

119TH CONGRESS
2D SESSION

S. 4656

To provide for secure and accountable use of artificial intelligence by the
Department of Defense, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 2, 2026

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

A BILL

To provide for secure and accountable use of artificial intel-
ligence by the Department of Defense, 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 “Secure and Account-
5 able Military AI Act of 2026”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) **ARTIFICIAL INTELLIGENCE.**—The term “ar-
9 tificial intelligence” has the meaning given that term

1 in section 5002 of the National Artificial Intelligence
2 Initiative Act of 2020 (15 U.S.C. 9401).

3 (2) AUTONOMOUS WEAPON SYSTEM.—The term
4 “autonomous weapon system” means a weapon sys-
5 tem that, once activated, can select and engage tar-
6 gets without further intervention by an operator, in-
7 cluding operator-supervised autonomous weapon sys-
8 tems that, after activation, can select and engage
9 targets without further operator input.

10 (3) COVERED CONTRACT.—The term “covered
11 contract” means a contract, task order, delivery
12 order, or other agreement for the development,
13 training, fine-tuning, evaluation, hosting, integra-
14 tion, or provision of an artificial intelligence model
15 or artificial intelligence system for use by the De-
16 partment.

17 (4) COVERED CONTRACTOR.—The term “cov-
18 ered contractor” means an entity that develops or
19 provides a frontier artificial intelligence model to the
20 Department under a covered contract.

21 (5) COVERED INCIDENT.—The term “covered
22 incident” means any of the following:

23 (A) Theft, unauthorized access, unauthor-
24 ized acquisition, or exfiltration of model weights
25 for an artificial intelligence model, including—

1 (i) instances in which a model autono-
2 mously attempts to exfiltrate such model
3 weights or acquire unauthorized access to
4 systems containing such model weights;
5 and

6 (ii) credible evidence indicating at-
7 tempts or material vulnerabilities, relating
8 to any such theft, access, acquisition, or
9 exfiltration.

10 (B) Attempts by a foreign adversary or in-
11 dividual acting on behalf of a foreign adversary
12 to obtain unauthorized access to, acquire, influ-
13 ence, or exfiltrate sensitive information, sys-
14 tems, or intellectual property related to an arti-
15 ficial intelligence model or artificial intelligence
16 system, including through insider threats, com-
17 promised personnel, covert affiliations, or other
18 deceptive means.

19 (C) A compromise of the software, hard-
20 ware, cloud, data, or other supply chain used to
21 develop, train, fine-tune, evaluate, secure, or de-
22 ploy an artificial intelligence model or artificial
23 intelligence system, where such compromise
24 could reasonably affect the confidentiality, in-

1 integrity, availability, reliability, or security of the
2 model or system provided to the Department.

3 (D) Poisoning, corruption, manipulation,
4 or unauthorized alteration of training data,
5 fine-tuning data, retrieval corpora, model check-
6 points, system prompts, safety filters, moni-
7 toring systems, evaluation pipelines, or model-
8 update mechanisms.

9 (E) The discovery of a material vulner-
10 ability, exploit, backdoor, or failure of access
11 controls that could permit unauthorized modi-
12 fication, extraction, degradation, or misuse of
13 an artificial intelligence model or artificial intel-
14 ligence system.

15 (F) Any materially concerning model be-
16 havior, including materially increased capability
17 for cyber offense, exploitation, exploitation or
18 evasion of safeguards, deceptive behavior, capa-
19 bilities related to chemical or biological weap-
20 ons, automated research and development in
21 national security domains, automated research
22 and development toward increasingly powerful
23 artificial systems, unauthorized autonomous ac-
24 tion, or other behavior that poses a significant
25 risk to national security or the operations, per-

sonnel, or systems of the Department, when such behavior was not previously disclosed to the Department.

(G) Any incident for which the Secretary determines that timely notice is necessary to protect national security or operations of the Department.

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

(7) FRONTIER ARTIFICIAL INTELLIGENCE MODEL.—The term “frontier artificial intelligence model” means a general-purpose model, foundation model, or other large-scale model designated by the Secretary, in consultation with the Chief Digital and Artificial Intelligence Officer and the Secretary of Commerce, as appropriate, as presenting significant national security relevance due to scale, capability, operational use, or potential for misuse.

