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 intelligence by the Department of Defense, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Secure and Accountable Military AI Act of 2026''.

SEC. 2. DEFINITIONS.

In this Act:

(1) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given that term

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

(2) AUTONOMOUS WEAPON SYSTEM.—The term ''autonomous weapon system'' means a weapon system that, once activated, can select and engage targets without further intervention by an operator, including operator-supervised autonomous weapon systems that, after activation, can select and engage targets without further operator input.

(3) COVERED CONTRACT.—The term ''covered contract'' means a contract, task order, delivery order, or other agreement for the development, training, fine-tuning, evaluation, hosting, integration, or provision of an artificial intelligence model or artificial intelligence system for use by the Department.

(4) COVERED CONTRACTOR.—The term ''covered contractor'' means an entity that develops or provides a frontier artificial intelligence model to the Department under a covered contract.

(5) COVERED INCIDENT.—The term ''covered incident'' means any of the following:

(A) Theft, unauthorized access, unauthorized acquisition, or exfiltration of model weights for an artificial intelligence model, including—

(i) instances in which a model autonomously attempts to exfiltrate such model weights or acquire unauthorized access to systems containing such model weights; and

(ii) credible evidence indicating attempts or material vulnerabilities, relating to any such theft, access, acquisition, or exfiltration.

(B) Attempts by a foreign adversary or individual acting on behalf of a foreign adversary to obtain unauthorized access to, acquire, influence, or exfiltrate sensitive information, systems, or intellectual property related to an artificial intelligence model or artificial intelligence system, including through insider threats, compromised personnel, covert affiliations, or other deceptive means.

(C) A compromise of the software, hardware, cloud, data, or other supply chain used to develop, train, fine-tune, evaluate, secure, or deploy an artificial intelligence model or artificial intelligence system, where such compromise could reasonably affect the confidentiality, in-

tegrity, availability, reliability, or security of the model or system provided to the Department.

(D) Poisoning, corruption, manipulation, or unauthorized alteration of training data, fine-tuning data, retrieval corpora, model checkpoints, system prompts, safety filters, monitoring systems, evaluation pipelines, or model-update mechanisms.

(E) The discovery of a material vulnerability, exploit, backdoor, or failure of access controls that could permit unauthorized modification, extraction, degradation, or misuse of an artificial intelligence model or artificial intelligence system.

(F) Any materially concerning model behavior, including materially increased capability for cyber offense, exploitation, exploitation or evasion of safeguards, deceptive behavior, capabilities related to chemical or biological weapons, automated research and development in national security domains, automated research and development toward increasingly powerful artificial systems, unauthorized autonomous action, or other behavior that poses a significant 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

relating to nuclear command, control, and communications, intelligence support to lethal targeting, cyber operations, autonomous weapon systems, military decision support in time-sensitive operations, homeland-facing surveillance or monitoring, or mission-critical logistics and sustainment.

(9) INDIVIDUAL.—The term ''individual'' means a natural person.

(10) LOCAL DEFENSE.—The term ''local defense'' means defense within a specifically defined geographic defensive area (commonly referred to as ''point defense'') or of a high-value physical asset (commonly referred to as ''platform defense'') and for a specifically defined period of operation approved for the system concerned.

(11) MATERIEL TARGET.—The term ''materiel target'' —

(A) means a weapon, munition, military vehicle, military vessel, military aircraft, unmanned system, or other military object; and

(B) does not include an individual.

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

tions, or routines of an individual or a group of individuals.

(13) PERSISTENT PERSON-CENTRIC ANALYTIC PRODUCT.—The term ''persistent person-centric analytic product'' means a dossier, watchlist, score, profile, targeting package, or other record organized primarily around an identified or identifiable individual.

(14) OPERATIONAL DEPLOYMENT.—The term ''operational deployment'' means use of an artificial intelligence system in support of, or as part of, an operational military mission, contingency, or real-world military activity other than testing, training, evaluation, or experimentation conducted in a controlled environment.

(15) OPERATOR-SUPERVISED AUTONOMOUS WEAPON SYSTEM.—The term ''operator-supervised autonomous weapon system'' means an autonomous weapon system that is designed to provide operators with the ability to intervene and terminate engagements, including in the event of a weapon system failure, before unacceptable levels of damage occur.

(16) SECRETARY.—The term ''Secretary'' means the Secretary of Defense.

(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

seeker activates are those individual targets or specific target groups that have been selected by an operator.

(18) UNITED STATES PERSON.—The term ''United States person'' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

SEC. 3. HIGH-CONSEQUENCE MILITARY ARTIFICIAL INTELLIGENCE OVERSIGHT.

