119TH CONGRESS
2D SESSION

S. _____

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

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

A BILL

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

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Human Authority in Lethal Operations Act of 2026'' or the ''HALO Act of 2026''.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

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

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

(2) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given such term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

(3) AUTONOMOUS WEAPON SYSTEM.—

(A) IN GENERAL.—The term ''autonomous weapon system'' means a weapon system that, once activated, can identify, select, or engage targets without further intervention by or communication with a human operator.

(B) INCLUDES.—The term defined in subparagraph (A) includes weapon systems that have human-operated supervision with the ability to override complete operation of the system, but can select and engage targets without fur-

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

(4) COVERED ARTIFICIAL INTELLIGENCE CAPABILITY.—The term ''covered artificial intelligence capability'' means an artificial intelligence designed, tested, developed, procured, deployed, or used by, on behalf of, or shared with the Department.

(5) DESIGNATED COMMANDER.—The term ''designated commander'' means the highest ranking commissioned officer within the chain of command who exercises operational or administrative command authority over an autonomous or semi-autonomous weapons system.

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

(7) ETHICAL PRINCIPLES FOR ARTIFICIAL INTELLIGENCE.—The term ''Ethical Principles for Artificial Intelligence'' means the Ethical Principles for Artificial Intelligence adopted by the Department on February 24, 2020, as in effect on January 1, 2025.

(8) MILITARY DEPARTMENTS.—The term ''military departments'' has the meaning given such term in section 101(a) of title 10, United States Code.

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

term ''Responsible Artificial Intelligence Strategy and Implementation Pathway'' means the Responsible Artificial Intelligence Strategy and Implementation Pathway dated June 2022 and prepared by the Department of Defense Responsible Artificial Intelligence Working Council in accordance with the memorandum issued by Deputy Secretary of Defense Kathleen Hicks on May 26, 2021, Implementing Responsible Artificial Intelligence in the Department of Defense, as in effect on January 1, 2025.

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

(11) 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 individual targets or specific target groups that have been previously selected by a human operator.

(B) INCLUDED.—The term defined in subparagraph (A) includes weapon systems that autonomously conduct engagement-related functions, including the following:

(i) Acquiring, tracking, and identifying potential targets.

(ii) Cuing potential targets to human operators.

(iii) Prioritizing selected targets.

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

(v) Providing terminal guidance on how to narrowly categorize selected targets, only if human operator control is retained for the purpose of selecting individual targets and specific target groups for engagement.

(12) SPECIFIC TARGET GROUP.—

(A) IN GENERAL.—The term ''specific target group'' means a discrete group of potential targets, such as a particular flight of enemy aircraft, a particular formation of enemy tanks, or a particular flotilla of enemy vessels.

(B) EXCLUDED.—The term defined in subparagraph (A) does not include a general class of targets or a specific type of target, such as a particular model of tank or aircraft.

(13) UNINTENDED ENGAGEMENT.—The term ''unintended engagement'' means the use of force outcomes resulting in damage to persons or objects 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)—

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

(B) the Secretary shall ensure that a designated commander is identified as accountable under applicable military and international laws for each engagement or class of engagements involving a system described in subsection (a)(2), regardless of the degree to which artificial intelligence contributed to the identification, development, recommendation, selection, or engagement of the target; and

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

(2) SYSTEM REQUIREMENTS.—Each system described in subsection (a)(2) shall incorporate the following:

(A) A system design that incorporates capabilities and interfaces that require the designated commander to exercise ultimate discretion, judgment and control in the envisioned development, planning, deployment, and use processes for the weapon system, including constraints on each such system's authorized actions, targets, and geographic, temporal, and contextual scope, which the system may not expand or modify without explicit human authorization.

(B) System capabilities, human-machine interfaces, doctrine, tactics, techniques, procedures, and human operator training must require commanders and human operators to use the system with deference to their discretion regarding care, and to analyze the output, in accordance with the Law of Armed Conflict and relevant laws of the United States and international laws, applicable treaties, weapon system safety rules, and rules of engagement that are applicable or reasonably expected to be applicable.

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

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

(D) The design, testing, development, procurement, deployment, legal analysis and review, and use of artificial intelligence capabilities in autonomous and semi-autonomous weapon systems shall be consistent with, but not limited to, the Ethical Principles for Artificial Intelligence and the Responsible Artificial Intelligence Strategy and Implementation Pathway.

