118TH CONGRESS
2D SESSION

S. ______

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

IN THE SENATE OF THE UNITED STATES

Mr. PETERS (for himself and Mr. TILLIS) introduced the following bill; which was read twice and referred to the Committee on ____________________

A BILL

To enable safe, responsible, and agile procurement, development, and use of artificial intelligence by the Federal Government, 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 ‘‘Promoting Responsible Evaluation and Procurement to Advance Readiness for Enterprise-wide Deployment for Artificial Intelligence Act’’ or the ‘‘PREPARED for AI Act’’.

SEC. 2. DEFINITIONS.

In this Act:

(1) ADVERSE INCIDENT.—The term ‘‘adverse incident’’ means any incident or malfunction of artificial intelligence that directly or indirectly leads to—

(A) harm impacting rights or safety, as described in section 7(a)(2)(D);

(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)(2)(D)(i)(II)(cc);

(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 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) has the meaning given that term in section 3502(1) of title 44, United States Code; and

(B) includes 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 or provides artificial intelligence, whether developed internally or by a third-party developer.

(8) DEVELOPER.—The term ‘‘developer’’ means an entity that designs, codes, produces, or owns artificial intelligence.

(9) DIRECTOR.—The term ‘‘Director’’ means the Director of the Office of Management and Budget.

(10) IMPACT ASSESSMENT.—The term ‘‘impact assessment’’ means a structured process for considering the implications of a proposed artificial intelligence use case.

(11) OPERATIONAL DESIGN DOMAIN.—The term ‘‘operational design domain’’ means a set of operating conditions for an automated system.

(12) PROCURE OR OBTAIN.—The term ‘‘procure or obtain’’ means—

(A) to acquire through contract actions awarded pursuant to the Federal Acquisition Regulation, including through interagency agreements, multi-agency use, and purchase card transactions;

(B) to acquire through contracts and agreements awarded through other special procurement authorities, including through other transactions and commercial solutions opening authorities; or

(C) to obtain through other means, including through open source platforms or freeware.

(13) 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.

(14) RISK.—The term ''risk'' means the combination of the probability of an occurrence of harm and the potential severity of that harm.

(15) USE CASE.—The term ''use case'' means the ways and context in which artificial intelligence is operated to perform a specific function.

SEC. 3. IMPLEMENTATION OF REQUIREMENTS.

(a) AGENCY IMPLEMENTATION.—Not later than 1 year after the date of enactment of this Act, the Director shall ensure that agencies have implemented the requirements of this Act.

(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 1 year 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 to ensure that agency procurement of artificial intelligence includes—

(A) a requirement to address the outcomes of the risk evaluation and impact assessments required under section 8(a);

(B) a requirement for consultation with an interdisciplinary team of 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) INTERDISCIPLINARY TEAM OF EXPERTS.—The interdisciplinary team of experts 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 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.

(3) ACQUISITION PLANNING.—The acquisition planning updates described in paragraph (1) shall include considerations for, at minimum, as appropriate depending on the use case—

(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 techniques;

(G) type and scope of artificial intelligence audits;

(H) environmental impact; and

(I) safety and security risk mitigation techniques, including a plan for how adverse event reporting can be incorporated, pursuant to section 5(g).

(b) REQUIREMENTS FOR HIGH RISK USE CASES.—

(1) IN GENERAL.—

(A) 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)(2)(D), prior to establishing and incorporating certain terms into relevant contracts, agreements, and employee guidelines for artificial intelligence, including—

(i) a requirement that the use of the artificial intelligence be limited to its operational design domain;

(ii) requirements for safety, security, and trustworthiness, including—

(I) a reporting mechanism through which agency personnel are notified by the deployer of any adverse incident;

(II) a requirement, in accordance with section 5(g), that agency personnel receive from the deployer a notification of any adverse incident, an explanation of the cause of the adverse incident, and any data directly connected to the adverse incident in order to address and mitigate the harm; and

