IN THE SENATE OF THE UNITED STATES—118th Cong., 2d Sess.

S. 4495

To enable safe, responsible, and agile procurement, development, and use of artificial intelligence by the Federal Government, and for other purposes.

Referred to the Committee on __________________ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Mr. Peters

Viz:

1 Strike all after the enacting clause and insert the fol-

owing:

3 SECTION 1. SHORT TITLE.

This Act may be cited as the “Promoting Responsible Evaluation and Procurement to Advance Readiness for Enterprise-wide Deployment for Artificial Intelligence Act” or the “PREPARED for AI Act”.

8 SEC. 2. DEFINITIONS.

In this Act:

10 (1) ADVERSE OUTCOME.—The term “adverse outcome” means any behavior or malfunction, such
as a hallucination, algorithmic bias, or inconsistent output, of artificial intelligence that leads to—

(A) harm impacting rights or safety, as described in section 7(a)(3);

(B) the death of an individual or damage to the health of an individual;

(C) material or irreversible disruption of the management and operation of critical infrastructure, as described in section 7(a)(3)(A)(ii)(III);

(D) material damage to property or the environment;

(E) loss of a mission-critical system or equipment;

(F) failure of the mission of an agency;

(G) the wrongful denial of a benefit, payment, or other service to an individual or group of individuals who would have otherwise been eligible;

(H) the denial of an employment, contract, grant, or similar opportunity that would have otherwise been offered; or

(I) another consequence, as determined by the Director with public notice.

(2) AGENCY.—The term “agency”—
(A) means each agency described in section 3502(1) of title 44, United States Code; and

(B) does not include each of the independent regulatory agencies described in section 3502(5) of title 44, United States Code.

(3) ARTIFICIAL INTELLIGENCE.—The term “artificial intelligence”—

(A) has the meaning given that term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401); and

(B) includes the artificial systems and techniques described in paragraphs (1) through (5) of section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 4061 note prec.).

(4) BIOMETRIC DATA.—The term “biometric data” means data resulting from specific technical processing relating to the unique physical, physiological, or behavioral characteristics of an individual, including facial images, dactyloscopic data, physical movement and gait, breath, voice, DNA, blood type, and expression of emotion, thought, or feeling.
(5) Commercial Technology.—The term “commercial technology”—

(A) means a technology, process, or method, including research or development; and

(B) includes commercial products, commercial services, and other commercial items, as defined in the Federal Acquisition Regulation, including any addition or update thereto by the Federal Acquisition Regulatory Council.

(6) Council.—The term “Council” means the Chief Artificial Intelligence Officers Council established under section 5(a).

(7) Deployer.—The term “deployer” means an entity that operates, whether for the entity itself or on behalf of a third party, artificial intelligence, whether developed internally or by a third-party developer.

(8) Developer.—The term “developer” means an entity that designs, codes, or produces artificial intelligence, including materially modifying artificial intelligence designed, coded, or produced by another entity.

(9) Director.—The term “Director” means the Director of the Office of Management and Budget.
(10) **GOVERNMENT DATA.**—The term “Government data” means data collected, processed, maintained, disseminated, or managed by an agency, including data reported to an agency.

(11) **IMPACT ASSESSMENT.**—The term “impact assessment” means a structured process for considering and evaluating the implications of a proposed artificial intelligence use case.

(12) **RELEVANT CONGRESSIONAL COMMITTEES.**—The term “relevant congressional committees” means the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Accountability of the House of Representatives.

(13) **RISK.**—The term “risk” means the combination of the probability of an occurrence of harm and the potential severity of that harm.

(14) **USE CASE.**—The term “use case” means the ways and context in which artificial intelligence is deployed to achieve a specific objective.

**SEC. 3. IMPLEMENTATION OF REQUIREMENTS.**

(a) **AGENCY IMPLEMENTATION.**—The Director shall facilitate the implementation of the requirements of this Act, including through the issuance of binding or non-binding guidance, as the Director determines appropriate.
(b) **ANNUAL BRIEFING.**—Not later than 180 days after the date of enactment of this Act, and annually thereafter, the Director shall brief the appropriate Congressional committees on implementation of this Act and related considerations.

**SEC. 4. PROCUREMENT OF ARTIFICIAL INTELLIGENCE.**

(a) **GOVERNMENT-WIDE REQUIREMENTS.**—

(1) **IN GENERAL.**—Not later than 15 months after the date of enactment of this Act, the Federal Acquisition Regulatory Council shall review Federal Acquisition Regulation acquisition planning, source selection, and other requirements and update the Federal Acquisition Regulation as needed for agency procurement of artificial intelligence, including—

(A) a requirement to address the outcomes of the risk evaluation and impact assessments required under section 7(a);

(B) a requirement for an interdisciplinary approach that includes consultation with agency experts prior to, and throughout, as necessary, procuring or obtaining artificial intelligence; and

(C) any other considerations determined relevant by the Federal Acquisition Regulatory Council.
(2) Harmonization.—The Federal Acquisition Regulation review described in paragraph (1) shall determine the extent to which existing requirements and procedures need to be revised or supplemented to address risks and opportunities specific to procurement of artificial intelligence.

(3) Interdisciplinary Approach.—The interdisciplinary approach described in paragraph (1)(B) may—

(A) vary depending on the use case and the risks determined to be associated with the use case; and

(B) include, as practicable, technologists, information security personnel, domain experts, privacy officers, data officers, civil rights and civil liberties officers, contracting officials, legal counsel, customer experience professionals, and others.