(8) HIGH-CONSEQUENCE ARTIFICIAL INTELLIGENCE APPLICATION.—The term “high-consequence artificial intelligence application” means any use by the Department of artificial intelligence that the Secretary designates under section 3 as presenting heightened national security, operational, safety, legal, or civil liberties risk, including any use

1 relating to nuclear command, control, and commu-
2 nications, intelligence support to lethal targeting,
3 cyber operations, autonomous weapon systems, mili-
4 tary decision support in time-sensitive operations,
5 homeland-facing surveillance or monitoring, or mis-
6 sion-critical logistics and sustainment.

7 (9) INDIVIDUAL.—The term “individual” means
8 a natural person.

9 (10) LOCAL DEFENSE.—The term “local de-
10 fense” means defense within a specifically defined
11 geographic defensive area (commonly referred to as
12 “point defense”) or of a high-value physical asset
13 (commonly referred to as “platform defense”) and
14 for a specifically defined period of operation ap-
15 proved for the system concerned.

16 (11) MATERIEL TARGET.—The term “materiel
17 target” —

18 (A) means a weapon, munition, military
19 vehicle, military vessel, military aircraft, un-
20 manned system, or other military object; and

21 (B) does not include an individual.

22 (12) PATTERN-OF-LIFE ANALYSIS.—The term
23 “pattern-of-life analysis” means the use of data over
24 time to infer or map the habits, movements, associa-

1 tions, or routines of an individual or a group of indi-
2 viduals.

3 (13) PERSISTENT PERSON-CENTRIC ANALYTIC
4 PRODUCT.—The term “persistent person-centric
5 analytic product” means a dossier, watchlist, score,
6 profile, targeting package, or other record organized
7 primarily around an identified or identifiable indi-
8 vidual.

9 (14) OPERATIONAL DEPLOYMENT.—The term
10 “operational deployment” means use of an artificial
11 intelligence system in support of, or as part of, an
12 operational military mission, contingency, or real-
13 world military activity other than testing, training,
14 evaluation, or experimentation conducted in a con-
15 trolled environment.

16 (15) OPERATOR-SUPERVISED AUTONOMOUS
17 WEAPON SYSTEM.—The term “operator-supervised
18 autonomous weapon system” means an autonomous
19 weapon system that is designed to provide operators
20 with the ability to intervene and terminate engage-
21 ments, including in the event of a weapon system
22 failure, before unacceptable levels of damage occur.

23 (16) SECRETARY.—The term “Secretary”
24 means the Secretary of Defense.

25 (17) SEMI-AUTONOMOUS WEAPON SYSTEM.—

(A) IN GENERAL.—The term “semi-autonomous weapon system” means a weapon system that, once activated, is intended to only engage single targets or specific target groups that have been selected by an operator.

(B) INCLUSIONS.—The term “semi-autonomous weapon system” includes weapon systems that employ autonomy for engagement-related functions, including—

(i) acquiring, tracking, and identifying potential targets;

(ii) cuing potential targets to operators;

(iii) prioritizing selected targets;

(iv) timing of when to fire;

(v) providing terminal guidance to home in on selected targets, provided that operator control is retained over the decision to select single targets and specific target groups for engagement; and

(vi) “fire and forget” or lock-on-after-launch homing munitions that rely on tactics techniques and procedures to maximize the probability that the only targets within the seeker’s acquisition basket when the

1 seeker activates are those individual tar-
 2 gets or specific target groups that have
 3 been selected by an operator.

4 (18) UNITED STATES PERSON.—The term
 5 “United States person” has the meaning given that
 6 term in section 101 of the Foreign Intelligence Sur-
 7 veillance Act of 1978 (50 U.S.C. 1801).

8 **SEC. 3. HIGH-CONSEQUENCE MILITARY ARTIFICIAL INTEL-**
 9 **LIGENCE OVERSIGHT.**

10 (a) DESIGNATION OF HIGH-CONSEQUENCE APPLICA-
 11 TIONS.—

12 (1) IN GENERAL.—Not later than 180 days
 13 after the date of the enactment of this Act, the Sec-
 14 retary shall establish and maintain a process to des-
 15 ignate categories of artificial intelligence applications
 16 of the Department as high-consequence.

