 actions the weapon system will perform;

4 (2) clear procedures exist for trained human op-
5 erators to activate, terminate, and disable all weapon
6 system functions;

7 (3) the system provides timely feedback on sys-
8 tem status, including regarding the quality and suf-
9 ficiency of the data inputs relied upon, to human op-
10 erators in real time or near-real time; and

11 (4) adequate training, tactics, techniques, pro-
12 cedures, and doctrine are available, reviewed on a
13 quarterly basis, by weapon system human operators
14 and designated commanders to understand the func-
15 tioning, capabilities, and limitations of the system's
16 autonomy in realistic operational conditions.

17 (f) DEGRADED COMMUNICATIONS SAFEGUARD.—Any
18 autonomous or semi-autonomous weapon system that is,
19 or is part of, an unmanned platform shall be designed such
20 that, in the event of degraded or lost communications, the
21 system does not autonomously select and engage indi-
22 vidual targets, specific target groups, or general classes
23 or specific types of targets that have not been previously
24 selected by an authorized human operator.

1 (g) CONTINUOUS MONITORING.—The Secretary
2 shall, in coordination with the Director of Operational
3 Test and Evaluation, the Under Secretary of Defense for
4 Research and Engineering, and the appropriate Secretary
5 of a military department or Assistant Secretary for Spe-
6 cial Operations and Low-Intensity Conflict, establish and
7 maintain procedures for continuous monitoring of each
8 system, to the greatest extent possible, described in sub-
9 section (a)(2) to identify and address circumstances in
10 which changes to the system design or operational environ-
11 ment require additional testing and evaluation or legal re-
12 view to provide sufficient confidence that the system will
13 continue—

- 14 (1) to function as intended;
15 (2) to avoid unintended engagements;
16 (3) to resist interference by unauthorized par-
17 ties; and
18 (4) to remain compliant with relevant laws of
19 the United States, the Law of Armed Conflict, and
20 international laws.

21 (h) ROBUST ARTIFICIAL INTELLIGENCE DESIGN.—
22 For any system described in subsection (a) that incor-
23 porates artificial intelligence capabilities, such system
24 shall be designed to utilize robust artificial intelligence, in
25 accordance with the Responsible Artificial Intelligence

1 Strategy and Implementation Pathway so that the system
2 is resilient in real-world settings and against adversarial
3 attacks and spoofing.

4 **SEC. 4. ADVANCED REVIEW AND APPROVAL AUTHORITY.**

5 (a) GENERAL REQUIREMENT FOR ADVANCED RE-
6 VIEW.—With the exception of systems described in sub-
7 section (e), the Secretary shall ensure that each system
8 described in section 3(a)(2) is approved in accordance with
9 this section before formal development and before fielding.

10 (b) PRE-DEVELOPMENT REVIEW.—Before a decision
11 to enter formal development of a system described in sub-
12 section (a), the Under Secretary of Defense for Policy, the
13 Under Secretary of Defense for Research and Engineer-
14 ing, and the Vice Chairman of the Joint Chiefs of Staff
15 shall jointly verify that—

16 (1) the weapon system design incorporates the
17 necessary capabilities to allow a designated com-
18 mander to exercise ultimate discretion, judgment,
19 and control over the use of force in the envisioned
20 planning, deployment, and use processes for the
21 weapon;

22 (2) the system is designed to complete engage-
23 ments within a designated timeframe and designated
24 geographic area and against a designated set of po-
25 tential targets, as well as other applicable param-

eters, consistent with designated commander intentions, and if unable to do so, to terminate use until additional human operator and commander evaluation is completed before continuing the engagement;

(3) the combination of the system's design and concept of use, including its target selection and engagement logic, accounts for risks of armed conflict, including to civilians, civilian populations, civilian objects, and other protected entities, consistent with commander and human operator intent and obligations under the Law of Armed Conflict, or other relevant laws of the United States and international laws;

(4) the system design, including system safety, anti-tamper mechanisms, and cybersecurity, addresses and minimizes the probability and consequences of failures;

(5) plans are in place for verification and validation and test and evaluation to establish system reliability, effectiveness, predictability of effects, and accuracy under realistic conditions, including possible adversary actions, interference, or unintended consequences;