(4) Acquisition Planning.—The updates described in paragraph (1) shall, at a minimum, include—

(A) data ownership and privacy;

(B) data information security;

(C) interoperability requirements;

(D) data and model assessment processes;
(E) scope of use;

(F) ongoing monitoring and evaluation techniques;

(G) environmental impact;

(H) cybersecurity minimum standards, including regular vulnerability testing and patching and cybersecurity monitoring;

(I) risk mitigation techniques, including a plan for minimizing the likelihood of adverse outcomes and reporting adverse outcomes, pursuant to section 5(h); and

(J) developer and deployer disclosure requirements necessary to comply with the requirements of this Act.

(b) REQUIREMENTS FOR HIGH RISK ARTIFICIAL INTELLIGENCE USE CASES.—

(1) ESTABLISHMENT.—Beginning on the date that is 1 year after the date of enactment of this Act, the head of an agency may not procure or obtain artificial intelligence for a high risk use case, as defined in section 7(a)(3), prior to establishing and incorporating certain terms into relevant contracts and agreements for an artificial intelligence use case, including—
(A) a requirement to disclose to the agency the purpose for which the artificial intelligence was intended to be used and any potential risks from the use of the artificial intelligence;

(B) requirements for safety, security, privacy, and trustworthiness, including—

(i) a reporting mechanism through which agency personnel are notified of an adverse outcome involving artificial intelligence procured or obtained by the agency;

(ii) a requirement, in accordance with section 5(h), that agency personnel receive a notification of an adverse outcome involving artificial intelligence procured or obtained by the agency, and, at a minimum, an explanation of the cause of the adverse outcome and any data directly connected to the adverse outcome;

(iii) that the agency may consider temporarily or permanently suspending use of the artificial intelligence, with minimal impact on unrelated services, if the risks of the artificial intelligence to rights or safety outweigh the benefits of the use case; and
(iv) a requirement that the deployer and any relevant developer utilize the most recently updated version of the framework developed and updated pursuant to section 22(A)(c) of the National Institute of Standards and Technology Act (15 U.S.C. 278h-1(e));

(C) requirements to disclose to the agency sufficient descriptive information relating to the ownership of data, as appropriate by use case, including—

(i) requirements for retention of rights to Government data and any modification to Government data, including to protect Government data from unauthorized disclosure and use to subsequently train or improve the functionality of commercial products offered by the deployer, any relevant developers, or others; and

(ii) a requirement that the deployer, if the deployer is not the agency, and any relevant developers or other parties isolate non-public Government data from all other data through methods, such as physical separation, electronic separation via secure
copies with strict access controls, or other computational isolation mechanisms;

(D) requirements for evaluation and testing of artificial intelligence based on use case, to be performed on an ongoing basis; and

(E) requirements to provide documentation, as determined necessary and requested by the agency, in accordance with section 7(b).

(2) REVIEW.—The Senior Procurement Executive, in coordination with the Chief Artificial Intelligence Officer, shall, as practicable, consult with technologists, information security and cybersecurity personnel, domain experts, privacy officers, data officers, civil rights and civil liberties officers, contracting officials, legal counsel, customer experience professionals, program evaluation officers, and other relevant agency officials to review the requirements described in subparagraphs (A) through (E) of paragraph (1) and determine whether it may be necessary to incorporate additional requirements into relevant contracts or agreements.

(3) REGULATION.—The Federal Acquisition Regulatory Council shall revise the Federal Acquisition Regulation as necessary to implement the requirements of this subsection.
SEC. 5. INTERAGENCY GOVERNANCE OF ARTIFICIAL INTELLIGENCE.

(a) Chief Artificial Intelligence Officers Council.—Not later than 60 days after the date of enactment of this Act, the Director shall establish a Chief Artificial Intelligence Officers Council.

(b) Duties.—The duties of the Council shall include—

(1) coordinating agency development and use of artificial intelligence in agency programs and operations, including practices relating to the design, operation, risk management, and performance of artificial intelligence;

(2) sharing experiences, ideas, best practices, and innovative approaches relating to artificial intelligence;

(3) identifying, developing, and coordinating multi-agency projects and other initiatives;

(4) harmonizing agency management of risks relating to developing, obtaining, or using artificial intelligence, including by developing a common template to guide agency Chief Artificial Intelligence Officers in implementing a risk evaluation process that may incorporate best practices, such as those from—

(A) the most recently updated version of
to section 22A(c) of the National Institute of Standards and Technology Act (15 U.S.C. 278h–1(c)); and

(B) the report published by the Government Accountability Office entitled “Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities” (GAO-21-519SP), published on June 30, 2021;

(5) promoting the development and use of secure, common, shared, or other approaches to key processes that improve the delivery of services for the public;

(6) soliciting and providing perspectives on matters of concern, including from and to—

(A) interagency councils;

(B) Federal Government entities;

(C) private sector, public sector, nonprofit, and academic experts;

(D) State, local, Tribal, territorial, and international governments; and

(E) other individuals and entities, as determined relevant by the Council;

(7) working with the Chief Acquisition Officers Council—
(A) to ensure contractors, including small businesses, have the benefit of integrity, fairness, competition, openness, and efficiency in accordance with the statutory functions of the Chief Acquisition Officers Council, as described in section 1312 of title 41, United States Code; and

(B) which shall establish a working group for the purpose described in subparagraph (A) and related purposes; and

(8) any other matters determined by the Council to be relevant.

(e) Membership of the Council.—

(1) Leaders.—

(A) Chair.—The Director shall serve as Chair of the Council.

(B) Vice Chair.—The Council shall have a Vice Chair, who shall be an individual selected by a majority of the members of the Council.