(3) AVAILABILITY TO THE PUBLIC.—The Secretary shall ensure that—

(A) the Ethical Principles for Artificial Intelligence and the Responsible Artificial Intelligence Strategy and Implementation Pathway are available to the public; and

(B) any revision to the Ethical Principles for Artificial Intelligence or the Responsible Artificial Intelligence Strategy and Implementation Pathway adopted by the Secretary is made available to the public before the date that is 30 days before the date on which the revision goes into effect.

(c) ENGAGEMENT CONSTRAINTS AND TERMINATION.—

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

(A) to complete engagements within a designated timeframe and designated geographic area and against a designated set of potential targets, as well as other relevant constraints, consistent with commander and human operator intentions;

(B) to require independent review and analysis of a designated commander before using force against previously unauthorized targets, materially expanding target sets or geographic scope, taking actions contravening applicable law, rules of engagement, other relevant laws of the United States and international laws, or taking actions likely to result in unintended engagement; and

(C) if unable to complete an engagement consistent with the parameters described in paragraph (1), to terminate the engagement until additional human operator and commander evaluation is completed.

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

(d) TRANSPARENCY, AUDITABILITY, AND EXPLAINABILITY.—Consistent with the potential consequences of an unintended engagement or unauthorized interference with the operation of a system described in subsection (a)(2), the physical hardware and software of such system shall be designed with—

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

(2) system safety, anti-tamper mechanisms, and cybersecurity in accordance with Department instructions and military standards governing cybersecurity and system safety.

(e) ACTIVATION, TERMINATION, AND HUMAN OPERATOR INTERFACE.—Each system described in subsection (a)(2) shall be designed so that—

(1) system design and human-machine interfaces are readily understandable to trained human

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

(2) clear procedures exist for trained human operators to activate, terminate, and disable all weapon system functions;

(3) the system provides timely feedback on system status, including regarding the quality and sufficiency of the data inputs relied upon, to human operators in real time or near-real time; and

(4) adequate training, tactics, techniques, procedures, and doctrine are available, reviewed on a quarterly basis, by weapon system human operators and designated commanders to understand the functioning, capabilities, and limitations of the system's autonomy in realistic operational conditions.

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

(g) CONTINUOUS MONITORING.—The Secretary shall, in coordination with the Director of Operational Test and Evaluation, the Under Secretary of Defense for Research and Engineering, and the appropriate Secretary of a military department or Assistant Secretary for Special Operations and Low-Intensity Conflict, establish and maintain procedures for continuous monitoring of each system, to the greatest extent possible, described in subsection (a)(2) to identify and address circumstances in which changes to the system design or operational environment require additional testing and evaluation or legal review to provide sufficient confidence that the system will continue—

(1) to function as intended;

(2) to avoid unintended engagements;

(3) to resist interference by unauthorized parties; and

(4) to remain compliant with relevant laws of the United States, the Law of Armed Conflict, and international laws.

(h) ROBUST ARTIFICIAL INTELLIGENCE DESIGN.—For any system described in subsection (a) that incorporates artificial intelligence capabilities, such system shall be designed to utilize robust artificial intelligence, in accordance with the Responsible Artificial Intelligence

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

SEC. 4. ADVANCED REVIEW AND APPROVAL AUTHORITY.

(a) GENERAL REQUIREMENT FOR ADVANCED REVIEW.—With the exception of systems described in subsection (e), the Secretary shall ensure that each system described in section 3(a)(2) is approved in accordance with this section before formal development and before fielding.

(b) PRE-DEVELOPMENT REVIEW.—Before a decision to enter formal development of a system described in subsection (a), the Under Secretary of Defense for Policy, the Under Secretary of Defense for Research and Engineering, and the Vice Chairman of the Joint Chiefs of Staff shall jointly verify that—

(1) the weapon system design incorporates the necessary capabilities to allow a designated commander to exercise ultimate discretion, judgment, and control over the use of force in the envisioned planning, deployment, and use processes for the weapon;

(2) the system is designed to complete engagements within a designated timeframe and designated geographic area and against a designated set of potential 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-

sistency with the Ethical Principles for Artificial Intelligence and the Responsible Artificial Intelligence Strategy and Implementation Pathway; and

(7) a thorough legal analysis, review, and risk assessment of a system described in subsection (a) has been completed in coordination with the General Counsel of the Department and other relevant Department General Counsels and in accordance with applicable directives governing the Defense Acquisition System, the Department of Defense Law of War Program, the Law of Armed Conflict, and other relevant laws of the United States and international laws.