(6) for systems incorporating artificial intelligence capabilities, plans are in place to ensure con-

1 sistency with the Ethical Principles for Artificial In-
2 telligence and the Responsible Artificial Intelligence
3 Strategy and Implementation Pathway; and

4 (7) a thorough legal analysis, review, and risk
5 assessment of a system described in subsection (a)
6 has been completed in coordination with the General
7 Counsel of the Department and other relevant De-
8 partment General Counsels and in accordance with
9 applicable directives governing the Defense Acquisi-
10 tion System, the Department of Defense Law of
11 War Program, the Law of Armed Conflict, and other
12 relevant laws of the United States and international
13 laws.

14 (c) PRE-FIELDING REVIEW.—Before fielding a sys-
15 tem described in subsection (a), the Under Secretary of
16 Defense for Policy, the Under Secretary of Defense for
17 Acquisition and Sustainment, and the Vice Chairman of
18 the Joint Chiefs of Staff shall jointly verify that—

19 (1) system capabilities, human-machine inter-
20 faces, doctrine, tactics, techniques, procedures, and
21 training have been demonstrated to allow a des-
22 ignated commander to exercise ultimate discretion,
23 control, and judgment over the use of force and to
24 use systems whose outcomes are sufficiently accurate
25 with thorough legal analysis in accordance with the

1 law of war, Law of Armed Conflict, applicable trea-
2 ties, weapon system safety rules, and rules of en-
3 gagement reasonably expected to be applicable;

4 (2) system safety, anti-tamper mechanisms,
5 cyber survivability, operational resilience, and cyber-
6 security capabilities have been implemented to mini-
7 mize the probability and consequences of failures, in-
8 cluding unpredictable outcomes, and a monitoring
9 protocol is in place to identify and address changes
10 in operational environment, data inputs, and use
11 that could contribute to such failures;

12 (3) verification and validation and test and
13 evaluation have—

14 (A) assessed system performance, capa-
15 bility, reliability, risk margins, effectiveness,
16 and suitability under realistic conditions, in-
17 cluding possible adversary actions, interference,
18 or unintended consequences; and

19 (B) have demonstrated that the system can
20 be revised as needed with sufficient rapidity to
21 enable timely correction of any unintended sys-
22 tem behaviors that may be observed or discov-
23 ered during future system operations;

24 (4) adequate training, tactics, techniques, pro-
25 cedures, and doctrine are available, quarterly re-

1 viewed, and used by system operators and com-
2 manders to understand the functioning, capabilities,
3 and limitations of the system in real world condi-
4 tions;

5 (5) system design and human-machine inter-
6 faces are readily understandable to trained human
7 operators, provide transparent feedback on system
8 status, provide secure logging to enable traceability,
9 and provide clear procedures for trained human op-
10 erators to activate and terminate system functions;

11 (6) for systems incorporating artificial intel-
12 ligence capabilities, the deployment and use of such
13 capabilities in the weapon system will be consistent
14 with the Ethical Principles for Artificial Intelligence,
15 the Responsible Artificial Intelligence Strategy and
16 Implementation Pathway, the Law of Armed Con-
17 flict, and other relevant laws of the United States
18 and international laws; and

19 (7) a legal review of the compliance of the
20 weapon system with the Defense Acquisition System,
21 the Department of Defense Law of War Program,
22 the Law of Armed Conflict, and other relevant laws
23 of the United States and international laws has been
24 completed in coordination with the General Counsel
25 of the Department.

1 (d) RE-REVIEW OF MODIFIED SYSTEMS.—A system
 2 described in subsection (a) that is a variant of an existing
 3 weapon system previously approved through the review
 4 process under this section shall not be covered by previous
 5 approval if changes to the system algorithms, intended
 6 mission set, intended operational environments, intended
 7 target sets, or expected adversarial countermeasures mate-
 8 rially differ from those applicable to the previously ap-
 9 proved weapon system. Such systems shall require a new
 10 analysis, review, and risk assessment before formal devel-
 11 opment and again before fielding.