(III) that the agency has the right to temporarily or permanently suspend use of the artificial intelligence if—

(aa) the risks of the artificial intelligence to rights or safety become unacceptable, as determined under the agency risk classification system pursuant to section 7; or

(bb) on or after the date that is 180 days after the publication of 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(c)), the deployer is found not to comply with such most recent update;

(iii) requirements for quality, relevance, sourcing and ownership of data, as appropriate by use case, and applicable unless the head of the agency waives such requirements in writing, including—

(I) retention of rights to Government data and any modification to the data including to protect the 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 and any relevant developers or other parties isolate Government data from all other data, through physical separation, electronic separation via secure copies with strict access controls, or other computational isolation mechanisms;

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

(v) requirements that the deployer and any relevant developers provide documentation, as determined necessary and requested by the agency, in accordance with section 8(b).

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

(C) REGULATION.—The Federal Acquisition Regulatory Council shall revise the Federal Acquisition Regulation as necessary to implement the requirements of this subsection.

(2) RULES OF CONSTRUCTION.—This Act shall supersede any requirements that conflict with this Act under the guidance required to be produced by the Director pursuant to section 7224(d) of the Advancing American AI Act (40 U.S.C. 11301 note).

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; and

(3) assisting the Director, as necessary, with respect to—

(A) the identification, development, and coordination of multi-agency projects and other initiatives, including initiatives to improve Government performance;

(B) the 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 classification system that may incorporate best practices, such as those from—

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

(ii) 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;

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

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

(i) interagency councils;

(ii) Federal Government entities;

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

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

(v) other individuals and entities, as determined relevant by the Council.

(c) MEMBERSHIP OF THE COUNCIL.—

(1) CO-CHAIRS.—The Council shall have 2 co-chairs, which shall be—

(A) the Director; and

(B) an individual selected by a majority of the members 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 intelligence of the Office of Management and Budget.

(d) STANDING COMMITTEES; WORKING GROUPS.—The Council shall have the authority to establish standing committees, including an executive committee, and working 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) DEVELOPMENT, ADAPTATION, AND DOCUMENTATION.—

(1) GUIDANCE.—Not later than 90 days after the date of enactment of this Act, the Director, in

consultation with the Council, shall issue guidance relating to—

(A) developments in artificial intelligence and implications for management of agency programs;

(B) the agency impact assessments described in section 8(a) and other relevant impact assessments as determined appropriate by the Director, including the appropriateness of substituting pre-existing assessments, including privacy impact assessments, for purposes of an artificial intelligence impact assessment;

(C) documentation for agencies to require from deployers of artificial intelligence;

(D) a model template for the explanations for use case risk classifications that each agency must provide under section 8(a)(4); and

(E) other matters, as determined relevant by the Director.

(2) ANNUAL REVIEW.—The Director, in consultation with the Council, shall periodically, but not less frequently than annually, review and update, as needed, the guidelines issued under paragraph (1).

(g) INCIDENT REPORTING.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director, in consultation with the Council, shall develop procedures for ensuring that—

(A) adverse incidents involving artificial intelligence procured, obtained, or used by agencies are reported promptly to the agency by the developer or deployer, or to the developer or deployer by the agency, whichever first becomes aware of the adverse incident; and

(B) information relating to an adverse incident described in subparagraph (A) is appropriately shared among agencies.

(2) SINGLE REPORT.—Adverse incidents 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 DEPLOYER.—

(A) IN GENERAL.—If an adverse incident is discovered by an agency, the agency shall report the adverse incident to the deployer and the deployer, in consultation with any relevant developers, shall take immediate action to resolve the adverse incident and mitigate the potential for future adverse incidents.

(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 incident.