17 (2) DESIGNATIONS.—The following categories
 18 shall be designated as high-consequence artificial in-
 19 telligence applications pursuant to paragraph (1):

20 (A) Artificial intelligence used for the se-
 21 lection of targets for, or execution of the launch
 22 or detonation of, a nuclear weapon.

23 (B) Artificial intelligence used in support
 24 of lethal targeting decisions, including intel-

1 ligence fusion or target recommendation for le-
2 thal operations.

3 (C) Artificial intelligence used in support
4 of cyber operations that are intended or reason-
5 ably likely to create effects outside Department-
6 owned or Department-controlled information
7 systems.

8 (D) Autonomous weapon systems and op-
9 erator-supervised autonomous weapon systems.

10 (E) Artificial intelligence used for domestic
11 person-based analysis described in section
12 6(a)(2).

13 (F) Any other category designated by the
14 Secretary as presenting a material risk of
15 death, serious bodily harm, unlawful use of
16 force, strategic surprise, major mission failure,
17 or substantial violation of law or policy if the
18 system malfunctions, is misused, or is employed
19 outside approved constraints.

20 (b) APPROVAL REQUIRED BEFORE OPERATIONAL
21 DEPLOYMENT.—The Secretary shall require that a high-
22 consequence artificial intelligence application may not be
23 approved for operational deployment unless a senior De-
24 partment official designated by the Secretary, who may
25 not be below the level of the Under Secretary of Defense

1 or the Vice Chairman of the Joint Chiefs of Staff, deter-
2 mines in writing that the application satisfies the require-
3 ments of subsection (c).

4 (c) MINIMUM REQUIREMENTS.—Before approving a
5 high-consequence artificial intelligence application for
6 operational deployment, the approving official shall ensure
7 that the Department has completed, as appropriate to the
8 application, the following:

9 (1) Realistic developmental and operational
10 testing and evaluation sufficient to assess perform-
11 ance, capability, reliability, effectiveness, suitability,
12 and resilience under expected operational conditions,
13 including adversarial conditions where feasible.

14 (2) Legal and policy review.

15 (3) Documentation of intended missions, in-
16 tended operational environments, intended target or
17 decision sets, known limitations, failure modes, and
18 assumptions.

19 (4) Clear procedures for trained operators to
20 activate, deactivate, override, or terminate system
21 functions, and the circumstances requiring such ac-
22 tions.

23 (5) Fallback procedures and mission-continuity
24 measures in the event of degradation, anomalous be-
25 havior, compromise, or system failure.

1 (6) Logging, auditability, and record-retention
2 mechanisms sufficient to support oversight, inves-
3 tigation, and after-action review.

4 (7) Post-deployment continuous monitoring
5 mechanisms.

6 (8) Training, doctrine, and tactics, techniques,
7 and procedures appropriate to the use of the appli-
8 cation.

9 (d) CONGRESSIONAL NOTIFICATION.—

10 (1) IN GENERAL.—Except as provided in para-
11 graph (3), not later than 15 days before the initial
12 operational deployment of a category of high-con-
13 sequence artificial intelligence application, the Sec-
14 retary shall notify the Committees on Armed Serv-
15 ices of the Senate and House of Representatives of
16 such deployment.

17 (2) CONTENTS.—A notification required by
18 paragraph (1) shall include—

19 (A) a description of the application;

20 (B) the mission set, operational environ-
21 ment, and, as appropriate, target or decision set
22 for which the application is intended;

23 (C) a summary of the testing and evalua-
24 tion conducted;

1 (D) a description of key safeguards, limita-
2 tions, and fallback procedures;

3 (E) an identification of the accountable
4 human decision-makers and operators; and

5 (F) any other matters the Secretary deter-
6 mines appropriate.

7 (3) EXCEPTION.—The Secretary may provide a
8 notification required by paragraph (1) not later than
9 48 hours after the initial operational deployment if
10 the Secretary—

11 (A) determines that there are extraor-
12 dinary circumstances affecting the national se-
13 curity of the United States; and

14 (B) provides, with the notification, a state-
15 ment of such circumstances necessitating de-
16 layed notice.

17 (e) ANNUAL BRIEFING.—Not later than 1 year after
18 the date of the enactment of this Act, and annually there-
19 after, the Secretary shall brief the Committees on Armed
20 Services of the Senate and House of Representatives on
21 the implementation of this section.