(C) Additional roles.—The Council may establish additional leadership roles, at the discretion of the Council.

(2) Members.—Other members of the Council shall include—
(A) the Chief Artificial Intelligence Officer
of each agency; and
(B) the senior official for artificial intel-
ligence of the Office of Management and Budg-
et.

(d) **STANDING COMMITTEES; WORKING GROUPS.**—
The Council shall have the authority to establish standing
committees, including an executive committee, and work-
ing groups.

(e) **COUNCIL STAFF.**—The Council may enter into an
interagency agreement with the Administrator of General
Services for shared services for the purpose of staffing the
Council.

(f) **REPORTS.**—

(1) **IN GENERAL.**—Not later than 3 years after
the date of enactment of this Act, the Comptroller
General of the United States shall submit to the
Committee on Homeland Security and Governmental
Affairs of the Senate and the Committee on Over-
sight and Accountability of the House of Represent-
atives a report that—

(A) identifies, to the extent practicable,
ways to improve coordination with other coun-
cils throughout the Federal Government; and
(B) recommends ways to improve the utility of the Council for the public and other agencies.

(2) CONSOLIDATION.—In fulfilling the requirement under paragraph (1), the Comptroller General of the United States may, if desired, consolidate the report under that paragraph with another report concerning interagency coordination.

(g) DEVELOPMENT, ADAPTATION, AND DOCUMENTATION.—

(1) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Director shall issue guidance on—

(A) how to conduct the agency impact assessments described in section 7(a) and other relevant impact assessments as determined appropriate by the Director, including the appropriateness of adapting pre-existing assessments, including privacy and security impact assessments, for purposes of an artificial intelligence impact assessment;

(B) development of a model template for the risk classification explanations that each agency must provide under section 7(a)(6);
(C) development of a model template for procurement of artificial intelligence intended to help agencies use consistent terms, definitions, and documentation requirements; and

(D) additional matters relating to the implementation of this Act, as determined relevant by the Director.

(2) BIENNIAL REVIEW.—The Director shall periodically, but not less frequently than biennially, review and update, as needed, the guidance issued under paragraph (1).

(h) ADVERSE OUTCOME REPORTING.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall develop procedures for ensuring that, at a minimum—

(A) adverse outcomes involving artificial intelligence procured or obtained or used by agencies are reported promptly to the relevant agency or agencies by the developer or deployer, if the deployer is not the agency, or to the developer or deployer by the relevant agency, whichever first becomes aware of the adverse outcome; and
(B) information relating to an adverse outcome described in subparagraph (A) is appropriately shared among agencies.

(2) SINGLE REPORT.—Adverse outcomes also qualifying for incident reporting under section 3554 of title 44, United States Code, or other relevant laws or policies, may be reported under such other reporting requirement and are not required to be additionally reported under this subsection.

(3) NOTICE TO DEVELOPERS AND DEPLOYERS.—

(A) IN GENERAL.—If and upon discovery of an adverse outcome by an agency, the agency shall—

(i) report the adverse outcome to the deployer, if the deployer is not the agency, and any relevant developers; and

(ii) in consultation with any relevant deployers and developers, take action to resolve the adverse outcome and mitigate the potential for future adverse outcomes.

(B) WAIVER.—

(i) IN GENERAL.—Unless otherwise required by law, the head of an agency may issue a written waiver that waives the
applicability of some or all of the requirements under subparagraph (A), with respect to a specific adverse outcome.

(ii) **Written waiver contents.**—A written waiver under clause (i) shall include justification for the waiver.

(iii) **Notice.**—The head of an agency shall forward advance notice of any waiver under this subparagraph to the Director.

**SEC. 6. AGENCY GOVERNANCE OF ARTIFICIAL INTELLIGENCE.**

(a) **In general.**—The head of an agency shall—

(1) ensure the responsible adoption of artificial intelligence, including by—

(A) requiring the development or revision of relevant agency policies and directives;

(B) testing, verifying, validating, and monitoring artificial intelligence and the use case-specific performance of artificial intelligence, proportionate to risk level, to minimize the likelihood of adverse outcomes by—

(i) ensuring the use of artificial intelligence is appropriate to and improves the effectiveness of the mission of the agency;
(ii) guarding against bias in data collection, use, and dissemination;

(iii) ensuring reliability, fairness, and transparency; and

(iv) protecting against impermissible discrimination;

(C) continuing to hire, train, and develop a workforce that—

(i) understands the risks and benefits of artificial intelligence, including artificial intelligence embedded in agency systems and operations;

(ii) is able to provide human oversight for the design, implementation, and end uses of artificial intelligence; and

(iii) is able to review and provide redress for erroneous decisions made in the course of artificial intelligence-assisted processes; and

(D) ensuring implementation of the agency requirements under this Act;

(2) designate a Chief Artificial Intelligence Officer, whose duties shall include—

(A) ensuring appropriate use of artificial intelligence;
(B) coordinating agency use of artificial intelligence;

(C) promoting artificial intelligence innovation;

(D) managing the risks of use of artificial intelligence;

(E) minimizing the likelihood of adverse outcomes;

(F) supporting the head of the agency with developing the risk evaluation process required under section 7(a) and complying with other requirements of this Act;

(G) supporting agency personnel leading the procurement and deployment of artificial intelligence to comply with the requirements under this Act; and

(H) coordinating with other responsible officials and appropriate stakeholders with respect to the duties described in subparagraphs (A) through (G), as appropriate; and

(3) form and convene an Artificial Intelligence Governance Board, if required by subsection (b), which shall coordinate and govern artificial intelligence issues across the agency.
(b) Designation of Chief Artificial Intelligence Officer.—The head of an agency may designate as Chief Artificial Intelligence Officer an existing official within the agency, including the Chief Technology Officer, Chief Data Officer, Chief Information Officer, or other official with relevant or complementary authorities and responsibilities, if such existing official has expertise in artificial intelligence and meets the requirements of this section.