(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, or the designee of 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) articulating a clear vision of what the head of the agency wants to achieve by developing, procuring or obtaining, or using artificial intelligence;

(B) ensuring the agency develops, procures, obtains, or uses artificial intelligence that follows the principles of trustworthy artificial intelligence in government set forth under Executive Order 13960 (85 Fed. Reg. 78939; relating to promoting the use of trustworthy artificial intelligence in Federal Government) and the principles for safe, secure, and trustworthy artificial intelligence in government set forth under section 2 of Executive Order 14110 (88 Fed. Reg. 75191; relating to the safe, secure, and trustworthy development and use of artificial intelligence);

(C) testing, validating, and monitoring artificial intelligence and the use case-specific performance of artificial intelligence, among others, to—

(i) ensure all use of artificial intelligence is appropriate to and improves the effectiveness of the mission of the agency;

(ii) guard against bias in data collection, use, and dissemination;

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

(iv) protect against impermissible discrimination;

(D) developing, adopting, and applying a suitable enterprise risk management framework approach to artificial intelligence, incorporating the requirements under this Act;

(E) continuing to develop a workforce that—

(i) understands the strengths and weaknesses of artificial intelligence, including artificial intelligence embedded in agency data systems and operations;

(ii) is aware of the benefits and risk of artificial intelligence; and

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

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

(F) ensuring implementation of the requirements under section 8(a) for the identification and evaluation of risks posed by the deployment of artificial intelligence in agency use cases;

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

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

(3) form and convene an Artificial Intelligence Governance Board, as described in subsection (b), which shall coordinate and govern artificial intelligence issues across the agency.

(b) Artificial Intelligence Governance Board.—

(1) Leadership.—Each Artificial Intelligence Governance Board (referred to in this subsection as "Board") of an agency 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 comprised of senior agency officials from operational components, if relevant, program officials responsible for implementing artificial intelligence, and officials responsible for information technology, data, privacy, civil rights and civil liberties, human capital, procurement, finance, legal counsel, 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).

(c) 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.

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

SEC. 7. AGENCY RISK CLASSIFICATION OF ARTIFICIAL INTELLIGENCE USE CASES FOR PROCUREMENT AND USE.

(a) RISK CLASSIFICATION SYSTEM.—

(1) DEVELOPMENT.—The head of each agency shall be responsible for developing, not later than 1 year after the date of enactment of this Act, a risk classification system for agency use cases of artificial intelligence, without respect to whether artificial intelligence is embedded in a commercial product.

(2) REQUIREMENTS.—

(A) RISK CLASSIFICATIONS.—The risk classification system under paragraph (1) shall, at a minimum, include unacceptable, high, medium, and low risk classifications.

(B) FACTORS FOR RISK CLASSIFICATIONS.—In developing the risk classifications under subparagraph (A), the head of the agency shall consider the following:

(i) MISSION AND OPERATION.—The mission and operations of the agency.

(ii) SCALE.—The seriousness and probability of adverse impacts.

(iii) SCOPE.—The breadth of application, such as the number of individuals affected.

(iv) OPTIONALITY.—The degree of choice that an individual, group, or entity has as to whether to be subject to the effects of artificial intelligence.

(v) STANDARDS AND FRAMEWORKS.—Standards and frameworks for risk classification of use cases that support democratic values, such as the standards and frameworks developed by the National Institute of Standards and Technology, the

International Standards Organization, and the Institute of Electrical and Electronics Engineers.

(C) CLASSIFICATION VARIANCE.—

(i) CERTAIN LOWER RISK USE CASES.—The risk classification system may allow for an operational use case to be categorized under a lower risk classification, even if the use case is a part of a larger area of the mission of the agency that is categorized under a higher risk classification.

(ii) CHANGES BASED ON TESTING OR NEW INFORMATION.—The risk classification system may allow for changes to the risk classification of an artificial intelligence use case based on the results from procurement process testing or other information that becomes available.

