AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 9363

OFFERED BY M__. _____

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''AI Security and Innovation Act''.

SEC. 2. ARTIFICIAL INTELLIGENCE ADVANCEMENT AND RELIABILITY.

(a) IN GENERAL.—The National Artificial Intelligence Initiative Act of 2020 (enacted as division E of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021; Public Law 116–283) is amended—

(1) in section 5002 (15 U.S.C. 9401)—

(A) in paragraph (3)—

(i) in the heading, by striking ''ARTIFICIAL'' and inserting ''AI; ARTIFICIAL'';

(ii) by striking ''term 'artificial intelligence' means'' and inserting ''terms 'AI' and 'artificial intelligence' mean''; and

(iii) by adding at the end the following new paragraphs:

''(4) ARTIFICIAL INTELLIGENCE MODEL.—The term 'artificial intelligence model' means a component of an artificial intelligence system that is—

''(A) derived using mathematical, computational, statistical, or machine-learning techniques; and

''(B) used as part of an artificial intelligence system to produce outputs or behaviors from a defined set of inputs.

''(5) ARTIFICIAL INTELLIGENCE SYSTEM.—The term 'artificial intelligence system' means a data system, software, application, hardware, tool, service, or utility that operates in whole or in part using artificial intelligence.'';

(B) by redesignating paragraphs (4), (5), (6), (7), (8), (9), (10), and (11) as paragraphs (6), (8), (9), (10), (11), (13), (14), and (15), respectively;

(C) by inserting after paragraph (6), as so redesignated, the following new paragraphs:

''(7) FOREIGN ADVERSARY.—The term 'foreign adversary' has the meaning given the term 'covered

nation' in section 4872(f)(2) of title 10, United States Code.''; and

(D) by inserting after paragraph (11), as so redesignated, the following new paragraph:

''(12) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).''; and

(2) in title LIII (15 U.S.C. 9441 et seq.), by adding at the end the following new section:

''SEC. 5304. CENTER FOR AI SECURITY AND INNOVATION.

''(a) ESTABLISHMENT.—

''(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this section, the Secretary of Commerce, acting through the Under Secretary of Commerce for Standards and Innovation (in this section referred to as the 'Secretary' and 'Under Secretary', respectively), shall establish in the National Institute of Standards and Technology a center on artificial intelligence, to be known as the 'Center for AI Security and Innovation' (in this section referred to as the 'Center').

''(2) ACTIVITIES.—The Center shall carry out the following:

''(A) Measure risks related to artificial intelligence systems, including national security risks and economic security risks.

''(B) Support the exchange of information between non-governmental entities and Federal departments and agencies to facilitate mitigation related to any such risks.

''(C) Support activities to ensure continued leadership in the United States with respect to research, development, and evaluation of artificial intelligence systems.

''(3) TRANSFER STUDY.—

''(A) IN GENERAL.—The Secretary may conduct a study, as the Secretary determines appropriate, that includes the following:

''(i) An assessment of the feasibility, and the advantages and disadvantages, of transferring the Center to an agency of the Department of Commerce, or establishing the Center as an agency of the Department.

''(ii) Recommendations for Congress related to the following:

''(I) Any additional authority the Center should have or any other change to the authority of the Center.

''(II) Amounts of funding for the Center.

''(B) CONGRESSIONAL REVIEW.—If the Secretary conducts the study under subparagraph (A), the Secretary shall, not later than 30 days after so conducting such study, submit to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate such study for review.

''(b) DIRECTOR.—

''(1) IN GENERAL.—Not later than 3 months after the date of the enactment of this section, the Secretary, acting through the Under Secretary, shall appoint a director for the Center (referred to in this section as the 'Director').

''(2) EXPERIENCE.—The Secretary, acting through the Under Secretary, shall ensure the Director has the experience and is qualified to provide advice and leadership to carry out the duties under subsection (c).

''(c) DUTIES.—

''(1) IN GENERAL.—The Director shall carry out the following:

''(A) Evaluate and improve security measures with respect to covered artificial intelligence systems and seek to reduce any risk of misuse of such systems, including the evaluation and improvement of security measures that address threats relating to the following:

''(i) Model serialization attacks.

''(ii) Model tampering.

''(iii) Data leakage.