(c) Artificial Intelligence Governance Board.—

(1) Leadership.—Each agency identified in section 901(b) of title 31, United States Code, shall establish an Artificial Intelligence Governance Board (referred to in this subsection as “Board”) that shall be chaired by the Deputy Secretary of the agency or equivalent official and vice-chaired by the Chief Artificial Intelligence Officer of the agency. Neither the chair nor the vice-chair may assign or delegate these roles to other officials.

(2) Representation.—The Board shall, at a minimum, include representatives consisting of—

(A) senior agency officials from operational components, if relevant;
(B) program officials responsible for implementing artificial intelligence; and

(C) officials responsible for information technology, data, cybersecurity, privacy, statistics, civil rights and civil liberties, human capital, procurement, finance, legal counsel, agency management, program evaluation, and customer experience.

(3) EXISTING BODIES.—An agency may rely on an existing governance body to fulfill the requirements of this subsection if the body satisfies or is adjusted to satisfy the leadership and representation requirements of paragraphs (1) and (2).

(d) EFFECTIVE DATE.—Beginning on the date that is 120 days after the date of enactment of this Act, an agency shall not develop, procure, or obtain artificial intelligence prior to completing the requirements under paragraphs (2) and (3) of subsection (a).

SEC. 7. AGENCY REQUIREMENTS FOR USE OF ARTIFICIAL INTELLIGENCE.

(a) RISK EVALUATION PROCESS.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Chief Artificial Intelligence Officer of each agency, in coordination with the Artificial Intelligence Govern-
ance Board of the agency, shall develop and implement a process for identifying when the use of artificial intelligence by the agency meets the definition of high risk, as defined in paragraph (3).

(2) PROCESS REQUIREMENTS.—The risk evaluation process described in paragraph (1), shall include, for each artificial intelligence use case—

(A) identification of the purpose, expected benefits, and potential risks of the artificial intelligence use case;

(B) a plan to periodically review the artificial intelligence use case to examine whether the expected benefits and potential risks identified under subparagraph (A) have changed or evolved; and

(C) if a high risk determination has been made, the need for targeted impact assessments, beyond those required under any other provision of law, to further evaluate specific risks of the artificial intelligence use case in coordination with other responsible officials within certain impact areas, which shall include privacy, security, civil rights and civil liberties, accessibility, environmental impact, health and safety, and any other impact area relating to
high risk classification under paragraph (3) as determined appropriate by the Chief Artificial Intelligence Officer.

(3) HIGH RISK USE CASES.—

(A) IN GENERAL.—High risk classification shall, at a minimum, apply to use cases for which the outputs serve as a principal basis for—

(i) a decision or action that has a legal, material, binding, or similarly significant effect, with respect to an individual or community, on—

(I) civil rights, civil liberties, or privacy;

(II) access to education, housing, insurance, credit, employment, and other programs where civil rights and equal opportunity protections apply; or

(III) access to or the ability to apply for critical government resources or services, including healthcare, financial services, public housing, social services, transport-
(ii) a decision that substantially impacts the safety of, or has the potential to substantially impact the safety of—

(I) an individual or community, including loss of life, serious injury, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, or mental health;

(II) the environment, including irreversible or significant environmental damage;

(III) critical infrastructure, including the critical infrastructure sectors defined in National Security Memorandum 22 (NSM-22) (dated April 30, 2024) (or any successor directive) and the infrastructure for voting and protecting the integrity of elections; or

(IV) strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.
(B) **Classification variance.**—

(i) **Variance within a mission area.**—The risk evaluation process may allow for a particular operational use case to not be classified as high risk, even if the use case is a part of a larger area of the mission of the agency that is thought to be high risk, if the operational use case is determined not to be high risk based on the required risk evaluation under paragraph (1).

(ii) **Changes based on testing or new information.**—The risk evaluation process may allow for changes to the risk classification of an artificial intelligence use case based on the results from testing during the procurement process or other information that becomes available.

(4) **Review.**—Not later than 1 year after the date of enactment of this Act, the Chief Artificial Intelligence Officer of the agency shall—

(A) certify whether each existing use case presents a high risk; and

(B) identify and review any use cases the agency is planning, developing, procuring, or
obtaining to determine whether each such use cases presents a high risk.

(5) DEVELOPMENT.—For any artificial intelligence that is developed by the agency, the agency shall ensure a risk evaluation is conducted prior to deployment in a production or operational environment that is fit for the intended use.

(6) RATIONALE FOR RISK CLASSIFICATION.—

(A) IN GENERAL.—A high risk classification of an artificial intelligence use case shall be accompanied by an explanation from the agency, that a reasonable person would consider sufficient to understand, of how the classification was determined, which shall be included in the artificial intelligence use case inventory of the agency.

(B) TEMPLATE.—A risk classification explanation under subparagraph (A) shall utilize the model template developed by the Director under section 5(g)(1)(B) if the explanation is written after the date that such model template has become available.

(b) DOCUMENTATION REQUIREMENTS.—

(1) DOCUMENTATION FOR HIGH RISK USE CASES.—Beginning on the date that is 1 year after
the date of enactment of this Act, prior to developing, procuring or obtaining, or using artificial intelligence to be used in a high risk use case, an agency shall require the deployer, if the deployer is not the agency, in consultation with any relevant developers, to submit the following documentation:

(A) A description of the types of data sources used to train the artificial intelligence, whether the data is from licensed material, and an identification of the specific issues related to safety, bias, and fairness, that may be expected to arise from the use of the data, and any mitigation techniques used, if applicable.