(D) HIGH RISK USE CASES.—

(i) IN GENERAL.—High risk classification shall, at a minimum, apply to use cases for which the outputs of the system—

(I) are presumed to serve as a principal basis for a decision or action that has a legal, material, binding, or similarly significant effect, with respect to an individual or community, on—

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

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

(cc) access to or the ability to apply for critical government resources or services, including healthcare, financial services, public housing, social services, transportation, and essential goods and services; or

(II) are presumed to serve as a principal basis for a decision that substantially impacts the safety of, or has the potential to substantially impact the safety of—

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

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

(cc) critical infrastructure, including the critical infrastructure sectors defined in Presidential Policy Directive 21, entitled ''Critical Infrastructure Security and Resilience'' (dated February 12, 2013) (or any successor directive) and the infrastructure for voting and protecting the integrity of elections; or

(dd) strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government and controlled unclassified information.

(ii) ADDITIONS.—The head of each agency shall add other use cases to the high risk category, as appropriate.

(E) MEDIUM AND LOW RISK USE CASES.—If a use case is not high risk, as described in subparagraph (D), the head of an agency shall have the discretion to define the risk classification.

(F) UNACCEPTABLE RISK.—If an agency identifies, through testing, adverse incident, or other means or information available to the agency, that a use or outcome of an artificial intelligence use case is a clear threat to human safety or rights that cannot be adequately or practicably mitigated, the agency shall identify the risk classification of that use case as unacceptable risk.

(3) TRANSPARENCY.—The risk classification system under paragraph (1) shall be published on a public-facing website, with the methodology used to determine different risk levels and examples of par-

ticular use cases for each category in language that is easy to understand to the people affected by the decisions and outcomes of artificial intelligence.

(b) EFFECTIVE DATE.—This section shall take effect on the date that is 180 days after the date of enactment of this Act, on and after which an agency that has not complied with the requirements of this section may not develop, procure or obtain, or use artificial intelligence until the agency complies with such requirements.

SEC. 8. AGENCY REQUIREMENTS FOR USE OF ARTIFICIAL INTELLIGENCE.

(a) RISK EVALUATION PROCESS.—

(1) IN GENERAL.—Not later than 180 days after the effective date in section 7(b), the Chief Artificial Intelligence Officer of each agency, in coordination with the Artificial Intelligence Governance Board of the agency, shall develop and implement a process for the identification and evaluation of risks posed by the deployment of artificial intelligence in agency use cases to ensure an interdisciplinary and comprehensive evaluation of potential risks and determination of risk classifications under such section.

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

(A) identification of the risks and benefits of the artificial intelligence use case;

(B) a plan to periodically review the artificial intelligence use case to examine whether risks have changed or evolved and to update the corresponding risk classification as necessary;

(C) a determination of the need for targeted impact assessments to further evaluate specific risks of the artificial intelligence use case 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 section 7(a)(2)(D) as determined appropriate by the Chief Artificial Intelligence Officer; and

(D) if appropriate, consultation with and feedback from affected communities and the public on the design, development, and use of the artificial intelligence use case.

(3) REVIEW.—

(A) EXISTING USE CASES.—With respect to each use case that an agency is planning, developing, or using on the date of enactment of this Act, not later than 1 year after such date, the Chief Artificial Intelligence Officer of the agency shall identify and review the use case to determine the risk classification of the use case, pursuant to the risk evaluation process under paragraphs (1) and (2).

(B) NEW USE CASES.—

(i) IN GENERAL.—Beginning on the date of enactment of this Act, the Chief Artificial Intelligence Officer of an agency shall identify and review any artificial intelligence use case that the agency will plan, develop, or use and determine the risk classification of the use case, pursuant to the risk evaluation process under paragraphs (1) and (2), before procuring or obtaining, developing, or using the use case.

(ii) DEVELOPMENT.—For any use case described in clause (i) that is developed by the agency, the agency shall perform an additional risk evaluation prior to deployment in a production or operational environment.

(4) RATIONALE FOR RISK CLASSIFICATION.—Risk classification of an artificial intelligence use case shall be accompanied by an explanation from the agency of how the risk classification was determined, which shall be included in the artificial intelligence use case inventory of the agency, and written referencing the model template developed by the Director under section 5(f)(1)(D).