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

(1) system capabilities, human-machine interfaces, doctrine, tactics, techniques, procedures, and training have been demonstrated to allow a designated commander to exercise ultimate discretion, control, and judgment over the use of force and to use systems whose outcomes are sufficiently accurate with thorough legal analysis in accordance with the

law of war, Law of Armed Conflict, applicable treaties, weapon system safety rules, and rules of engagement reasonably expected to be applicable;

(2) system safety, anti-tamper mechanisms, cyber survivability, operational resilience, and cybersecurity capabilities have been implemented to minimize the probability and consequences of failures, including unpredictable outcomes, and a monitoring protocol is in place to identify and address changes in operational environment, data inputs, and use that could contribute to such failures;

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

(A) assessed system performance, capability, reliability, risk margins, effectiveness, and suitability under realistic conditions, including possible adversary actions, interference, or unintended consequences; and

(B) have demonstrated that the system can be revised as needed with sufficient rapidity to enable timely correction of any unintended system behaviors that may be observed or discovered during future system operations;

(4) adequate training, tactics, techniques, procedures, and doctrine are available, quarterly re-

viewed, and used by system operators and commanders to understand the functioning, capabilities, and limitations of the system in real world conditions;

(5) system design and human-machine interfaces are readily understandable to trained human operators, provide transparent feedback on system status, provide secure logging to enable traceability, and provide clear procedures for trained human operators to activate and terminate system functions;

(6) for systems incorporating artificial intelligence capabilities, the deployment and use of such capabilities in the weapon system will be consistent with the Ethical Principles for Artificial Intelligence, the Responsible Artificial Intelligence Strategy and Implementation Pathway, the Law of Armed Conflict, and other relevant laws of the United States and international laws; and

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

(d) RE-REVIEW OF MODIFIED SYSTEMS.—A system described in subsection (a) that is a variant of an existing weapon system previously approved through the review process under this section shall not be covered by previous approval if changes to the system algorithms, intended mission set, intended operational environments, intended target sets, or expected adversarial countermeasures materially differ from those applicable to the previously approved weapon system. Such systems shall require a new analysis, review, and risk assessment before formal development and again before fielding.

(e) SYSTEMS NOT REQUIRING ADVANCED REVIEW.—

(1) IN GENERAL.—Except as provided in paragraph (2), the advance review described in this section is not required for weapon systems intended to be used in the following manners:

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

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

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

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

(C) Human operator-supervised autonomous weapon systems used to select and engage materiel targets for purpose of protecting remotely piloted or autonomous vehicles and vessels.

(D) Autonomous weapon systems used to apply non-lethal, non-kinetic force against materiel targets.

(2) EXCEPTION.—Paragraph (1) shall not apply to a weapon system intended to be used in the manner described in subparagraph (B) of such paragraph in a case in which the engagement zone for the system encompasses densely populated areas or essential civilian infrastructure. In such a case, the weapon system shall undergo the advanced review described in this section to certify that the system can effectively distinguish between military targets and non-combatants or civilian objects in high-clutter environments.

SEC. 5. ROLE OF THE CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER.

(a) MONITORING AND EVALUATION.—The Chief Digital and Artificial Intelligence Officer shall monitor and evaluate artificial intelligence capabilities in, and cybersecurity for, autonomous and semi-autonomous weapon systems, and shall advise the Secretary on such matters.

(b) TESTABLE REQUIREMENTS.—The Chief Digital and Artificial Intelligence Officer shall, in collaboration with the Under Secretary of Defense for Research and Engineering—

(1) formulate concrete, testable requirements for implementing the Ethical Principles for Artificial Intelligence and the Responsible Artificial Intelligence Strategy and Implementation Pathway;

(2) establish policy and issue guidance on definitions of requirements and testability for artificial intelligence-enabled systems to implement and demonstrate adherence to the Ethical Principles for Artificial Intelligence and the Responsible Artificial Intelligence Strategy and Implementation Pathway; and

(3) issue guidance on test and evaluation practices for artificial intelligence capabilities in autonomous or semi-autonomous weapon systems, which shall include an adversarial assessment (known as

''red-team assessment'') that evaluates weapon system vulnerability to adversarial manipulation under operationally realistic conditions.