(B) A description of the methodologies used to evaluate the performance of the artificial intelligence for its intended use.

(C) Documentation demonstrating implementation of risk evaluation and management measures, including the evaluation and management of safety, bias, and fairness risks, as appropriate.

(D) Information on the collection, management, and protection of data, in compliance with applicable laws.
(E) Documentation of the known limitations of the artificial intelligence, and if applicable, supplementary guidelines on how the artificial intelligence is intended to be used.

(2) SUFFICIENCY OF DOCUMENTATION.—The Chief Artificial Intelligence Officer of an agency shall determine the sufficiency of the documentation provided in meeting the requirements under paragraph (1).

(3) UPDATES.—An agency shall require that a deployer, if the deployer is not the agency, in consultation with any relevant developers, submit updates to the documentation required under paragraph (1), if and when there are any material changes to the information in such documentation.

(4) REVIEW OF REQUIREMENTS.—Not later than 2 years after the date of enactment of this Act, the Comptroller General shall conduct a review of the documentation requirements under paragraphs (1) and (3) to—

(A) examine whether agencies, third-party deployers, and developers are complying with the requirements under those paragraphs, and make associated findings and recommendations; and
(B) make general findings and recommendations to further assist in ensuring safe, responsible, and efficient agency procurement and use of artificial intelligence.

(5) SECURITY OF PROVIDED DOCUMENTATION.—The head of each agency shall ensure that appropriate security measures and access controls are in place to protect documentation provided pursuant to this section.

(c) INFORMATION AND USE PROTECTIONS.—Information provided to an agency under subsection (b) may be used by the agency, consistent with otherwise applicable provisions of Federal law, solely for—

(1) assessing the ability of artificial intelligence to achieve the requirements and objectives of the agency and the requirements of this Act; and

(2) identifying—

(A) adverse effects of artificial intelligence on the rights or safety factors identified in subsection (a)(3);

(B) cyber threats, including the sources of the cyber threats; and

(C) security vulnerabilities.

(d) PRE-DEPLOYMENT REQUIREMENTS FOR HIGH RISK ARTIFICIAL INTELLIGENCE USE CASES.—Beginning
on the date that is 18 months after the date of enactment of this Act, the head of an agency shall not deploy or use artificial intelligence for a high risk use case prior to—

(1) complying with the requirements of subsection (a);

(2) obtaining documentation of the artificial intelligence described in subsection (b)(2), source, and use case in agency software and use case inventories;

(3) testing the artificial intelligence in an operational, real-world setting with privacy, security, civil rights, and civil liberty safeguards to ensure the artificial intelligence is capable of meeting its objectives, and to determine, to the maximum extent practicable, the likelihood and impact of adverse outcomes occurring during use;

(4) establishing appropriate agency rules of behavior for the use case, including required human involvement in, and reasonable plain-language notice about, decisions made in whole or part by the artificial intelligence, as determined by the Chief Artificial Intelligence Officer in coordination with the program manager or equivalent agency personnel;

(5) if appropriate, consultation with and collection of feedback from affected communities and the
public on the design, development, and use of the high risk use case;

(6) establishing appropriate agency training programs, including documentation of completion of training prior to use of artificial intelligence, that educate agency personnel involved with the application of artificial intelligence in high risk use cases on the capacities and limitations of artificial intelligence, including training on—

(A) monitoring, detecting, and reporting anomalies, dysfunctions, and unexpected performance in a timely manner;

(B) reducing over-reliance on the output produced by artificial intelligence in a high risk use case, particularly if artificial intelligence is used to make decisions impacting individuals;

(C) accurately interpreting the output of artificial intelligence, particularly considering the characteristics of the system and the interpretation tools and methods available;

(D) when to not use, disregard, override, or reverse the output of artificial intelligence;

(E) how to intervene or interrupt the operation of artificial intelligence;
34

(F) limiting the use of artificial intelligence to its intended purpose; and

(G) procedures for reporting adverse outcomes, as determined under section 5(h), and other problems that may arise with artificial intelligence that does not function as intended; and

(7) determining whether the benefits of the use case outweigh the risks by—

(A) evaluating the information learned from completing the requirements under paragraphs (2) and (3); and

(B) assessing whether the requirements under paragraphs (2) through (6) have been accomplished and known risks have been effectively mitigated.

(e) Determinations.—

(1) Requests for determination information.—The head of an agency shall make available to the relevant congressional committees or the Director, upon request, a determination under subsection (d)(7) and the respective supporting documentation.

(2) Reevaluation.—If it is determined under subsection (d)(7) that the benefits of a use case do
not outweigh the risks and the risks cannot be effectively mitigated, the agency may decide to reevaluate the use case indefinitely or until appropriate measures under the requirements in paragraphs (2) through (6) of that subsection are established.

(f) ONGOING MONITORING OF ARTIFICIAL INTELLIGENCE IN HIGH RISK USE CASES.—Beginning on the date that is 1 year after the date of enactment of this Act, the Chief Artificial Intelligence Officer of each agency shall—

(1) establish a reporting system, consistent with section 5(h), and suspension and shut-down protocols for defects or adverse outcomes of artificial intelligence, and conduct ongoing monitoring, as determined necessary by use case;

(2) oversee the development and implementation of ongoing testing and evaluation processes for artificial intelligence in high risk use cases to ensure continued mitigation of the potential risks identified in the risk evaluation process; and

(3) implement a process to ensure that risk mitigation efforts for artificial intelligence are reviewed not less than annually and updated as necessary to account for the development of new
versions of artificial intelligence and changes to the risk profile.