1 **SEC. 4. HUMAN ACCOUNTABILITY FOR HIGH-CON-**
2 **SEQUENCE MILITARY ARTIFICIAL INTEL-**
3 **LIGENCE.**

4 (a) **POLICY.**—It shall be the policy of the Department
5 that artificial intelligence may support analysis,
6 prioritization, recommendations, automation, and other
7 decision-support functions, but may not substitute for ac-
8 countable human judgment in decisions involving the use
9 of force, detention, domestic person-based analysis, or
10 other high-consequence artificial intelligence applications
11 designated pursuant to section 3.

12 (b) **ACCOUNTABLE HUMAN DECISION-MAKER.**—For
13 each high-consequence artificial intelligence application
14 approved for operational deployment, the Secretary shall
15 ensure that there is a clearly identified accountable human
16 decision-maker or accountable chain of decision-makers
17 with authority commensurate to the operational risk pre-
18 sented by the application.

19 (c) **REQUIRED ELEMENTS.**—The accountable human
20 decision-maker or chain of decision-makers under sub-
21 section (b) shall have, as appropriate to the application—

22 (1) documented commander intent and mission
23 parameters;

24 (2) sufficient training on the capabilities, limi-
25 tations, and failure modes of the application;

1 (3) access to relevant information necessary to
2 understand the basis for significant system outputs
3 or recommendations, to the extent technically fea-
4 sible;

5 (4) authority and practical ability to pause,
6 override, deactivate, or terminate use of the applica-
7 tion when required by law, policy, or operational cir-
8 cumstances; and

9 (5) procedures for elevating uncertainty, anom-
10 alous outputs, or significant incidents for further
11 human review.

12 **SEC. 5. REPORTING OF SECURITY INCIDENTS AND CON-**
13 **CERNING MODEL BEHAVIORS BY CERTAIN**
14 **FRONTIER ARTIFICIAL INTELLIGENCE CON-**
15 **TRACTORS.**

16 (a) REQUIREMENT FOR CONTRACT CLAUSE.—The
17 Secretary shall require—

18 (1) in any covered contract entered into on or
19 after the date that is 30 days after the date of the
20 enactment of this Act, a clause requiring a covered
21 contractor to report to the Secretary any covered in-
22 cident relating to an artificial intelligence model or
23 artificial intelligence system developed, trained, fine-
24 tuned, hosted, or provided by the contractor; and

1 (2) in any covered contract entered into prior to
2 the date that is 30 days after the date of the enact-
3 ment of this Act, such a clause to be added not later
4 than 90 days after the date of the enactment of this
5 Act.

6 (b) IMPLEMENTATION GUIDANCE AND CLARITY.—

7 (1) IN GENERAL.—Not later than 90 days after
8 the date of the enactment of this Act, the Secretary
9 shall issue guidance to covered contractors regarding
10 the implementation of this section in order to pro-
11 mote clear, predictable, and consistent reporting ex-
12 pectations and support good-faith compliance.

13 (2) ELEMENTS.—The guidance required by
14 paragraph (1) shall include—

15 (A) illustrative examples of covered inci-
16 dents, factors relevant to determining whether
17 an incident is material or reportable;

18 (B) reporting procedures and timelines;
19 and

20 (C) other information the Secretary deter-
21 mines appropriate to promote consistent imple-
22 mentation and reduce uncertainty for covered
23 contractors.

24 (3) UPDATES TO GUIDANCE.—The Secretary
25 shall update such guidance as appropriate to reflect

1 changes in artificial intelligence capabilities, deploy-
2 ment practices, threat environments, and reporting
3 needs of the Department.

4 (4) CONSULTATION.—In issuing and updating
5 such guidance, the Secretary shall consult with the
6 Chief Digital and Artificial Intelligence Officer, the
7 Director of the Artificial Intelligence Security Center
8 of the National Security Agency, and the heads of
9 any other Federal agencies or Departments the Sec-
10 retary deems appropriate.

11 (c) REPORTING TIMELINE FOR COVERED CONTRAC-
12 TORS.—

13 (1) IN GENERAL.—A covered contractor shall
14 submit to the Under Secretary for Research and En-
15 gineering—

16 (A) an initial report regarding a covered
17 incident described in subparagraph (A), (B),
18 (C), or (D) of section 2(5) not later than 72
19 hours after the discovery of such covered inci-
20 dent; and

21 (B) an initial report regarding a covered
22 incident described in subparagraph (E) or (F)
23 of section 2(5) not later than 7 days after the
24 contractor discovers a behavior specified by the
25 implementation guidance issued pursuant to

1 subsection (b) or that a reasonable person
2 would deem likely to be material.