(a) DESIGNATION OF HIGH-CONSEQUENCE APPLICATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall establish and maintain a process to designate categories of artificial intelligence applications of the Department as high-consequence.

(2) DESIGNATIONS.—The following categories shall be designated as high-consequence artificial intelligence applications pursuant to paragraph (1):

(A) Artificial intelligence used for the selection of targets for, or execution of the launch or detonation of, a nuclear weapon.

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

ligence fusion or target recommendation for lethal operations.

(C) Artificial intelligence used in support of cyber operations that are intended or reasonably likely to create effects outside Department-owned or Department-controlled information systems.

(D) Autonomous weapon systems and operator-supervised autonomous weapon systems.

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

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

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

or the Vice Chairman of the Joint Chiefs of Staff, determines in writing that the application satisfies the requirements of subsection (c).

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

(1) Realistic developmental and operational testing and evaluation sufficient to assess performance, capability, reliability, effectiveness, suitability, and resilience under expected operational conditions, including adversarial conditions where feasible.

(2) Legal and policy review.

(3) Documentation of intended missions, intended operational environments, intended target or decision sets, known limitations, failure modes, and assumptions.

(4) Clear procedures for trained operators to activate, deactivate, override, or terminate system functions, and the circumstances requiring such actions.

(5) Fallback procedures and mission-continuity measures in the event of degradation, anomalous behavior, compromise, or system failure.

(6) Logging, auditability, and record-retention mechanisms sufficient to support oversight, investigation, and after-action review.

(7) Post-deployment continuous monitoring mechanisms.

(8) Training, doctrine, and tactics, techniques, and procedures appropriate to the use of the application.

(d) CONGRESSIONAL NOTIFICATION.—

(1) IN GENERAL.—Except as provided in paragraph (3), not later than 15 days before the initial operational deployment of a category of high-consequence artificial intelligence application, the Secretary shall notify the Committees on Armed Services of the Senate and House of Representatives of such deployment.

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

(A) a description of the application;

(B) the mission set, operational environment, and, as appropriate, target or decision set for which the application is intended;

(C) a summary of the testing and evaluation conducted;

(D) a description of key safeguards, limitations, and fallback procedures;

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

(F) any other matters the Secretary determines appropriate.

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

(A) determines that there are extraordinary circumstances affecting the national security of the United States; and

(B) provides, with the notification, a statement of such circumstances necessitating delayed notice.

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

SEC. 4. HUMAN ACCOUNTABILITY FOR HIGH-CONSEQUENCE MILITARY ARTIFICIAL INTELLIGENCE.

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

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

(c) REQUIRED ELEMENTS.—The accountable human decision-maker or chain of decision-makers under subsection (b) shall have, as appropriate to the application—

(1) documented commander intent and mission parameters;

(2) sufficient training on the capabilities, limitations, and failure modes of the application;

(3) access to relevant information necessary to understand the basis for significant system outputs or recommendations, to the extent technically feasible;

(4) authority and practical ability to pause, override, deactivate, or terminate use of the application when required by law, policy, or operational circumstances; and

(5) procedures for elevating uncertainty, anomalous outputs, or significant incidents for further human review.

SEC. 5. REPORTING OF SECURITY INCIDENTS AND CONCERNING MODEL BEHAVIORS BY CERTAIN FRONTIER ARTIFICIAL INTELLIGENCE CONTRACTORS.

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

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

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

(b) IMPLEMENTATION GUIDANCE AND CLARITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall issue guidance to covered contractors regarding the implementation of this section in order to promote clear, predictable, and consistent reporting expectations and support good-faith compliance.

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

(A) illustrative examples of covered incidents, factors relevant to determining whether an incident is material or reportable;

(B) reporting procedures and timelines; and

(C) other information the Secretary determines appropriate to promote consistent implementation and reduce uncertainty for covered contractors.

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

changes in artificial intelligence capabilities, deployment practices, threat environments, and reporting needs of the Department.

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

(c) REPORTING TIMELINE FOR COVERED CONTRACTORS.—

(1) IN GENERAL.—A covered contractor shall submit to the Under Secretary for Research and Engineering—

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

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

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

(2) SUPPLEMENTAL UPDATES.—A covered contractor shall submit to the Secretary supplemental updates with respect to any covered incident as material new information becomes available.