''(iv) Adversarial prompt injection.

''(v) Model extraction.

''(vi) Model jailbreaks.

''(vii) Supply chain attacks.

''(B) Establish a process for a covered entity that is not located in a foreign adversary to enter into a voluntary agreement with the Director to conduct classified or unclassified evaluations, as appropriate, of covered artificial intelligence systems regarding risks that such systems may pose to national security or economic security, including risks related to cybersecurity or chemical, biological, radiological, or nuclear threats.

''(C) Conduct evaluations and assessments with respect to the following:

''(i) Covered artificial intelligence systems developed by covered entities located in the following:

''(I) The United States.

''(II) A foreign adversary.

''(ii) Any potential security vulnerability, flaw, or malign foreign activity that results from artificial intelligence systems.

''(iii) Any relevant artificial intelligence system, as determined by the Director.

''(D) Support the laboratories of the National Institute of Standards and Technology in the development and voluntary adoption of standards, guidelines, and best practices relating to the following:

''(i) The testing and evaluation of covered artificial intelligence systems.

''(ii) Measuring and improving the security and reliability of artificial intelligence systems, including in areas such as robustness, interpretability of artificial in-

telligence, security relating to data centers and hardware security mechanisms.

''(iii) Any other matter relating to a covered artificial intelligence system, as determined appropriate by the Director.

''(E) Assess the following:

''(i) Whether covered entities are voluntarily adopting any such standards, guidelines, or best practices.

''(ii) Any barrier to such voluntary adoption.

''(F) Assess trends with respect to the development of artificial intelligence in the United States and in foreign adversaries, including through comparative assessments of how the capabilities of artificial intelligence systems in the U.S. and foreign adversaries differ with respect to key artificial intelligence capabilities milestones, as determined by the Director.

''(G) Any other action the Director determines necessary to carry out the activities of the Center under subsection (a)(2).

''(2) INTERAGENCY CONSULTATION.—In carrying out paragraph (1), the Director shall consult with the following:

''(A) The Director of the Office of Science and Technology Policy.

''(B) The Secretary of Energy.

''(C) The Secretary of Defense.

''(D) The Secretary of Homeland Security.

''(E) Members of the intelligence community.

''(F) The heads of any other relevant Federal departments or agencies as the Director determines appropriate.

''(3) CONSULTATION WITH NON-FEDERAL STAKEHOLDERS.—In carrying out paragraph (1), the Director shall seek to consult with private sector entities as the Director determines appropriate, including the following:

''(A) Small business concerns.

''(B) Members of academia.

''(C) Nonprofit organizations.

''(4) INTERAGENCY PARTICIPATION.—The Director shall be included in any interagency process convened by the Executive Office of the President relating to artificial intelligence policy, and may submit assessments and recommendations directly to the National Security Council and the Office of

Science and Technology Policy on matters within the scope of the duties described in paragraph (1).

''(5) DEFINING COVERED ARTIFICIAL INTELLIGENCE SYSTEM.—

''(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Under Secretary, acting through the Director, in coordination with the Director of the Office of Science and Technology Policy, the Director of National Intelligence, the Director of the Cybersecurity and Infrastructure Security Agency, and the heads of any other agency as the Director determines appropriate, shall publish, and update as the Director determines appropriate, a definition of the term 'covered artificial intelligence system' that identifies the characteristics and capabilities of artificial intelligence systems with national or economic security implications.

''(B) ACTIVITIES.—In carrying out subparagraph (A), the Under Secretary, acting through the Director, in consultation with relevant non-governmental entities (including developers of artificial intelligence), shall carry out a program of measurement research to un-

derstand and benchmark the capabilities and limitations of artificial intelligence systems over time.

''(6) OPTIONAL PUBLICATION.—The Director may make any evaluation or assessment conducted under paragraph (1)(C) publicly available, as the Director determines appropriate.

''(d) CRITICAL TECHNICAL EXPERTS.—

''(1) IN GENERAL.—The Secretary may appoint officers and employees for the Center as the Secretary determines necessary.