3 (2) SUPPLEMENTAL UPDATES.—A covered con-
4 tractor shall submit to the Secretary supplemental
5 updates with respect to any covered incident as ma-
6 terial new information becomes available.

7 (d) CONTENTS OF CONTRACTOR REPORT.—Each re-
8 port submitted by a covered contractor in accordance with
9 this section shall include, to the extent known at the time
10 of submission—

11 (1) a description of the covered incident;

12 (2) the date or approximate period of occur-
13 rence and discovery;

14 (3) the artificial intelligence model, artificial in-
15 telligence system, or relevant training, fine-tuning,
16 evaluation, or deployment environment affected;

17 (4) the actual or suspected means of com-
18 promise, exfiltration, manipulation, degradation, or
19 misuse;

20 (5) whether model weights, training data, sys-
21 tem prompts, source code, evaluation data, safety
22 systems, or software dependencies were accessed, al-
23 tered, degraded, poisoned, exfiltrated, or otherwise
24 compromised;

1 (6) an assessment of actual or potential impact
2 on missions, users, systems, operations, or decision-
3 making of the Department;

4 (7) any actions taken to contain, mitigate, re-
5 mediate, or investigate the covered incident;

6 (8) whether the covered incident has been re-
7 ported to any other Federal department or agency;
8 and

9 (9) such other information as the Secretary de-
10 termines appropriate.

11 (e) RECIPIENTS WITHIN THE DEPARTMENT.—A re-
12 port submitted to the Secretary under this section shall
13 be transmitted by the Secretary to—

14 (1) the contracting officer for the covered con-
15 tract;

16 (2) the Chief Digital and Artificial Intelligence
17 Office;

18 (3) the Chief Information Officer of the Depart-
19 ment of Defense;

20 (4) the Under Secretary of Defense for Acquisi-
21 tion and Sustainment;

22 (5) the Artificial Intelligence Security Center of
23 the National Security Agency;

24 (6) the Commander of the United States Cyber
25 Command; and

1 (7) the heads of such other components of the
2 Department and other Federal departments or agen-
3 cies as the Secretary determines appropriate.

4 (f) CONGRESSIONAL NOTIFICATION BY DEPART-
5 MENT.—

6 (1) IN GENERAL.—Not later than 7 days after
7 receipt of an initial report under subsection (b) re-
8 garding a covered incident, or the discovery of a cov-
9 ered incident by the Department, the Secretary shall
10 submit to the Committees on Armed Services of the
11 Senate and House of Representatives notice of such
12 covered incident.

13 (2) CONTENTS.—A notice required by para-
14 graph (1) shall include, to the extent known at the
15 time of submission—

16 (A) a summary description of the covered
17 incident;

18 (B) the date or approximate period of oc-
19 currence and discovery;

20 (C) the artificial intelligence model, artifi-
21 cial intelligence system, or relevant training,
22 fine-tuning, evaluation, or deployment environ-
23 ment affected;

1 (D) the actual or suspected means of com-
2 promise, exfiltration, manipulation, degradation,
3 or misuse;

4 (E) an initial assessment of actual or po-
5 tential impact on missions, users, systems, or
6 operations of the Department; and

7 (F) any actions taken or planned to con-
8 tain, mitigate, remediate, or investigate the cov-
9 ered incident.

10 (3) ADDITIONAL UPDATES.—The Secretary
11 shall provide to the Committees on Armed Services
12 of the Senate and House of Representatives addi-
13 tional briefings or updates on a covered incident as
14 material information becomes available.

15 (g) PROTECTION OF REPORTED INFORMATION.—The
16 Secretary shall establish procedures for the handling of
17 reports under this section, including procedures to protect
18 classified information, proprietary information, trade se-
19 crets, security-sensitive information, and information re-
20 garding vulnerabilities that, if disclosed publicly, could
21 reasonably be expected to harm national security.