12 (e) SYSTEMS NOT REQUIRING ADVANCED REVIEW.—

13 (1) IN GENERAL.—Except as provided in para-
 14 graph (2), the advance review described in this sec-
 15 tion is not required for weapon systems intended to
 16 be used in the following manners:

17 (A) Semi-autonomous weapon systems
 18 used to apply lethal or non-lethal, kinetic or
 19 non-kinetic, force without capability to function
 20 as an autonomous weapon system.

21 (B) Human operator-supervised autono-
 22 mous weapon systems used to select and engage
 23 materiel targets for local defense to intercept
 24 attempted time-critical or saturation attacks
 25 for—

- 1 (i) static defense of installations with
2 personnel, including networked defense
3 where the autonomous weapon system is
4 not co-located with the installation; or
5 (ii) onboard or networked defense of
6 platforms with onboard personnel.

7 (C) Human operator-supervised autono-
8 mous weapon systems used to select and engage
9 materiel targets for purpose of protecting re-
10 motely piloted or autonomous vehicles and ves-
11 sels.

12 (D) Autonomous weapon systems used to
13 apply non-lethal, non-kinetic force against ma-
14 teriel targets.

15 (2) EXCEPTION.—Paragraph (1) shall not
16 apply to a weapon system intended to be used in the
17 manner described in subparagraph (B) of such para-
18 graph in a case in which the engagement zone for
19 the system encompasses densely populated areas or
20 essential civilian infrastructure. In such a case, the
21 weapon system shall undergo the advanced review
22 described in this section to certify that the system
23 can effectively distinguish between military targets
24 and non-combatants or civilian objects in high-clut-
25 ter environments.

1 **SEC. 5. ROLE OF THE CHIEF DIGITAL AND ARTIFICIAL IN-**
2 **TELLIGENCE OFFICER.**

3 (a) MONITORING AND EVALUATION.—The Chief Dig-
4 ital and Artificial Intelligence Officer shall monitor and
5 evaluate artificial intelligence capabilities in, and cyberse-
6 curity for, autonomous and semi-autonomous weapon sys-
7 tems, and shall advise the Secretary on such matters.

8 (b) TESTABLE REQUIREMENTS.—The Chief Digital
9 and Artificial Intelligence Officer shall, in collaboration
10 with the Under Secretary of Defense for Research and En-
11 gineering—

12 (1) formulate concrete, testable requirements
13 for implementing the Ethical Principles for Artificial
14 Intelligence and the Responsible Artificial Intel-
15 ligence Strategy and Implementation Pathway;

16 (2) establish policy and issue guidance on defi-
17 nitions of requirements and testability for artificial
18 intelligence-enabled systems to implement and dem-
19 onstrate adherence to the Ethical Principles for Ar-
20 tificial Intelligence and the Responsible Artificial In-
21 telligence Strategy and Implementation Pathway;
22 and

23 (3) issue guidance on test and evaluation prac-
24 tices for artificial intelligence capabilities in autono-
25 mous or semi-autonomous weapon systems, which
26 shall include an adversarial assessment (known as

1 “red-team assessment”) that evaluates weapon sys-
2 tem vulnerability to adversarial manipulation under
3 operationally realistic conditions.

4 (c) COMMON TOOLS AND INFRASTRUCTURE.—The
5 Chief Digital and Artificial Intelligence Officer shall co-
6 ordinate with the Under Secretary of Defense for Re-
7 search and Engineering and the Director of Operational
8 Test and Evaluation on developing and using common
9 tools and infrastructure for test and evaluation and
10 verification and validation of artificial intelligence capa-
11 bilities in autonomous or semi-autonomous weapon sys-
12 tems, including assurance benchmarks for reliability,
13 robustness, security, and human-machine team perform-
14 ance.

15 **SEC. 6. TESTING AND EVALUATION REQUIREMENTS.**

16 (a) GENERAL REQUIREMENT.—The Secretary shall
17 ensure that, regardless of the acquisition pathway or test-
18 ing and evaluation oversight status for a weapon system,
19 each system described in section 3(a)(2) undergoes—

20 (1) rigorous hardware and software verification
21 and validation; and

22 (2) realistic system developmental and oper-
23 ational test and evaluation, including analysis of un-
24 anticipated emergent behavior.

