Calendar No. 722

118TH CONGRESS
2D SESSION

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.

IN THE SENATE OF THE UNITED STATES

OCTOBER 30, 2023

Mr. LUJÁN (for himself, Mr. DURBIN, Mr. THUNE, Mrs. BLACKBURN, Mr. RISCH, and Mr. WELCH) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

DECEMBER 17 (legislative day, DECEMBER 16), 2024

Reported by Ms. CANTWELL, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

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.

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 ''Testing and Evaluation Systems for Trusted Artificial Intelligence Act of 2023'' or the ''TEST AI Act of 2023''.

SEC. 2. INTERAGENCY COORDINATION TO FACILITATE TESTBEDS.

Subsection (g) of section 22A of the National Institute of Standards and Technology Act (15 U.S.C. 278h–1) is amended to read as follows:

''(g) TESTBEDS.—

''(1) DEFINITION OF ARTIFICIAL INTELLIGENCE.—In this subsection, the term 'artificial intelligence' has the meaning given such term in section 5002 of the National Artificial Intelligence Act of 2020 (15 U.S.C. 9401).

''(2) IN GENERAL.— The Director shall, in coordination with the Secretary of Energy, 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)), and such heads of such Federal agencies, private sector entities, and institutions of higher education as the head of such interagency committee considers appropriate,

establish testbeds, including virtual and experimental environments, to support the development and testing of trustworthy artificial intelligence systems, including testbeds that support development of artificial intelligence guardrails, examine risks of misuse of such systems, and evaluate the vulnerabilities and conditions that may lead to failure in, malfunction of, or attacks on such systems.

"(3) MEMORANDUM OF UNDERSTANDING.—

"(A) 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 paragraph (2).

"(B) REQUIREMENTS.—The memorandum shall be sufficient to ensure the Institute and other Federal agencies have access as may be necessary to the resources, personnel, and facilities at the Department of Energy, including the cross-cutting research and development programs—

"(i) to advance artificial intelligence tools, systems, facilities, capabilities, and workforce needs;

~~"(ii) to improve the reliability and trustworthiness of artificial intelligence methods and solutions relevant to the mission of the Federal agencies conducting development or testing of artificial intelligence systems for use by the agency, or in conducting Federal oversight of commercial uses of artificial intelligence systems; and~~

~~"(iii) to establish testbeds, including a classified testbed as necessary, to support safeguards and systems to prevent the misuse of artificial intelligence systems, particularly in but not limited to weapons of mass destruction proliferation, undertake annual risk assessments of artificial intelligence misuse, formulate evaluation strategies, and employ testing and evaluation resources to support Federal oversight of artificial intelligence systems.".~~

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 program

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.—

(1) DEFINITIONS.—In this subsection:

(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(i) the congressional intelligence committees (as defined in section 3 of the Na-

tional Security Act of 1947 (50 U.S.C. 3003));

(ii) the Committee on Armed Services, the Committee on Energy and Natural Resources, the Committee on Foreign Relations, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on Appropriations of the Senate; and

(iii) the Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Foreign Affairs, the Committee on the Judiciary, the Committee on Homeland Security, the Committee on Space, Science, and Technology, and the Committee on Appropriations of the House of Representatives.

(B) COUNTRY OF RISK.—The term "country of risk" means a country identified in the report submitted to Congress by the Director of National Intelligence in 2024 pursuant to section 108B of the National Security Act of 1947 (50

U.S.C. 3043b) (commonly referred to as the "Annual Threat Assessment").

(C) COVERED ASSIGNEE; COVERED VISITOR.—The terms "covered assignee" and "covered visitor" mean a foreign national from a country of risk that is "engaging in competitive behavior that directly threatens U.S. national security", who is not an employee of either the Department of Energy or the management and operations contractor operating a National Laboratory on behalf of the Department of Energy, and has requested access to the premises, information, or technology of a National Laboratory.

(D) DIRECTOR.—The term "Director" means the Director of the Office of Intelligence and Counterintelligence of the Department of Energy (or their designee).

(E) FOREIGN NATIONAL.—The term "foreign national" has the meaning given the term "alien" in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

(F) NATIONAL LABORATORY.—The term "National Laboratory" has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(G) NONTRADITIONAL COLLECTION THREAT.—The term "nontraditional collection threat" means a threat posed by an individual not employed by a foreign intelligence service, who is seeking access to information about a capability, research, or organizational dynamics of the United States to inform a foreign adversary or non-state actor.

(2) SENSE OF THE SENATE.—It is the sense of the Senate that—

(A) before being granted access to the premises, information, or technology of a National Laboratory, citizens of foreign countries identified in the 2024 Annual Threat Assessment of the intelligence community as "engaging in competitive behavior that directly threatens U.S. national security" should be appropriately screened by the National Laboratory to which they seek access, and by the Office of intelligence and Counterintelligence of the Department, to identify risks associated with granting the requested access to sensitive military, or dual-use technologies; and

(B) identified risks should be mitigated.

(3) REVIEW OF COUNTRY OF RISK COVERED VISITOR AND COVERED ASSIGNEE ACCESS REQUESTS.—The Director shall, in consultation with the applicable Under Secretary of the Department of Energy that oversees the National Laboratory, or their designee, promulgate a policy to assess the counterintelligence risk that covered visitors or covered assignees pose to the research or activities undertaken at a National Laboratory.

(4) ADVICE WITH RESPECT TO COVERED VISITORS OR COVERED ASSIGNEES.—

(A) IN GENERAL.—The Director shall provide advice to a National Laboratory on covered visitors and covered assignees when 1 or more of the following conditions are present:

(i) The Director has reason to believe that a covered visitor or covered assignee is a nontraditional intelligence collection threat.

(ii) The Director is in receipt of information indicating that a covered visitor or covered assignee constitutes a counterintelligence risk to a National Laboratory.

(B) ADVICE DESCRIBED.—Advice provided to a National Laboratory in accordance with

paragraph (1) shall include a description of the assessed risk.

(C) RISK MITIGATION.—When appropriate, the Director shall, in consultation with the applicable Under Secretary of the Department of Energy that oversees the National Laboratory, or their designee, provide recommendations to mitigate the risk as part of the advice provided in accordance with paragraph (1).

(5) REPORTS TO CONGRESS.—Not later than 90 days after the date of the enactment of this Act, and quarterly thereafter, the Secretary of Energy shall submit to the appropriate congressional committees a report, which shall include—

(A) the number of covered visitors or covered assignees permitted to access the premises, information, or technology of each National Laboratory;

(B) the number of instances in which the Director provided advice to a National Laboratory in accordance with subsection (e); and

(C) the number of instances in which a National Laboratory took action inconsistent with advice provided by the Director in accordance with subsection (e).

(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).

Calendar No. 722

118TH CONGRESS
2D SESSION

S. 3162

A BILL

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.

DECEMBER 17 (legislative day, DECEMBER 16), 2024

Reported with an amendment