22 (h) RULE OF CONSTRUCTION.—Nothing in this sec-
23 tion shall be construed—

24 (1) to require the disclosure of information in
25 a manner inconsistent with the protection of classi-

1 fied information, sensitive compartmented informa-
2 tion, or other information protected by law;

3 (2) to waive any applicable privilege or legal
4 protection; or

5 (3) to limit any other reporting obligation im-
6 posed by law, regulation, or contract.

7 **SEC. 6. LIMITATIONS ON CERTAIN USES OF ARTIFICIAL IN-**
8 **TELLIGENCE BY THE DEPARTMENT.**

9 (a) IN GENERAL.—The Department may not—

10 (1) use artificial intelligence for the selection of
11 targets for the use of a nuclear weapon or for the
12 execution of launching or detonating a nuclear weap-
13 on;

14 (2) except as provided in subparagraph (b), use
15 artificial intelligence to acquire, collect, ingest, re-
16 tain, query, correlate, analyze, or disseminate infor-
17 mation concerning a United States person located in
18 the United States for the purpose of—

19 (A) identifying or resolving the identity of
20 such person across datasets;

21 (B) tracking or conducting pattern-of-life
22 analysis of such person;

23 (C) conducting link analysis regarding the
24 associations, contacts, activities, or movements
25 of such person;

1 (D) assigning a risk score, threat score, or
2 other predictive assessment to such person;

3 (E) creating or maintaining a watchlist,
4 dossier, targeting package, or other persistent
5 person-centric analytic product regarding such
6 person; or

7 (F) selecting such person for investigative,
8 operational, or law enforcement attention, un-
9 less such activity is expressly authorized by
10 Federal law and supported by a lawful and doc-
11 umented predicate; or

12 (3) develop, procure, field, or employ an autono-
13 mous weapon system, except as provided in sub-
14 section (d).

15 (b) RULE OF CONSTRUCTION.—Subsection (a) shall
16 not be construed to prohibit the use of artificial intel-
17 ligence—

18 (1) for cybersecurity, information assurance,
19 threat detection, vulnerability management, malware
20 analysis, incident response, or defensive cyberspace
21 operations undertaken to protect the Department of
22 Defense Information Network, information systems,
23 weapons systems, military networks, or defense crit-
24 ical infrastructure of the Department from malicious
25 cyber activity;

1 (2) for force protection or counterintelligence
2 purposes to identify, assess, or warn of a specific,
3 credible, and articulable threat to personnel, installa-
4 tions, facilities, operations, activities, or covered as-
5 sets of the Department; or

6 (3) with the informed consent of the person
7 concerned.

8 (c) ADDITIONAL LIMITATIONS ON DOMESTIC
9 USES.—The Department may not use artificial intel-
10 ligence—

11 (1) solely on the basis of activity protected by
12 the First Amendment of the Constitution of the
13 United States or the lawful exercise of any other
14 right secured by the Constitution of the United
15 States or the laws of the United States; or

16 (2) to acquire, correlate, or analyze publicly
17 available information, commercially available infor-
18 mation, or hacked, leaked, or breached data that is
19 posted online or made available for sale for the pri-
20 mary purpose of circumventing otherwise applicable
21 constitutional, statutory, or regulatory protections
22 governing collection, retention, querying, or dissemi-
23 nation of information by the Federal Government
24 concerning United States persons.

1 (d) EXCEPTIONS FOR AUTONOMOUS WEAPON SYS-
2 TEMS.—Subsection (a)(3) shall not apply to the following,
3 provided that any such system satisfies the conditions of
4 subsection (e):

5 (1) Semi-autonomous weapon systems used to
6 apply lethal or non-lethal, kinetic or non-kinetic
7 force, so long as such semi-autonomous weapon sys-
8 tems do not include any mode of operation in which
9 the semi-autonomous weapon system is intended to
10 function as an autonomous weapon system.

11 (2) Operator-supervised autonomous weapon
12 systems used to select and engage materiel targets
13 for local defense to intercept attempted time-critical
14 or saturation attacks for—

15 (A) static defense of installations with per-
16 sonnel, including networked defense in which
17 the autonomous weapon system is not co-lo-
18 cated with the installation; or

19 (B) onboard or networked defense of plat-
20 forms with onboard personnel.

21 (3) Interception of surface-to-air missiles.

22 (4) Autonomous weapon systems used to apply
23 non-lethal, non-kinetic force against materiel targets
24 in accordance with Department of Defense Directive
25 3000.03E.