1 (b) SPECIFIC CONSIDERATIONS.—Testing and eval-
2 uation of a system under subsection (a)(2) may include
3 testing on how human operators respond to ensure they
4 are provided with enough time to exercise judgment and
5 can reject or challenge suggestions or recommendations.

6 (c) SPECIFIC REQUIREMENTS.—Testing and evalua-
7 tion of a system under subsection (a) shall include the fol-
8 lowing:

9 (1) Verification that the system functions as
10 anticipated in realistic operational environments
11 against adaptive adversaries, including with realistic
12 civilian presence, activities, actions, and reactions,
13 and are sufficiently robust to minimize failures.

14 (2) For a system incorporating artificial intel-
15 ligence capabilities, rigorous developmental and
16 operational test and evaluation to verify and validate
17 that the artificial intelligence is robust according to
18 design requirements.

19 (3) Testing to confirm that autonomy algo-
20 rithms in systems incorporating artificial intelligence
21 capabilities can be rapidly reprogrammed on new
22 input data.

23 (d) POST-FIELDING TESTING.—The Secretary shall
24 ensure that, after initial operational test and evaluation

1 of a system under subsection (a), as directed by the Direc-
2 tor of Operational Test and Evaluation—

3 (1) system data is collected and any further
4 changes to the system undergo appropriate
5 verification and validation and test and evaluation to
6 ensure that critical safety features have not been de-
7 graded;

8 (2) system software is tested using best-avail-
9 able Department means and methods to validate
10 that critical safety features have not been degraded,
11 and automated testing tools, such as modeling and
12 simulation, are used whenever feasible;

13 (3) any new or revised operating states or other
14 relevant changes in the system are identified and un-
15 dergoes appropriate and tailored additional test and
16 evaluation to characterize the system behavior in
17 that new operating state; and

18 (4) changes to the state transition matrix are
19 evaluated to determine whether they require whole
20 system follow-on operational test and evaluation.

21 (e) ITERATIVE CYBER TESTING.—The Secretary
22 shall ensure that hardware and software verification and
23 validation of a system under subsection (a) includes quar-
24 terly cyber test and evaluation to verify that the system
25 is resilient and survivable in contested cyberspace.

1 (f) ROLE OF THE DIRECTOR OF OPERATIONAL TEST
2 AND EVALUATION.—Under this section, the Director of
3 Operational Test and Evaluation shall—

4 (1) oversee development of realistic operational
5 test, risk assessments, and evaluation standards for
6 autonomous and semi-autonomous weapon systems,
7 including requirements for data collection and stand-
8 ards for test and evaluation of any changes to the
9 system following initial operational test and evalua-
10 tion;

11 (2) evaluate whether autonomous and semi-au-
12 tonomous weapon systems under the Director's over-
13 sight have met standards after being tested for rig-
14 orous verification, validation, and evaluation in real-
15 istic operational conditions, including potential ad-
16 versary action, to ensure that the system is robust
17 to minimize failures;

18 (3) establish standards for data collection post-
19 fielding and monitoring and assessment by pro-
20 grams;

21 (4) establish and maintain a centralized reposi-
22 tory for reporting, collecting, and analyzing oper-
23 ational incidents, weapon system failures, and unin-
24 tended weapon system behaviors;

1 (5) review and approve operational and live fire
2 test plans for autonomous and semi-autonomous
3 weapon systems; and

4 (6) coordinate with the Under Secretary of De-
5 fense for Research and Engineering and the appro-
6 priate Secretary of a military department or Assist-
7 ant Secretary for Low-Intensity Conflict to provide
8 for monitoring to identify and address when changes
9 to the system design or operational environment re-
10 quire additional testing and evaluation to ensure
11 that the system is robust to minimize failures such
12 as unintended engagements with civilians and civil-
13 ian infrastructure, densely populated areas, and re-
14 sist interference by unauthorized parties.