(d) CONTENTS OF CONTRACTOR REPORT.—Each report submitted by a covered contractor in accordance with this section shall include, to the extent known at the time of submission—

(1) a description of the covered incident;

(2) the date or approximate period of occurrence and discovery;

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

(4) the actual or suspected means of compromise, exfiltration, manipulation, degradation, or misuse;

(5) whether model weights, training data, system prompts, source code, evaluation data, safety systems, or software dependencies were accessed, altered, degraded, poisoned, exfiltrated, or otherwise compromised;

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

(7) any actions taken to contain, mitigate, remediate, or investigate the covered incident;

(8) whether the covered incident has been reported to any other Federal department or agency; and

(9) such other information as the Secretary determines appropriate.

(e) RECIPIENTS WITHIN THE DEPARTMENT.—A report submitted to the Secretary under this section shall be transmitted by the Secretary to—

(1) the contracting officer for the covered contract;

(2) the Chief Digital and Artificial Intelligence Office;

(3) the Chief Information Officer of the Department of Defense;

(4) the Under Secretary of Defense for Acquisition and Sustainment;

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

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

(7) the heads of such other components of the Department and other Federal departments or agencies as the Secretary determines appropriate.

(f) CONGRESSIONAL NOTIFICATION BY DEPARTMENT.—

(1) IN GENERAL.—Not later than 7 days after receipt of an initial report under subsection (b) regarding a covered incident, or the discovery of a covered incident by the Department, the Secretary shall submit to the Committees on Armed Services of the Senate and House of Representatives notice of such covered incident.

(2) CONTENTS.—A notice required by paragraph (1) shall include, to the extent known at the time of submission—

(A) a summary description of the covered incident;

(B) the date or approximate period of occurrence and discovery;

(C) the artificial intelligence model, artificial intelligence system, or relevant training, fine-tuning, evaluation, or deployment environment affected;

(D) the actual or suspected means of compromise, exfiltration, manipulation, degradation, or misuse;

(E) an initial assessment of actual or potential impact on missions, users, systems, or operations of the Department; and

(F) any actions taken or planned to contain, mitigate, remediate, or investigate the covered incident.

(3) ADDITIONAL UPDATES.—The Secretary shall provide to the Committees on Armed Services of the Senate and House of Representatives additional briefings or updates on a covered incident as material information becomes available.

(g) PROTECTION OF REPORTED INFORMATION.—The Secretary shall establish procedures for the handling of reports under this section, including procedures to protect classified information, proprietary information, trade secrets, security-sensitive information, and information regarding vulnerabilities that, if disclosed publicly, could reasonably be expected to harm national security.

(h) RULE OF CONSTRUCTION.—Nothing in this section shall be construed—

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

fied information, sensitive compartmented information, or other information protected by law;

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

(3) to limit any other reporting obligation imposed by law, regulation, or contract.

SEC. 6. LIMITATIONS ON CERTAIN USES OF ARTIFICIAL INTELLIGENCE BY THE DEPARTMENT.

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

(1) use artificial intelligence for the selection of targets for the use of a nuclear weapon or for the execution of launching or detonating a nuclear weapon;

(2) except as provided in subparagraph (b), use artificial intelligence to acquire, collect, ingest, retain, query, correlate, analyze, or disseminate information concerning a United States person located in the United States for the purpose of—

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

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

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

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

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

(F) selecting such person for investigative, operational, or law enforcement attention, unless such activity is expressly authorized by Federal law and supported by a lawful and documented predicate; or

(3) develop, procure, field, or employ an autonomous weapon system, except as provided in subsection (d).

(b) RULE OF CONSTRUCTION.—Subsection (a) shall not be construed to prohibit the use of artificial intelligence—

(1) for cybersecurity, information assurance, threat detection, vulnerability management, malware analysis, incident response, or defensive cyberspace operations undertaken to protect the Department of Defense Information Network, information systems, weapons systems, military networks, or defense critical infrastructure of the Department from malicious cyber activity;

(2) for force protection or counterintelligence purposes to identify, assess, or warn of a specific, credible, and articulable threat to personnel, installations, facilities, operations, activities, or covered assets of the Department; or

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

(c) ADDITIONAL LIMITATIONS ON DOMESTIC USES.—The Department may not use artificial intelligence—

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

(2) to acquire, correlate, or analyze publicly available information, commercially available information, or hacked, leaked, or breached data that is posted online or made available for sale for the primary purpose of circumventing otherwise applicable constitutional, statutory, or regulatory protections governing collection, retention, querying, or dissemination of information by the Federal Government concerning United States persons.

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

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

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

(A) static defense of installations with personnel, including networked defense in which the autonomous weapon system is not co-located with the installation; or

(B) onboard or networked defense of platforms with onboard personnel.