(c) COMMON TOOLS AND INFRASTRUCTURE.—The Chief Digital and Artificial Intelligence Officer shall coordinate with the Under Secretary of Defense for Research and Engineering and the Director of Operational Test and Evaluation on developing and using common tools and infrastructure for test and evaluation and verification and validation of artificial intelligence capabilities in autonomous or semi-autonomous weapon systems, including assurance benchmarks for reliability, robustness, security, and human-machine team performance.

SEC. 6. TESTING AND EVALUATION REQUIREMENTS.

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

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

(2) realistic system developmental and operational test and evaluation, including analysis of unanticipated emergent behavior.

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

(c) SPECIFIC REQUIREMENTS.—Testing and evaluation of a system under subsection (a) shall include the following:

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

(2) For a system incorporating artificial intelligence capabilities, rigorous developmental and operational test and evaluation to verify and validate that the artificial intelligence is robust according to design requirements.

(3) Testing to confirm that autonomy algorithms in systems incorporating artificial intelligence capabilities can be rapidly reprogrammed on new input data.

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

of a system under subsection (a), as directed by the Director of Operational Test and Evaluation—

(1) system data is collected and any further changes to the system undergo appropriate verification and validation and test and evaluation to ensure that critical safety features have not been degraded;

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

(3) any new or revised operating states or other relevant changes in the system are identified and undergoes appropriate and tailored additional test and evaluation to characterize the system behavior in that new operating state; and

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

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

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

(1) oversee development of realistic operational test, risk assessments, and evaluation standards for autonomous and semi-autonomous weapon systems, including requirements for data collection and standards for test and evaluation of any changes to the system following initial operational test and evaluation;

(2) evaluate whether autonomous and semi-autonomous weapon systems under the Director's oversight have met standards after being tested for rigorous verification, validation, and evaluation in realistic operational conditions, including potential adversary action, to ensure that the system is robust to minimize failures;

(3) establish standards for data collection post-fielding and monitoring and assessment by programs;

(4) establish and maintain a centralized repository for reporting, collecting, and analyzing operational incidents, weapon system failures, and unintended weapon system behaviors;

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

(6) coordinate with the Under Secretary of Defense for Research and Engineering and the appropriate Secretary of a military department or Assistant Secretary for Low-Intensity Conflict to provide for monitoring to identify and address when changes to the system design or operational environment require additional testing and evaluation to ensure that the system is robust to minimize failures such as unintended engagements with civilians and civilian infrastructure, densely populated areas, and resist interference by unauthorized parties.

SEC. 7. PROHIBITED USES OF ARTIFICIAL INTELLIGENCE.

(a) GENERAL PROHIBITION.—No covered artificial intelligence capability may be used in any manner that violates the Constitution of the United States, Federal law, the Law of Armed Conflict, or international treaty or other legal obligation of the United States, or in any manner that poses an unacceptable level of risk to the safety of an individual or the civil liberty of an individual.

(b) SPECIFIC PROHIBITIONS.—

(1) IN GENERAL.—No covered artificial intelligence capability may be used with the intent, purpose, or outcome of—

(A) profiling, targeting, tracking, monitoring, inferring, or concluding based on the data points of activity of any individual based solely on the exercise of rights protected under the Constitution or Federal law, including freedom of expression, association, and assembly;

(B) detecting, measuring, or inferring the emotional state of any individual from data acquired about such individual, including the support of the health of consenting personnel of the Federal Government;

(C) inferring or determining an individual's religion, ethnicity, race, sexual orientation, immigration status, disability status, gender identity, or political identity;

(D) tracking, monitoring, or inferring the past, real-time, or anticipated future location of any individual in the United States, including using data acquired from commercial, data brokers, data aggregators, or other third-party sources, unless such acquisition and use is authorized pursuant to an individualized judicial

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

(E) aggregating or analyzing internal data or data acquired from commercial, data brokers, data aggregators, or other third-party sources, including but not limited to location data, financial transaction data, communications metadata, or biometric data, to accomplish any purpose prohibited under paragraphs (1) through (4);

(F) removing a human from the chain of decisionmaking for actions critical to informing and executing decisions by the President, including initiating or terminating nuclear weapons employment; or

(G) obtaining, receiving, or otherwise accessing, for a fee or other consideration, any personal data of a United States person from a data broker or other third-party source, including any other governmental entity (including State, local, or Federal entities) if such data was obtained by that entity in a manner that would violate this subsection if performed by the Department.