15 **SEC. 7. PROHIBITED USES OF ARTIFICIAL INTELLIGENCE.**

16 (a) GENERAL PROHIBITION.—No covered artificial
17 intelligence capability may be used in any manner that vio-
18 lates the Constitution of the United States, Federal law,
19 the Law of Armed Conflict, or international treaty or
20 other legal obligation of the United States, or in any man-
21 ner that poses an unacceptable level of risk to the safety
22 of an individual or the civil liberty of an individual.

23 (b) SPECIFIC PROHIBITIONS.—

1 (1) IN GENERAL.—No covered artificial intel-
2 ligence capability may be used with the intent, pur-
3 pose, or outcome of—

4 (A) profiling, targeting, tracking, moni-
5 toring, inferring, or concluding based on the
6 data points of activity of any individual based
7 solely on the exercise of rights protected under
8 the Constitution or Federal law, including free-
9 dom of expression, association, and assembly;

10 (B) detecting, measuring, or inferring the
11 emotional state of any individual from data ac-
12 quired about such individual, including the sup-
13 port of the health of consenting personnel of
14 the Federal Government;

15 (C) inferring or determining an individ-
16 ual's religion, ethnicity, race, sexual orientation,
17 immigration status, disability status, gender
18 identity, or political identity;

19 (D) tracking, monitoring, or inferring the
20 past, real-time, or anticipated future location of
21 any individual in the United States, including
22 using data acquired from commercial, data bro-
23 kers, data aggregators, or other third-party
24 sources, unless such acquisition and use is au-
25 thorized pursuant to an individualized judicial

1 order, warrant, or otherwise required by the
2 Constitution or Federal law;

3 (E) aggregating or analyzing internal data
4 or data acquired from commercial, data bro-
5 kers, data aggregators, or other third-party
6 sources, including but not limited to location
7 data, financial transaction data, communica-
8 tions metadata, or biometric data, to accom-
9 plish any purpose prohibited under paragraphs
10 (1) through (4);

11 (F) removing a human from the chain of
12 decisionmaking for actions critical to informing
13 and executing decisions by the President, in-
14 cluding initiating or terminating nuclear weap-
15 ons employment; or

16 (G) obtaining, receiving, or otherwise ac-
17 cessing, for a fee or other consideration, any
18 personal data of a United States person from a
19 data broker or other third-party source, includ-
20 ing any other governmental entity (including
21 State, local, or Federal entities) if such data
22 was obtained by that entity in a manner that
23 would violate this subsection if performed by
24 the Department.

1 (2) PERSONAL DATA.—For purposes of para-
2 graph (1)(G), the term “personal data”—

3 (A) means data, derived data, or any
4 unique identifier that is linked to, or is reason-
5 ably linkable to, an individual or to an elec-
6 tronic device that is linked to, or is reasonably
7 linkable to, one or more individuals in a house-
8 hold;

9 (B) includes anonymized data that, if com-
10 bined with other data, can be linked to, or is
11 reasonably linkable to, an individual or to an
12 electronic device that identifies, is linked to, or
13 is reasonably linkable to one or more individuals
14 in a household; and

15 (C) does not include data that is lawfully
16 available through Federal, State, or local gov-
17 ernment records or through widely distributed
18 media.

19 (c) APPLICABILITY.—The prohibitions in this section
20 shall apply to all activities of the Department, including
21 operational planning, logistics, intelligence analysis, and
22 operational support to any other agencies or military per-
23 sonnel, regardless of status of deployment. In any case in
24 which the Department shares systems, data, or analytical
25 products derived from a covered artificial intelligence ca-

1 pability or protected data (as described in subsection
2 (b)(7)) with another department or agency of the Federal
3 Government, the receiving department or agency shall be
4 subject to the same prohibitions and requirements as the
5 Department with respect to the use, querying, or further
6 dissemination of such systems, data, or products. The Sec-
7 retary shall ensure that such department or agency is noti-
8 fied of, and in compliance with, the restrictions under this
9 section.

10 (d) **JOINT OPERATIONS.**—The prohibitions of this
11 section shall apply to any Departmental participation in
12 joint task forces, fusion centers, or interagency working
13 groups, regardless of which agency serves as the lead or
14 providing entity.