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

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

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

(1) has undergone legal review for consistency with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement;

(2) has completed rigorous verification and validation and realistic developmental and operational testing and evaluation under conditions that reflect the intended operational environment and reasonably anticipated adversary countermeasures;

(3) is designed and fielded to permit commanders and operators to exercise appropriate levels of human judgment over the use of force;

(4) includes human-machine interfaces and controls that—

(A) are readily understandable to trained operators;

(B) provide transparent feedback on system status;

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

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

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

(5) is approved for use only within defined temporal, geographic, environmental, and operational constraints, and, if unable to complete an engagement consistent with such constraints, is designed to terminate the engagement or obtain additional operator input before continuing; and

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

(f) CERTIFICATION AND NOTIFICATION.—

(1) IN GENERAL.—Not later than 30 days before fielding a system pursuant to subsection (d), the Secretary shall submit to the congressional defense committees a written certification that the system falls within one of the exceptions under subsection (d) and satisfies the conditions of subsection (e).

(2) CONTENTS.—A certification under paragraph (1) shall include—

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

(B) a summary of the legal review conducted under subsection (e)(1);

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

(D) the temporal, geographic, environmental, and operational constraints approved for the system;

(E) a description of the operator supervision concept, including procedures for intervention, termination, activation, and deactivation;

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

(G) any substantial modification to the system's algorithms, intended mission set, intended operational environment, intended target set, or expected adversarial countermeasures since any prior certification submitted under this subsection.

SEC. 7. IMPLEMENTATION.

(a) REGULATIONS.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall revise the Defense Federal Acquisition Regulation Supplement and issue such regulations, guidance, and instructions as are necessary to implement this Act.

(b) INITIAL IMPLEMENTATION BRIEFING.—Not later than 240 days after the date of the enactment of this Act, the Secretary shall brief the Committees on Armed Services of the Senate and House of Representatives on the implementation plan for this Act, including—

(1) planned regulatory changes;

(2) directive and instruction updates; and

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

SEC. 8. AUTHORIZATION FOR SPECIALIZED AUTONOMOUS WEAPON SYSTEMS.

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

(b) REQUIRED ELEMENTS OF REQUEST.—Any request submitted under subsection (a) shall include a classified annex containing the following:

(1) MILITARY NECESSITY STATEMENT.—A detailed justification of why the mission cannot be accomplished through semi-autonomous weapon systems or existing human-in-the-loop capabilities.

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

(3) LAW OF ARMED CONFLICT COMPLIANCE CERTIFICATION.—A written legal opinion from the General Counsel of the Department certifying that the system's intended use complies with the Law of Armed Conflict, specifically addressing how the system will satisfy the principles of distinction and proportionality.

(4) RISK MITIGATION PLAN.—A description of the technical safeguards designed to prevent unauthorized autonomous action, flash wars, or unintended escalation.

(5) HUMAN JUDGMENT FRAMEWORK.—A description of the appropriate levels of human judgment that will be exercised, even if the system operates autonomously during the engagement phase.

(c) CONGRESSIONAL ACTION.—

(1) JOINT RESOLUTION OF APPROVAL.—A system requested under subsection (a) may only be fielded if Congress enacts a joint resolution of approval specifically naming the system and the authorized mission set.

(2) EXPEDITED PROCEDURES.—For the purposes of this section, the term ''joint resolution'' means only a joint resolution that is introduced within the 30-day period beginning on the date in which the Secretary submits a request under subsection (a), and the matter after the resolving clause is as follows: ''That Congress approves the operational deployment of the autonomous weapon system described in the request submitted by the Secretary of Defense on _____.'', with the blank space being filled with the date the request was submitted to Congress under subsection (a).

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

(4) DISCHARGE OF COMMITTEE.—If the committee to which is referred a joint resolution has not reported such joint resolution (or an identical resolution) at the end of the 20 calendar days after the introduction of such joint resolution, such committee shall be deemed to be discharged from further consideration of such resolution, and such joint resolu-

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

(5) PRIVILEGED MOTION IN THE SENATE.—

(A) MOTION TO PROCEED.—Notwithstanding Rule XXII of the Standing Rules of the Senate, it is in order at any time after the Committee on Armed Services has reported or has been discharged from consideration of a joint resolution to move to proceed on the consideration of the joint resolution. The motion is privileged and is not debatable. The motion to proceed is not subject to a motion to postpone. A motion to reconsider the vote by which the motion is agreed to or disagreed to shall not be in order.

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

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

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

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

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

○