S. 3162 Lujan-Thune_substitute

Ben Ray Luján

AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

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

S. 3162

To improve the requirement for the Director of the National Institute of Standards and Technology to establish testbeds to support the development and testing of trustworthy artificial intelligence systems and to improve interagency coordination in development of such testbeds, 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. LUJÁN (for himself and Mr. Thune)

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Testing and Evaluation Systems for Trusted Artificial Intelligence Act of 2024'' or the ''TEST AI Act of 2024''.

SEC. 2. PILOT PROGRAM ON ESTABLISHING TESTBEDS TO SUPPORT DEVELOPMENT, RED-TEAMING, AND BLUE-TEAMING OF ARTIFICIAL INTELLIGENCE SYSTEMS.

(a) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE BLUE-TEAMING.—The term ''artificial intelligence blue-teaming'' means an effort to conduct operational vulnerability evaluations and provide mitigation techniques to entities who have a need for an independent technical review of the security posture of an artificial intelligence system.

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

(3) ARTIFICIAL INTELLIGENCE RED-TEAMING.—The term ''artificial intelligence red-teaming'' means structured adversarial testing efforts of an artificial intelligence system.

(4) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term in subsection (e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(5) NATIONAL SECURITY.—The term ''national security'' means—

(A) the protection of the United States from foreign aggression; and

(B) does not otherwise include the protection of the general welfare of the United States.

(6) TESTBED.—The term ''testbed'' means a facility or mechanism equipped for conducting rigorous and replicable testing of tools and technologies to help evaluate the functionality, performance, and security of those tools or technologies.

(b) PILOT PROGRAM REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology and the Secretary of Energy shall, in coordination with the head of the interagency committee established under section 5103(a) of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9413(a)), private sector entities, and institutions of higher education as the Director and Secretary of Energy consider appropriate, jointly carry out a pilot program to assess the feasibility and advisability of establishing testbeds, including virtual and experimental environments, to support the development, red-teaming and blue-teaming of artificial intelligence systems.

(c) TESTBEDS.—In carrying out the pilot program required by subsection (b), the Director and the Secretary shall jointly establish one or more testbeds for the purposes described in subsection (b), including testbeds that support development of artificial intelligence standards for identifying, evaluating, and mitigating cyber, data, and network vulnerabilities that if exploited would create substantial risks to critical infrastructure or national security.

(d) PRIMARY FOCUS.—The primary focus of the pilot program required by subsection (b) shall be artificial intelligence systems used by Federal agencies or that are under evaluation for future use by Federal agencies.

(e) MEMORANDUM OF UNDERSTANDING.—

(1) IN GENERAL.—The Secretary of Commerce and the Secretary of Energy shall enter into a memorandum of understanding to implement the coordination between the Secretary of Energy and the Director required by subsection (b).

(2) REQUIREMENTS.—The memorandum of understanding entered into under paragraph (1) shall be sufficient to ensure the National Institute of Standards and Technology has such access as may be necessary to the resources, personnel, and facilities at the Department of Energy, including the cross-cutting research and development programs—

(A) to employ testing and evaluation resources to support Federal agency adoption and use of artificial intelligence systems by improving the reliability, functionality, performance, and security of artificial intelligence systems used by the Federal agencies;

(B) to establish testbeds, including a classified testbed as necessary, to support the testing, evaluation and development of artificial intelligence systems to identify, evaluate, and mitigate cybersecurity, data, and network vulnerabilities that if exploited would create substantial risks to critical infrastructure or national security, such as weapons of mass destruction proliferation; and

(C) to support the development of testing and evaluation standards, tools, and technologies inclusive of standards, tools, and technologies for artificial intelligence red-teaming and artificial intelligence blue-teaming, for such purposes.

(f) METRICS.—Not later than 1 year after the commencement of the pilot program required by subsection (b), the Director and the Secretary of Energy shall jointly develop metrics to assess the effectiveness of the pilot pro-

gram in achieving the requirements set forth under subsection (e)(2).

(g) EVALUATION.—Not later than 3 years after the commencement of the pilot program required by subsection (b) and not less frequently than once each year thereafter for the duration of the pilot program, the Director and the Secretary shall jointly—

(1) evaluate the success of the pilot program, using the metrics developed pursuant to subsection (f); and

(2) submit to Congress the findings of the Director and the Secretary with respect to the evaluation carried out pursuant to paragraph (1).

(h) SUNSET.—The pilot program required by subsection (b) and the memorandum of understanding entered into under subsection (e) shall both terminate on the date that is 7 years after the date of the enactment of this Act.

(i) RESEARCH SECURITY.—The activities authorized under this section shall be carried out in a accordance with the provisions of subtitle D of title VI of the Research and Development, Competition, and Innovation Act (42 U.S.C. 19231 et seq.; enacted as part of division B of Public Law 117–167).

(j) CONFORMING REPEAL.—Section 22A of the National Institute of Standards and Technology Act (15 U.S.C. 278h–1) is amended—

(1) by striking subsection (g); and

(2) by redesignating subsection (h) as subsection (g).