(g) CHANGED RISKS.—In the process of complying with subsections (d) and (f), an agency shall determine whether an intended use case should be paused, stopped permanently, or continued if new information changes the risks associated with the use case or requires new testing and monitoring procedures under those subsections.

(h) EXCEPTION.—The requirements under subsections (a) and (b) shall not apply to an algorithm software update, enhancement, derivative, correction, defect, or fix for artificial intelligence that does not materially change the compliance of the deployer with the requirements of those subsections, unless determined otherwise by the agency Chief Artificial Intelligence Officer.

(i) WAIVERS.—

(1) IN GENERAL.—The head of an agency, or 1 or more deputy heads of an agency designated by the head of the agency, may waive 1 or more requirements under subsection (d) for a specific use case after making a written determination, based upon a risk assessment conducted by a human, that fulfilling the requirement or requirements would increase risks to safety or rights overall, would create an unacceptable impediment to critical agency oper-
ations, or would not be in the national security interests of the United States.

(2) Requirements.—A waiver under paragraph (1) shall—

(A) include, at a minimum, the reasons for the waiver and a plan to bring the specific use case into compliance with subsection (d) before the end of the waiver, pursuant to paragraph (4); and

(B) be submitted to the relevant congressional committees and the Director not later than 15 days after the head of the agency grants the waiver.

(3) Review.—The Director shall review the waiver and relevant documentation to determine whether the waiver was improperly granted.

(4) Duration.—A waiver under paragraph (1) shall be limited to a duration of 1 year, at which time, if the agency is unable to bring the specific use case into compliance with subsection (d), the agency shall cease use or deployment of the use case until the use case can be brought into compliance with that subsection.

(j) Infrastructure Security.—The head of an agency, in consultation with the agency Chief Artificial In-
intelligence Officer, Chief Information Officer, Chief Data Officer, and other relevant agency officials, shall reevaluate infrastructure security protocols based on the artificial intelligence use cases and associated risks to infrastructure security of the agency.

(k) **COMPLIANCE DEADLINE.**—Not later than 270 days after the date of enactment of this Act, the requirements of subsections (a) through (j) of this section shall apply with respect to artificial intelligence that is already in use on the date of enactment of this Act.

SEC. 8. PROHIBITION ON SELECT ARTIFICIAL INTELLIGENCE USE CASES.

No agency may develop, procure, obtain, or use artificial intelligence for—

(1) mapping facial biometric features of an individual to assign corresponding emotion and potentially take action against the individual;

(2) categorizing and taking action against an individual based on biometric data of the individual to deduce or infer race, political opinion, religious or philosophical beliefs, trade union status, sexual orientation, or other personal trait, with the exception of deducing or inferring age in the context of investigating child sexual abuse; or
(3) evaluating, classifying, rating, or scoring the trustworthiness or social standing of an individual based on multiple data points and time occurrences related to the social behavior of the individual in multiple contexts or known or predicted personal or personality characteristics in a manner that may lead to discriminatory outcomes.

SEC. 9. AGENCY PROCUREMENT INNOVATION LABS.

(a) In General.—Each agency identified in 901(b) of title 31, United States Code, that does not have a Procurement Innovation Lab on the date of enactment of this Act should consider establishing a lab or similar mechanism to test new approaches, share lessons learned, and promote best practices in procurement, including for commercial technology, such as artificial intelligence, that is trustworthy and best-suited for the needs of the agency.

(b) Functions.—The functions of the Procurement Innovation Lab or similar mechanism should include—

(1) providing leadership support as well as capability and capacity to test, document, and help agency programs adopt new and better practices through all stages of the acquisition lifecycle, beginning with project definition and requirements development;
40

(2) providing the workforce of the agency with a clear pathway to test and document new acquisition practices and facilitate fresh perspectives on existing practices;

(3) helping programs and integrated project teams successfully execute emerging and well-established acquisition practices to achieve better results; and

(4) promoting meaningful collaboration among offices that are responsible for requirements development, contracting officers, and others, including financial and legal experts, that share in the responsibility for making a successful procurement.

(e) STRUCTURE.—An agency should consider placing the Procurement Innovation Lab or similar mechanism as a supporting arm of the Chief Acquisition Officer or Senior Procurement Executive of the agency and shall have wide latitude in structuring the Procurement Innovation Lab or similar mechanism and in addressing associated personnel staffing issues.

SEC. 10. MULTI-PHASE COMMERCIAL TECHNOLOGY TEST PROGRAM.

(a) Test Program.—The head of an agency may, if desired, procure commercial technology through a multi-
phase test program of contracts in accordance with this section.

(b) PURPOSE.—A test program established under this section shall—

(1) provide a means by which an agency may post a solicitation, including for a general need or area of interest, for which the agency intends to explore commercial technology solutions and for which an offeror may submit a bid based on existing commercial capabilities of the offeror with minimal modifications or a technology that the offeror is developing for commercial purposes; and

(2) use phases, as described in subsection (c), to minimize government risk and incentivize competition.

(e) CONTRACTING PROCEDURES.—Under a test program established under this section, the head of an agency may acquire commercial technology through a competitive evaluation of proposals resulting from general solicitation in the following phases:

(1) PHASE 1 (VIABILITY OF POTENTIAL SOLUTION).—Selectees may be awarded a portion of the total contract award and have a period of performance of not longer than 1 year to prove the merits,
feasibility, and technological benefit the proposal would achieve for the agency.