(b) MODEL CARD DOCUMENTATION REQUIREMENTS.—

(1) IN GENERAL.—Beginning on the date that is 180 days after the date of enactment of this Act, any time during developing, procuring or obtaining, or using artificial intelligence, an agency shall require, as determined necessary by the Chief Artificial Intelligence Officer, that the deployer and any relevant developer submit documentation about the artificial intelligence, including—

(A) a description of the architecture of the artificial intelligence, highlighting key parameters, design choices, and the machine learning techniques employed;

(B) information on the training of the artificial intelligence, including computational resources utilized;

(C) an account of the source of the data, size of the data, any licenses under which the data is used, collection methods and dates of the data, and any preprocessing of the data undertaken, including human or automated refinement, review, or feedback;

(D) information on the management and collection of personal data, outlining data protection and privacy measures adhered to in compliance with applicable laws;

(E) a description of the methodologies used to evaluate the performance of the artificial intelligence, including key metrics and outcomes; and

(F) an estimate of the energy consumed by the artificial intelligence during training and inference.

(2) ADDITIONAL DOCUMENTATION FOR MEDIUM AND HIGH RISK USE CASES.—Beginning on the date that is 270 days after the date of enactment of this Act, with respect to use cases categorized as medium risk or higher, an agency shall require that the

deployer of artificial intelligence, in consultation with any relevant developers, submit (including proactively, as material updates of the artificial intelligence occur) the following documentation:

(A) MODEL ARCHITECTURE.—Detailed information on the model or models used in the artificial intelligence, including model date, model version, model type, key parameters (including number of parameters), interpretability measures, and maintenance and updating policies.

(B) ADVANCED TRAINING DETAILS.—A detailed description of training algorithms, methodologies, optimization techniques, computational resources, and the environmental impact of the training process.

(C) DATA PROVENANCE AND INTEGRITY.—A detailed description of the training and testing data, including the origins, collection methods, preprocessing steps, and demographic distribution of the data, and known discriminatory impacts and mitigation measures with respect to the data.

(D) PRIVACY AND DATA PROTECTION.—Detailed information on data handling practices, including compliance with legal standards, anonymization techniques, data security measures, and whether and how permission for use of data is obtained.

(E) RIGOROUS TESTING AND OVERSIGHT.—A comprehensive disclosure of performance evaluation metrics, including accuracy, precision, recall, and fairness metrics, and test dataset results.

(F) NIST ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK.—Documentation demonstrating compliance with the most recently updated version of the framework developed and updated pursuant to section 22A(c) of the National Institute of Standards and Technology Act (15 U.S.C. 278h–1(c)).

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

(A) examine whether agencies and deployers are complying with the requirements under those paragraphs; and

(B) make findings and recommendations to further assist in ensuring safe, responsible, and efficient artificial intelligence.

(4) 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)(3) is exempt from disclosure under section 552 of title 5, United States Code (commonly known as the ''Freedom of Information Act'') and 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 section 7(a)(2)(D);

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

(C) security vulnerabilities.

(d) PRE-DEPLOYMENT REQUIREMENTS FOR HIGH RISK USE CASES.—Beginning on the date that is 1 year 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) collecting documentation of the artificial intelligence, source, and use case in agency software and use case inventories;

(2) testing of the artificial intelligence in an operational, real-world setting with privacy, civil rights, and civil liberty safeguards to ensure the artificial intelligence is capable of meeting its objectives;

(3) establishing appropriate agency rules of behavior for the use case, including required human involvement in, and user-facing explainability of, 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; and

(4) 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 the operation of artificial intelligence in high risk use cases to detect and address anomalies, dysfunctions, and unexpected performance in a timely manner to mitigate harm;

(B) lessening reliance or 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;

(F) limiting the use of artificial intelligence to its operational design domain; and

(G) procedures for reporting incidents involving misuse, faulty results, safety and security issues, and other problems with use of artificial intelligence that does not function as intended.