(2) PERSONAL DATA.—For purposes of paragraph (1)(G), the term ''personal data''—

(A) means data, derived data, or any unique identifier that is linked to, or is reasonably linkable to, an individual or to an electronic device that is linked to, or is reasonably linkable to, one or more individuals in a household;

(B) includes anonymized data that, if combined with other data, can be linked to, or is reasonably linkable to, an individual or to an electronic device that identifies, is linked to, or is reasonably linkable to one or more individuals in a household; and

(C) does not include data that is lawfully available through Federal, State, or local government records or through widely distributed media; and

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

pability or protected data (as described in subsection (b)(7)) with another department or agency of the Federal Government, the receiving department or agency shall be subject to the same prohibitions and requirements as the Department with respect to the use, querying, or further dissemination of such systems, data, or products. The Secretary shall ensure that such department or agency is notified of, and in compliance with, the restrictions under this section.

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

SEC. 8. WHISTLEBLOWER PROTECTIONS.

(a) PROTECTIONS.—The Secretary shall update such whistleblower protections as the Secretary considers appropriate to clarify procedures for artificial intelligence systems, which shall ensure that all personnel who develop, assess, deploy, operate, or use artificial intelligence as a component of a National Security System (as defined in section 3552(b) of title 44, United States Code) or otherwise for military or intelligence purposes can report concerns about artificial intelligence, including concerns about improperly harming civil liberties, privacy, safety, or com-

pliance with the requirements of this Act, to relevant oversight officials.

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

(1) section 1034 of title 10, United States Code, and its implementation guidance under Department of Defense Directive 7050.06 (relating to military whistleblower protection);

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

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

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

(c) ANONYMITY.—

(1) IN GENERAL.—The Secretary shall ensure that adequate and special procedures exist to receive, investigate, respond to, and redress complaints anonymously, when appropriate, and that reports may be made confidentially so that personnel may raise concerns without fear of reprisal for any disclosures related to artificial intelligence.

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

(d) INVESTIGATION AND CORRECTIVE ACTION.—The Secretary shall ensure that adequate and special procedures exist for reporting incidents of artificial intelligence misuse, investigations of reported incidents, and processes for taking corrective actions.

SEC. 9. REPORTING REQUIREMENTS.

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

(1) A description of exemplary use cases of artificial intelligence within the Department during the preceding year, identifying best practices, failure modes, and risk mitigation strategies employed.

(2) After-action reports on significant operational use of covered artificial intelligence capabilities during the preceding year, including—

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

(B) any identified risks or failure modes;

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

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

(3) A description of training provided to human operators of autonomous and semi-autonomous weapon systems and other artificial intelligence capabilities covered by this Act, including documentation on employment procedures and responsible retirement of systems.

(b) ANNUAL REPORT ON INFRASTRUCTURE AND BARRIERS.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the Secretary shall submit to the appropriate committees of Congress a report identifying—

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

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

for artificial intelligence capabilities covered by this Act; and

(3) recommended hardware, software, or other infrastructure needs necessary to fulfill the requirements of this Act.

(c) SEMIANNUAL REPORT ON COMPLIANCE FOR FIELDED SYSTEMS.—Not later than six months after the date of the enactment of this Act, and semiannually thereafter, the Secretary shall submit to the appropriate committees of Congress a report identifying—

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

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

(3) a remediation plan and timeline for bringing each such system into compliance or, if compliance is not practicable, a plan for the responsible retirement or modification of the system.

SEC. 10. EXCEPTIONS.

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

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

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

(1) systems employed exclusively for the defense against incoming munitions, rockets, artillery, mortars, missiles; or

(2) unmanned aircraft systems.

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

(1) unguided munitions;

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

(3) mines;

(4) unexploded explosive ordnance; or

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

(e) IDENTIFICATION SYSTEMS.—The requirements of sections 3, 4, 5, and 7 shall not apply to a system described in section 3(a)(2) with the sole purpose and outcome of identifying potential targets without further intervention by or communication with a human operator.

SEC. 11. EFFECTIVE DATE; REVIEW OF SYSTEMS CURRENTLY IN USE.

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

(b) REVIEW OF SYSTEMS CURRENTLY IN USE.—

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

(2) ATTESTATION.—Upon completion of the review required under paragraph (1), the Secretary shall submit to the appropriate committees of Congress a written attestation identifying, for each reviewed system, whether the system is compliant with the requirements of sections 3, 6, and 7.

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

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

(A) a description of the specific requirement or requirements with which the system does not comply;

(B) an operational or national security justification, if any, for continued use of the system pending remediation; and

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