1 (e) CONDITIONS ON EXCEPTED SYSTEMS.—A system
2 described in subsection (d) may be developed, procured,
3 fielded, or employed only if the Secretary certifies that
4 such system—

5 (1) has undergone legal review for consistency
6 with the law of war, applicable treaties, weapon sys-
7 tem safety rules, and applicable rules of engagement;

8 (2) has completed rigorous verification and vali-
9 dation and realistic developmental and operational
10 testing and evaluation under conditions that reflect
11 the intended operational environment and reasonably
12 anticipated adversary countermeasures;

13 (3) is designed and fielded to permit com-
14 manders and operators to exercise appropriate levels
15 of human judgment over the use of force;

16 (4) includes human-machine interfaces and con-
17 trols that—

18 (A) are readily understandable to trained
19 operators;

20 (B) provide transparent feedback on sys-
21 tem status;

22 (C) provide clear procedures for activation
23 and deactivation of system functions; and

24 (D) for operator-supervised autonomous
25 weapon systems, permit operators to intervene

1 and terminate engagements before unacceptable
2 levels of damage occur, including in the event of
3 weapon system failure;

4 (5) is approved for use only within defined tem-
5 poral, geographic, environmental, and operational
6 constraints, and, if unable to complete an engage-
7 ment consistent with such constraints, is designed to
8 terminate the engagement or obtain additional oper-
9 ator input before continuing; and

10 (6) uses technologies and data sources that are,
11 to the maximum extent practicable consistent with
12 military necessity, transparent to, auditable by, and
13 explainable to relevant personnel.

14 (f) CERTIFICATION AND NOTIFICATION.—

15 (1) IN GENERAL.—Not later than 30 days be-
16 fore fielding a system pursuant to subsection (d),
17 the Secretary shall submit to the congressional de-
18 fense committees a written certification that the sys-
19 tem falls within one of the exceptions under sub-
20 section (d) and satisfies the conditions of subsection
21 (e).

22 (2) CONTENTS.—A certification under para-
23 graph (1) shall include—

24 (A) the exception under subsection (d) on
25 which the Department relies;

1 (B) a summary of the legal review con-
2 ducted under subsection (e)(1);

3 (C) the intended mission set, target class,
4 and operational concept for the system;

5 (D) the temporal, geographic, environ-
6 mental, and operational constraints approved
7 for the system;

8 (E) a description of the operator super-
9 vision concept, including procedures for inter-
10 vention, termination, activation, and deactiva-
11 tion;

12 (F) a summary of testing, verification, and
13 validation conducted for the system; and

14 (G) any substantial modification to the
15 system's algorithms, intended mission set, in-
16 tended operational environment, intended target
17 set, or expected adversarial countermeasures
18 since any prior certification submitted under
19 this subsection.

20 **SEC. 7. IMPLEMENTATION.**

21 (a) REGULATIONS.—Not later than 180 days after
22 the date of the enactment of this Act, the Secretary shall
23 revise the Defense Federal Acquisition Regulation Supple-
24 ment and issue such regulations, guidance, and instruc-
25 tions as are necessary to implement this Act.

1 (b) INITIAL IMPLEMENTATION BRIEFING.—Not later
2 than 240 days after the date of the enactment of this Act,
3 the Secretary shall brief the Committees on Armed Serv-
4 ices of the Senate and House of Representatives on the
5 implementation plan for this Act, including—

6 (1) planned regulatory changes;

7 (2) directive and instruction updates; and

8 (3) any resource or organizational issues likely
9 to affect implementation.

10 **SEC. 8. AUTHORIZATION FOR SPECIALIZED AUTONOMOUS**
11 **WEAPON SYSTEMS.**

12 (a) PETITION FOR AUTHORIZATION.—The Secretary
13 may submit to the House and Senate Armed Services
14 Committees a formal request for authorization to develop,
15 procure, or field a specific autonomous weapon system or
16 category of systems that does not meet the exceptions
17 under section 6(d).

18 (b) REQUIRED ELEMENTS OF REQUEST.—Any re-
19 quest submitted under subsection (a) shall include a clas-
20 sified annex containing the following:

21 (1) MILITARY NECESSITY STATEMENT.—A de-
22 tailed justification of why the mission cannot be ac-
23 complished through semi-autonomous weapon sys-
24 tems or existing human-in-the-loop capabilities.