(e) ONGOING MONITORING OF ARTIFICIAL INTELLIGENCE IN HIGH RISK USE CASES.—The Chief Artificial Intelligence Officer of each agency shall—

(1) establish a reporting system, consistent with section 5(g), and suspension and shut-down protocols for defects or adverse impacts 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;

(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; and

(4) adhere to pre-deployment requirements under subsection (d) in each case in which a low or medium risk artificial intelligence use case becomes a high risk artificial intelligence use case.

(f) Exemption From Requirements for Select Use Cases.—The Chief Artificial Intelligence Officer of each agency—

(1) may designate select, low risk use cases, including current and future use cases, that do not have to comply with all or some of the requirements in this Act; and

(2) shall publicly disclose all use cases exempted under paragraph (1) with a justification for each exempted use case.

(g) 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.

(h) Waivers.—

(1) In general.—The head of an agency, on a case by case basis, 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 with respect to the specific use case, that fulfilling the requirement or requirements prior to procuring or obtain-

ing, developing, or using artificial intelligence would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations.

(2) REQUIREMENTS; LIMITATIONS.—A waiver under this subsection shall be—

(A) in the national security interests of the United States, as determined by the head of the agency;

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

(C) limited to a duration of 1 year, at which time the head of the agency may renew the waiver and submit the renewed waiver to the relevant congressional committees.

(i) INFRASTRUCTURE SECURITY.—The head of an agency, in consultation with the agency Chief Artificial 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.

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

SEC. 9. PROHIBITION ON SELECT ARTIFICIAL INTELLIGENCE USE CASES.

No agency may develop, procure or 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;

(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; or

(4) any other use found by the agency to pose an unacceptable risk under the risk classification system of the agency, pursuant to section 7.

SEC. 10. AGENCY PROCUREMENT INNOVATION LABS.

(a) IN GENERAL.—An agency subject to the Chief Financial Officers Act of 1990 (31 U.S.C. 901 note; Public Law 101–576) 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;

(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.

(c) 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. 11. MULTI-PHASE COMMERCIAL TECHNOLOGY TEST PROGRAM.

(a) TEST PROGRAM.—The head of an agency may 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.

(c) 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. 12. RESEARCH AND DEVELOPMENT PROJECT PILOT PROGRAM.

(a) PILOT PROGRAM.—The head of an agency may 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 procedures under this section shall be considered to be use of commercial technology, as defined in section 2.

(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. 13. 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 personnel, domain experts, privacy officers, data officers, civil rights and civil liberties officers, contracting officials, legal counsel, customer experience professionals, 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.

(c) 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) SUNSET.—The requirements under this section shall terminate on the date that is 10 years after the date of enactment of this Act.

SEC. 14. 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) COMPLIANCE.—

(1) IN GENERAL.—The Director shall ensure that agencies submit artificial intelligence use case inventories and that the inventories comply with applicable artificial intelligence inventory guidance.

(2) ANNUAL REPORT.—The Director shall submit to the relevant congressional committees an annual report on agency compliance with artificial intelligence inventory guidance.

(c) DISCLOSURE.—

(1) IN GENERAL.—The artificial intelligence inventory of each agency shall publicly disclose—

(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, including identifying the source 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;

(D) a list of targeted impact assessments conducted pursuant to section 7(a)(2)(C); and

(E) the number of artificial intelligence use cases excluded from public reporting as being ''sensitive.''

(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.

(d) CONGRESSIONAL REPORTING.—The head of each agency shall 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.

(e) GOVERNMENT TRENDS REPORT.—Beginning 1 year after the date of enactment of this Act, and annually thereafter, the Director, in coordination with the Council, shall issue a report, based on the artificial intelligence use cases reported in use case inventories, that describes trends in the use of artificial intelligence in the Federal Government.

(f) COMPTROLLER GENERAL.—

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

(2) APPROPRIATE CLASSIFICATION.—The Comptroller General of the United States shall examine 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.