(2) Phase 2 (Major Details and Scaled Test).—Selectees may be awarded a portion of the total contract award and have a period of performance of not longer than 1 year to create a detailed timeline, establish an agreeable intellectual property ownership agreement, and implement the proposal on a small scale.

(3) Phase 3 (Implementation or Recycle).—

(A) In General.—Following successful performance on phase 1 and 2, selectees may be awarded up to the full remainder of the total contract award to implement the proposal, depending on the agreed upon costs and the number of contractors selected.

(B) Failure to Find Suitable Selectees.—If no selectees are found suitable for phase 3, the agency head may determine not to make any selections for phase 3, terminate the solicitation and utilize any remaining funds to issue a modified general solicitation for the same area of interest.
(d) **TREATMENT AS COMPETITIVE PROCEDURES.**—

The use of general solicitation competitive procedures for a test program under this section shall be considered to be use of competitive procedures as defined in section 152 of title 41, United States Code.

(e) **LIMITATION.**—The head of an agency shall not enter into a contract under the test program for an amount in excess of $25,000,000.

(f) **GUIDANCE.**—

(1) **FEDERAL ACQUISITION REGULATORY COUNCIL.**—The Federal Acquisition Regulatory Council shall revise the Federal Acquisition Regulation as necessary to implement this section, including requirements for each general solicitation under a test program to be made publicly available through a means that provides access to the notice of the general solicitation through the System for Award Management or subsequent government-wide point of entry, with classified solicitations posted to the appropriate government portal.

(2) **AGENCY PROCEDURES.**—The head of an agency may not award contracts under a test program until the agency issues guidance with procedures for use of the authority. The guidance shall be
issued in consultation with the relevant Acquisition Regulatory Council and shall be publicly available.

(g) SUNSET.—The authority for a test program under this section shall terminate on the date that is 5 years after the date the Federal Acquisition Regulation is revised pursuant to subsection (f)(1) to implement the program.

SEC. 11. RESEARCH AND DEVELOPMENT PROJECT PILOT PROGRAM.

(a) PILOT PROGRAM.—The head of an agency may, if desired, carry out research and prototype projects in accordance with this section.

(b) PURPOSE.—A pilot program established under this section shall provide a means by which an agency may—

(1) carry out basic, applied, and advanced research and development projects; and

(2) carry out prototype projects that address—

(A) a proof of concept, model, or process, including a business process;

(B) reverse engineering to address obsolescence;

(C) a pilot or novel application of commercial technologies for agency mission purposes;

(D) agile development activity;
(E) the creation, design, development, or demonstration of operational utility; or
(F) any combination of items described in subparagraphs (A) through (E).

(c) CONTRACTING PROCEDURES.—Under a pilot program established under this section, the head of an agency may carry out research and prototype projects—

(1) using small businesses to the maximum extent practicable;

(2) using cost sharing arrangements where practicable;

(3) tailoring intellectual property terms and conditions relevant to the project and commercialization opportunities; and

(4) ensuring that such projects do not duplicate research being conducted under existing agency programs.

(d) TREATMENT AS COMPETITIVE PROCEDURES.—The use of research and development contracting procedures under this section shall be considered to be use of competitive procedures, as defined in section 152 of title 41, United States Code.

(e) TREATMENT AS COMMERCIAL TECHNOLOGY.—The use of research and development contracting proce-
dures under this section shall be considered to be use of commercial technology.

(f) Follow-on Projects or Phases.—A follow-on contract provided for in a contract opportunity announced under this section may, at the discretion of the head of the agency, be awarded to a participant in the original project or phase if the original project or phase was successfully completed.

(g) Limitation.—The head of an agency shall not enter into a contract under the pilot program for an amount in excess of $10,000,000.

(h) Guidance.—

(1) Federal Acquisition Regulatory Council.—The Federal Acquisition Regulatory Council shall revise the Federal Acquisition Regulation research and development contracting procedures as necessary to implement this section, including requirements for each research and development project under a pilot program to be made publicly available through a means that provides access to the notice of the opportunity through the System for Award Management or subsequent government-wide point of entry, with classified solicitations posted to the appropriate government portal.
(2) AGENCY PROCEDURES.—The head of an agency may not award contracts under a pilot program until the agency, in consultation with the relevant Acquisition Regulatory Council issues and makes publicly available guidance on procedures for use of the authority.

(i) REPORTING.—Contract actions entered into under this section shall be reported to the Federal Procurement Data System, or any successor system.

(j) SUNSET.—The authority for a pilot program under this section shall terminate on the date that is 5 years from the date the Federal Acquisition Regulation is revised pursuant to subsection (h)(1) to implement the program.

SEC. 12. DEVELOPMENT OF TOOLS AND GUIDANCE FOR TESTING AND EVALUATING ARTIFICIAL INTELLIGENCE.

(a) AGENCY REPORT REQUIREMENTS.—In a manner specified by the Director, the Chief Artificial Intelligence Officer shall identify and annually submit to the Council a report on obstacles encountered in the testing and evaluation of artificial intelligence, specifying—

(1) the nature of the obstacles;
(2) the impact of the obstacles on agency operations, mission achievement, and artificial intelligence adoption;

(3) recommendations for addressing the identified obstacles, including the need for particular resources or guidance to address certain obstacles; and

(4) a timeline that would be needed to implement proposed solutions.

(b) COUNCIL REVIEW AND COLLABORATION.—

(1) ANNUAL REVIEW.—Not less frequently than annually, the Council shall conduct a review of agency reports under subsection (a) to identify common challenges and opportunities for cross-agency collaboration.