15 **SEC. 8. WHISTLEBLOWER PROTECTIONS.**

16 (a) **PROTECTIONS.**—The Secretary shall update such
17 whistleblower protections as the Secretary considers ap-
18 propriate to clarify procedures for artificial intelligence
19 systems, which shall ensure that all personnel who develop,
20 assess, deploy, operate, or use artificial intelligence as a
21 component of a National Security System (as defined in
22 section 3552(b) of title 44, United States Code) or other-
23 wise for military or intelligence purposes can report con-
24 cerns about artificial intelligence, including concerns about
25 improperly harming civil liberties, privacy, safety, or com-

1 pliance with the requirements of this Act, to relevant over-
2 sight officials.

3 (b) COMPLIANCE WITH EXISTING LAW.—Updates to
4 whistleblower protections under subsection (a) shall be
5 compliant with—

6 (1) section 1034 of title 10, United States
7 Code, and its implementation guidance under De-
8 partment of Defense Directive 7050.06 (relating to
9 military whistleblower protection);

10 (2) section 2302 of title 5, United States Code;

11 (3) title VI of the Intelligence Authorization
12 Act of Fiscal Year 2014 (Public Law 113–126; 128
13 Stat. 1414) and the amendments made by such title;
14 and

15 (4) section 4701 of title 10, United States
16 Code.

17 (c) ANONYMITY.—

18 (1) IN GENERAL.—The Secretary shall ensure
19 that adequate and special procedures exist to re-
20 ceive, investigate, respond to, and redress complaints
21 anonymously, when appropriate, and that reports
22 may be made confidentially so that personnel may
23 raise concerns without fear of reprisal for any disclo-
24 sures related to artificial intelligence.

1 (2) EXCEPTION.—Confidentiality under para-
 2 graph (1) shall not extend to significant misconduct,
 3 including violations of law or government ethics, or
 4 when otherwise precluded by law.

5 (d) INVESTIGATION AND CORRECTIVE ACTION.—The
 6 Secretary shall ensure that adequate and special proce-
 7 dures exist for reporting incidents of artificial intelligence
 8 misuse, investigations of reported incidents, and processes
 9 for taking corrective actions.

10 **SEC. 9. REPORTING REQUIREMENTS.**

11 (a) SEMIANNUAL REPORT ON ARTIFICIAL INTEL-
 12 LIGENCE USE CASES.—Not later than six months after
 13 the date of the enactment of this Act, and semiannually
 14 thereafter, the Secretary shall submit to the appropriate
 15 committees of Congress a report containing the following:

16 (1) A description of exemplary use cases of arti-
 17 ficial intelligence within the Department during the
 18 preceding year, identifying best practices, failure
 19 modes, and risk mitigation strategies employed.

20 (2) After-action reports on significant oper-
 21 ational use of covered artificial intelligence capabili-
 22 ties during the preceding year, including—

23 (A) an assessment of system performance
 24 and effectiveness of human oversight;

25 (B) any identified risks or failure modes;

1 (C) a detailed accounting of any critical in-
2 cidents, including incidents resulting in civilian
3 casualties or injuries, damage to civilian objects
4 or protected infrastructure, or other unintended
5 effects inconsistent with the Law of Armed
6 Conflict; and

7 (D) recommendations for improvements to
8 human oversight, system safeguards, and the
9 mitigation of future civilian harm.

10 (3) A description of training provided to human
11 operators of autonomous and semi-autonomous
12 weapon systems and other artificial intelligence ca-
13 pabilities covered by this Act, including documenta-
14 tion on employment procedures and responsible re-
15 tirement of systems.

16 (b) ANNUAL REPORT ON INFRASTRUCTURE AND
17 BARRIERS.—Not later than 180 days after the date of the
18 enactment of this Act, and annually thereafter, the Sec-
19 retary shall submit to the appropriate committees of Con-
20 gress a report identifying—

21 (1) any significant barriers to the responsible
22 development and deployment of artificial intelligence
23 within the Department;

24 (2) gaps in infrastructure required to support
25 traceability, auditability, risk analysis, and forensics

1 for artificial intelligence capabilities covered by this
2 Act; and

3 (3) recommended hardware, software, or other
4 infrastructure needs necessary to fulfill the require-
5 ments of this Act.