1 (2) OPERATIONAL CONSTRAINTS.—The specific
2 operational, geographic, temporal, and target-class
3 constraints under which the system will operate.

4 (3) LAW OF ARMED CONFLICT COMPLIANCE
5 CERTIFICATION.—A written legal opinion from the
6 General Counsel of the Department certifying that
7 the system’s intended use complies with the Law of
8 Armed Conflict, specifically addressing how the sys-
9 tem will satisfy the principles of distinction and pro-
10 portionality.

11 (4) RISK MITIGATION PLAN.—A description of
12 the technical safeguards designed to prevent unau-
13 thorized autonomous action, flash wars, or unin-
14 tended escalation.

15 (5) HUMAN JUDGMENT FRAMEWORK.—A de-
16 scription of the appropriate levels of human judg-
17 ment that will be exercised, even if the system oper-
18 ates autonomously during the engagement phase.

19 (c) CONGRESSIONAL ACTION.—

20 (1) JOINT RESOLUTION OF APPROVAL.—A sys-
21 tem requested under subsection (a) may only be
22 fielded if Congress enacts a joint resolution of ap-
23 proval specifically naming the system and the au-
24 thorized mission set.

1 (2) EXPEDITED PROCEDURES.—For the pur-
2 poses of this section, the term “joint resolution”
3 means only a joint resolution that is introduced
4 within the 30-day period beginning on the date in
5 which the Secretary submits a request under sub-
6 section (a), and the matter after the resolving clause
7 is as follows: “That Congress approves the oper-
8 ational deployment of the autonomous weapon sys-
9 tem described in the request submitted by the Sec-
10 retary of Defense on _____.”, with the blank
11 space being filled with the date the request was sub-
12 mitted to Congress under subsection (a).

13 (3) REFERRAL.—A joint resolution introduced
14 in the Senate shall be referred to the Committee on
15 Armed Services. A joint resolution in the House of
16 Representatives shall be referred to the Committee
17 on Armed Services.

18 (4) DISCHARGE OF COMMITTEE.—If the com-
19 mittee to which is referred a joint resolution has not
20 reported such joint resolution (or an identical resolu-
21 tion) at the end of the 20 calendar days after the
22 introduction of such joint resolution, such committee
23 shall be deemed to be discharged from further con-
24 sideration of such resolution, and such joint resolu-

1 tion shall be placed on the appropriate calendar of
2 the chamber involved.

3 (5) PRIVILEGED MOTION IN THE SENATE.—

4 (A) MOTION TO PROCEED.—Notwith-
5 standing Rule XXII of the Standing Rules of
6 the Senate, it is in order at any time after the
7 Committee on Armed Services has reported or
8 has been discharged from consideration of a
9 joint resolution to move to proceed on the con-
10 sideration of the joint resolution. The motion is
11 privileged and is not debatable. The motion to
12 proceed is not subject to a motion to postpone.
13 A motion to reconsider the vote by which the
14 motion is agreed to or disagreed to shall not be
15 in order.

16 (B) LIMITS ON DEBATE.—Debate on the
17 joint resolution, and on all debatable motions
18 and appeals in connection therewith, shall be
19 limited to not more than 10 hours, which shall
20 be divided equally between those favoring and
21 those opposing the join resolution. A motion
22 further to limit debate is in order and not de-
23 batable.

24 (C) NO AMENDMENTS.—An amendment to
25 the joint resolution, or a motion to postpone, or

1 a motion to proceed to the consideration of
2 other business, or a motion to recommit the
3 joint resolution is not in order.

4 (6) VOTE ON FINAL PASSAGE.—Immediately
5 following the conclusion of the debate on a joint res-
6 olution, and a single quorum call at the conclusion
7 of the debate if requested in accordance with the
8 rules of the appropriate chamber, the vote on final
9 passage of the joint resolution shall occur.

10 (d) DURATION AND RENEWAL.—Any authorization
11 granted under this section shall expire 3 years after the
12 date of enactment of the joint resolution of approval, but
13 the Secretary may submit a renewed request under sub-
14 section (a) for expedited consideration under subsection
15 (c). The Secretary must certify in such request that sys-
16 tem has operated within the approved parameters.

○