''(2) HIRING CRITICAL TECHNICAL EXPERTS.—Notwithstanding section 3104 of title 5, United States Code, or the provisions of any other law relating to the appointment, number, classification, or compensation of employees, the Secretary shall have the authority to make appointments of scientific, engineering, and professional personnel, and to fix the basic pay of such personnel at a rate to be determined by the Secretary at rates not in excess of the highest total annual compensation payable at the rate determined under section 104 of title 3, United States Code. The Secretary shall appoint not more than 15 personnel under this subsection.

''(e) CONFIDENTIALITY OF RECORDS; LIMITATION.—Any information shared with or provided to the Director by a covered entity to carry out subsection (c)—

''(1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

''(2) may not—

''(A) be made public unless such covered entity provides the Director consent for such information to be disclosed to the public; and

''(B) be used by any Federal, State, local, or Tribal government to regulate an activity of such covered entity related to such information.

''(f) REQUIREMENTS.—

''(1) AVOIDING DUPLICATION.—In carrying out this section, the Director shall take such actions as may be necessary to ensure no unnecessary duplication with activities carried out pursuant to section 22A of the National Institute of Standards and Technology Act (15 U.S.C. 278h–1).

''(2) INTEGRITY.—The Director shall ensure any publication of the Center, including a publication relating to an evaluation conducted under subsection (c)(1), is published in accordance with any internal review processes and procedures relating to publications by the laboratories of the National In-

stitute of Standards and Technology, as determined practicable and appropriate by the Director.

''(g) PROHIBITION ON REGULATIONS.—This section does not confer upon the Director any regulatory, rulemaking, or enforcement authority.

''(h) INTERNATIONAL ENGAGEMENT.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the Director may share information, collaborate, and participate in talent exchanges with a center or institute similar to the Center that is located in another country.

''(2) EXCEPTION.—Paragraph (1) does not apply with respect to a center or institute similar to the Center that is located in a foreign adversary.

''(i) REPORT.—For each fiscal year beginning with fiscal year 2027, not later than 90 days after the President submits a budget for such fiscal year pursuant to section 1105 of title 31, United States Code, the Secretary shall submit to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report that includes the following:

''(1) The budget of the Center for such fiscal year.

''(2) Information relating to the consultation required by subsection (c)(2).

''(3) A description of any goals, priorities, and metrics for guiding and evaluating any activities of the Center under subsection (a)(2).

''(4) An assessment of the following:

''(A) The state of international competition relating to artificial intelligence, including a comparison between the capabilities of artificial intelligence systems developed by entities in the United States and foreign adversaries.

''(B) Any talent or personnel gaps affecting the ability of the Director to carry out subsection (c), and any recommendations relating to the recruitment and retention of personnel, including through temporary rotational assignments of personnel from other Federal departments or agencies or non-governmental entities, fellowship programs, or any other means of utilizing specialized technical expertise from non-governmental entities.

''(C) Any new or emerging capabilities that may impact the national or economic security of the United States that artificial intelligence systems currently possess or that the Director ex-

pects such systems to plausibly possess in the upcoming years, with a focus on any such capabilities that are most critical or relevant for the national security of the United States.

''(j) AUTHORIZATION OF APPROPRIATIONS.—There is to be authorized to be appropriated to the Secretary to carry out this section $20,000,000 for each of fiscal years 2027 through 2032.

''(k) SUNSET.—This section shall terminate on the date that is 5 years after the date of the enactment of this section.

''(l) DEFINITIONS.—In this section:

''(1) COVERED ARTIFICIAL INTELLIGENCE SYSTEM.—The term 'covered artificial intelligence system' has the meaning determined by the Director pursuant to subsection (c)(5).

''(2) COVERED ENTITY.—The term 'covered entity' means an entity or consortium of entities with a demonstrated ability to develop or evaluate a covered artificial intelligence system.

''(3) NONPROFIT ORGANIZATION.—The term 'nonprofit organization' means an organization that is described in section 501(c)(3) of the Internal Revenue Code of 1986 (26 U.S.C. 501(c)(3)).

''(4) SMALL BUSINESS CONCERN.—The term 'small business concern' has the meaning given such term under section 3 of the Small Business Act (15 U.S.C. 632).''.

(b) CLERICAL AMENDMENT.—The tables of contents in section 2(b) and title LIII of division E of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 are amended by inserting after the items relating to section 5303 the following new item:

''''Sec. 5304. Center for AI Standards and Innovation.''.