6 (c) SEMIANNUAL REPORT ON COMPLIANCE FOR
7 FIELDDED SYSTEMS.—Not later than six months after the
8 date of the enactment of this Act, and semiannually there-
9 after, the Secretary shall submit to the appropriate com-
10 mittees of Congress a report identifying—

11 (1) each fielded system for which compliance
12 under this Act cannot be certified, with a description
13 of the specific requirement or requirements with
14 which the system does not comply;

15 (2) the operational or national security legal
16 justification, if any, for the continued fielding of
17 each such non-compliant system; and

18 (3) a remediation plan and timeline for bringing
19 each such system into compliance or, if compliance
20 is not practicable, a plan for the responsible retire-
21 ment or modification of the system.

22 **SEC. 10. EXCEPTIONS.**

23 (a) CYBERSPACE CAPABILITIES.—The requirements
24 of sections 3, 4, 5, and 7 shall not apply to autonomous
25 or semi-autonomous cyberspace capabilities.

1 (b) UNARMED PLATFORMS.—The requirements of
2 sections 3, 4, 5, and 7 shall not apply to unarmed plat-
3 forms, whether remotely operated or operated by onboard
4 personnel, and whether autonomous or semi-autonomous.

5 (c) TIME-CRITICAL DEFENSIVE SYSTEMS.—In cases
6 where the time available between threat detection and re-
7 quired intercept is insufficient to allow for individual
8 human authorization of each engagement and provided
9 that such operations do not have death or serious bodily
10 harm to any person as a reasonably foreseeable con-
11 sequence, the requirements of sections 3, 4, 5, and 7 shall
12 not apply to—

13 (1) systems employed exclusively for the defense
14 against incoming munitions, rockets, artillery, mor-
15 tars, missiles; or

16 (2) unmanned aircraft systems.

17 (d) OTHER EXCLUDED SYSTEMS.—The requirements
18 of sections 3, 4, 5, and 7 shall not apply to—

19 (1) unguided munitions;

20 (2) munitions manually guided by the human
21 operator, such as laser- or wire-guided munitions;

22 (3) mines;

23 (4) unexploded explosive ordnance; or

24 (5) autonomous or semi-autonomous systems
25 that are not weapon systems.

1 (e) IDENTIFICATION SYSTEMS.—The requirements of
 2 sections 3, 4, 5, and 7 shall not apply to a system de-
 3 scribed in section 3(a)(2) with the sole purpose and out-
 4 come of identifying potential targets without further inter-
 5 vention by or communication with a human operator.

6 **SEC. 11. EFFECTIVE DATE; REVIEW OF SYSTEMS CUR-**
 7 **RENTLY IN USE.**

8 (a) IN GENERAL.—This Act shall take effect on the
 9 date that is 180 days after the date of the enactment of
 10 this Act.

11 (b) REVIEW OF SYSTEMS CURRENTLY IN USE.—

12 (1) IN GENERAL.—Not later than 180 days
 13 after the effective date set forth in subsection (a),
 14 the Secretary shall conduct a review of all systems
 15 described in section 3(a)(2) that are in use by the
 16 Department as of such effective date.

17 (2) ATTESTATION.—Upon completion of the re-
 18 view required under paragraph (1), the Secretary
 19 shall submit to the appropriate committees of Con-
 20 gress a written attestation identifying, for each re-
 21 viewed system, whether the system is compliant with
 22 the requirements of sections 3, 6, and 7.

23 (3) NONCOMPLIANT SYSTEMS.—For any system
 24 that the Secretary cannot attest is in compliance
 25 with sections 3, 6, and 7, the Secretary shall imme-

1 diately cease all use of such system and, concurrent
2 with the attestation required under paragraph (2),
3 submit to appropriate committees of Congress a re-
4 mediation plan that includes—

5 (A) a description of the specific require-
6 ment or requirements with which the system
7 does not comply;

8 (B) an operational or national security jus-
9 tification, if any, for continued use of the sys-
10 tem pending remediation; and

11 (C) a timeline for bringing the system into
12 compliance or, if compliance is not practicable,
13 for the responsible retirement or modification of
14 the system.

○