(2) DEVELOPMENT OF TOOLS AND GUIDANCE.—

(A) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Director, in consultation with the Council, shall convene a working group to—

(i) develop tools and guidance to assist agencies in addressing the obstacles that agencies identify in the reports under subsection (a);
(ii) support interagency coordination to facilitate the identification and use of relevant voluntary standards, guidelines, and other consensus-based approaches for testing and evaluation and other relevant areas; and

(iii) address any additional matters determined appropriate by the Director.

(B) WORKING GROUP MEMBERSHIP.—The working group described in subparagraph (A) shall include Federal interdisciplinary personnel, such as technologists, information security and cybersecurity personnel, domain experts, privacy officers, data officers, civil rights and civil liberties officers, contracting officials, legal counsel, customer experience professionals, program evaluation officers, and others, as determined by the Director.

(3) INFORMATION SHARING.—The Director, in consultation with the Council, shall establish a mechanism for sharing tools and guidance developed under paragraph (2) across agencies.

(e) CONGRESSIONAL REPORTING.—
(1) IN GENERAL.—Each agency shall submit the annual report under subsection (a) to relevant congressional committees.

(2) CONSOLIDATED REPORT.—The Director, in consultation with the Council, may suspend the requirement under paragraph (1) and submit to the relevant congressional committees a consolidated report that conveys government-wide testing and evaluation challenges, recommended solutions, and progress toward implementing recommendations from prior reports developed in fulfillment of this subsection.

(d) EXTREMELY LOW RISK ARTIFICIAL INTELLIGENCE USE CASES.—Not later than 2 years after the date of enactment of this Act, the Chief Artificial Intelligence Officers Council shall submit to the Director and the relevant congressional committees a report outlining—

(1) a proposed framework for identifying extremely low risk artificial intelligence use cases; and

(2) opportunities to facilitate the deployment and use of extremely low risk artificial intelligence.

(e) SUNSET.—The requirements under this section shall terminate on the date that is 10 years after the date of enactment of this Act.
SEC. 13. UPDATES TO ARTIFICIAL INTELLIGENCE USE CASE INVENTORIES.

(a) Amendments.—

(1) ADVANCING AMERICAN AI ACT.—The Advancing American AI Act (Public Law 117–263; 40 U.S.C. 11301 note) is amended—

(A) in section 7223(3), by striking the period and inserting “and in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).”; and

(B) in section 7225, by striking subsection (d).

(2) EXECUTIVE ORDER 13960.—The provisions of section 5 of Executive Order 13960 (85 Fed. Reg. 78939; relating to promoting the use of trustworthy artificial intelligence in Federal Government) that exempt classified and sensitive use cases from agency inventories of artificial intelligence use cases shall cease to have legal effect.

(b) Disclosure.—

(1) IN GENERAL.—The artificial intelligence inventory of each agency shall publicly disclose, subject to applicable laws and policies relating to the protection of privacy and classified and sensitive information—
(A) whether artificial intelligence was developed internally by the agency or procured externally, without excluding any use case on basis that the use case is “sensitive” solely because it was externally procured;

(B) data provenance information for high risk artificial intelligence use cases to identify the types of sources of the training data of the artificial intelligence, including internal government data, public data, commercially held data, or similar data;

(C) the level of risk at which the agency has classified the artificial intelligence use case and a brief explanation for how the determination was made; and

(D) the number of artificial intelligence use cases excluded from public reporting as being classified or “sensitive”, and an unclassified summary of each of these use cases.

(2) UPDATES.—

(A) IN GENERAL.—When an agency updates the public artificial intelligence use case inventory of the agency, the agency shall disclose the date of the modification and make change logs publicly available and accessible.
(B) GUIDANCE.—The Director shall issue guidance to agencies that describes how to appropriately update artificial intelligence use case inventories and clarifies how sub-agencies and regulatory agencies should participate in the artificial intelligence use case inventorying process.

(c) CONGRESSIONAL REPORTING.—The head of each agency shall, upon request, submit to the relevant congressional committees a copy of the annual artificial intelligence use case inventory of the agency, including—

(1) the use cases that have been identified as “sensitive” and not for public disclosure; and

(2) a classified annex of classified use cases.

(d) COMPTROLLER GENERAL.—

(1) REPORTS REQUIRED.—

(A) APPROPRIATE CLASSIFICATION.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for a period of 5 years, the Comptroller General of the United States shall submit to relevant congressional committees a report on whether agencies are appropriately classifying use cases.

(B) GOVERNMENT TRENDS.—Beginning 2 years after the date of enactment of this Act,
and annually thereafter, the Comptroller General of the United States, shall issue a report, based on the artificial intelligence use cases reported in use case inventories and other relevant information, that describes trends in the use of artificial intelligence by agencies and the impact of—

(i) such use on the Federal workforce and any cost savings; and

(ii) this Act on Federal contractors that are small business concerns, including—

(I) small business concerns owned and controlled by service-disabled veterans (as defined in section 3 of the Small Business Act (15 U.S.C. 632));

(II) qualified HUBZone small business concerns (as defined in section 31(b) of the Small Business Act (15 U.S.C. 657(b)(1)));

(III) socially and economically disadvantaged small business concerns (as defined in section 8(a)(4) of the
Small Business Act (15 U.S.C. 637(a)(4)), and

(IV) small business concerns owned and controlled by women (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(2) APPROPRIATE CLASSIFICATION.—The Comptroller General of the United States shall determine whether the appropriate level of disclosure of artificial intelligence use cases by agencies should be included on the High Risk List of the Government Accountability Office.