I

118TH CONGRESS
2D SESSION

H. R. 9720

To direct the Director of the National Institute of Standards and Technology to update the national vulnerability database to reflect vulnerabilities to artificial intelligence systems, study the need for voluntary reporting related to artificial intelligence security and safety incidents, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 20, 2024

Ms. ROSS (for herself, Mr. OBERNOLTE, and Mr. BEYER) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

---

A BILL

To direct the Director of the National Institute of Standards and Technology to update the national vulnerability database to reflect vulnerabilities to artificial intelligence systems, study the need for voluntary reporting related to artificial intelligence security and safety incidents, 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 ‘‘AI Incident Reporting and Security Enhancement Act’’.

SEC. 2. ACTIVITIES TO SUPPORT VOLUNTARY VULNERABILITY AND INCIDENT TRACKING ASSOCIATED WITH ARTIFICIAL INTELLIGENCE.

(a) UPDATE TO NATIONAL VULNERABILITY DATABASE.—Subject to the availability of appropriations, the Director of the National Institute of Standards and Technology, in coordination with industry stakeholders, standards development organizations, and appropriate Federal agencies, as appropriate, shall carry out the following:

(1) Establish or identify common definitions and any characteristics of artificial intelligence security vulnerabilities that make utilization of the National Vulnerability Database inappropriate for the management of such vulnerabilities, and develop processes and procedures for vulnerability management of such vulnerabilities.

(2) Support the development of standards and guidance for technical vulnerability management processes related to artificial intelligence.

(3) Consistent with paragraphs (1) and (2), as appropriate, initiate a process to update the Institute's processes and procedures associated with the National Vulnerability Database to ensure such Database and associated vulnerability management processes incorporate artificial intelligence security vulnerabilities to the greatest extent practicable.

(b) Assessing Voluntary Tracking of Substantial Artificial Intelligence Security and Safety Incidents.—

(1) In general.—Subject to the availability of appropriations, the Director of the National Institute of Standards and Technology, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall convene a multi-stakeholder process to consider the development of a process relating to the voluntary collection, reporting, and tracking of substantial artificial intelligence security incidents and substantial artificial intelligence safety incidents.

(2) Activities.—In carrying out paragraph (1), the Director of the National Institute of Standards and Technology shall convene appropriate representatives of industry, academia, nonprofit organizations, standards development organizations, civil society groups, Sector Risk Management Agencies, and appropriate Federal departments and agencies to carry out the following:

(A) Establish common definitions and characterizations for relevant aspects of substantial artificial intelligence security incidents and substantial artificial intelligence safety incidents, which may include the following:

(i) Classifications that sufficiently differentiate between the following:

(I) Artificial intelligence security incidents.

(II) Artificial intelligence safety incidents.

(ii) Taxonomies to classify incidents referred to in clause (i) based on relevant characteristics, impacts, or other appropriate criteria.

(B) Assess the usefulness and cost-effectiveness of an effort to voluntarily track substantial artificial intelligence security incidents and substantial artificial intelligence safety incidents.

(C) Identify and provide guidelines, best practices, methodologies, procedures, and processes for tracking and reporting substantial artificial intelligence security incidents and substantial artificial intelligence safety incidents across different sectors and use cases.

(D) Support the development of standardized reporting and documentation mechanisms, including automated mechanisms, that would help provide information, including public information, regarding substantial artificial intelligence security incidents and substantial artificial intelligence safety incidents.

(E) Support the development of norms for reporting of substantial artificial intelligence security incidents and substantial artificial intelligence safety incidents, taking into account when it is appropriate to publicly disclose such incidents.

(3) REPORT.—Not later than three years after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall submit to Congress a report on a process relating to the voluntary collection, reporting, and tracking of substantial artificial intelligence security incidents and substantial artificial intelligence safety incidents under paragraph (1). Such report shall include the following:

(A) Findings from the multi-stakeholder process referred to in such paragraph.

(B) An assessment of and recommendations for establishing reporting and collection mechanisms by which industry, academia, nonprofit organizations, standards development organizations, civil society groups, and appropriate public sector entities may voluntarily share standardized information regarding substantial artificial intelligence security incidents and substantial artificial intelligence safety incidents;

(c) LIMITATION.—Nothing in this section provides the Director of the National Institute of Standards and Technology with any enforcement authority that was not in effect on the day before the date of the enactment of this section.

(d) DEFINITIONS.—In this section:

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

(2) ARTIFICIAL INTELLIGENCE SECURITY VULNERABILITY.—The term ''artificial intelligence security vulnerability'' means a weakness in an artificial intelligence system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

(3) ARTIFICIAL INTELLIGENCE SYSTEM.—The term ''artificial intelligence system'' has the meaning

given such term in section 7223 of the Advancing American AI Act (40 U.S.C. 11301 note; as enacted as part of title LXXII of division G of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023; Public Law 117–263).

(4) SECTOR RISK MANAGEMENT AGENCY.—The term ''Sector Risk Management Agency'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(5) THREAT SOURCE.—The term ''threat source'' means any of the following:

(A) An intent and method targeted at the intentional exploitation of a vulnerability.

(B) A situation and method that may accidentally trigger a vulnerability.

○