AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

118TH CONGRESS
1ST SESSION

S. 3050

To require a report on artificial intelligence regulation in the financial services industry, to establish artificial intelligence bug bounty programs, to require a vulnerability analysis study for artificial intelligence-enabled military applications, and to require a report on data sharing and coordination, and for other purposes.

IN THE SENATE OF THE UNITED STATES

OCTOBER 17, 2023

Mr. ROUNDS (for himself, Mr. SCHUMER, Mr. YOUNG, and Mr. HEINRICH) introduced the following bill; which was read twice and referred to the Committee on Armed Services

---

A BILL

To require a report on artificial intelligence regulation in the financial services industry, to establish artificial intelligence bug bounty programs, to require a vulnerability analysis study for artificial intelligence-enabled military applications, and to require a report on data sharing and coordination, 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 ''Artificial Intelligence Advancement Act of 2023''.

SEC. 2. DEFINITIONS.

In this Act:

(1) CONGRESSIONAL DEFENSE COMMITTEES.—The term ''congressional defense committees'' has the meaning given such term in section 101 of title 10, United States Code.

(2) FOUNDATIONAL ARTIFICIAL INTELLIGENCE MODEL.—The term ''foundational artificial intelligence model'' means an adaptive generative model that is trained on a broad set of unlabeled data sets that can be used for different tasks, with minimal fine-tuning.

SEC. 3. REPORT ON ARTIFICIAL INTELLIGENCE REGULATION IN FINANCIAL SERVICES INDUSTRY.

(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, each of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the National Credit Union Administration, and the Bureau of Consumer Financial Protection shall submit to the Committee on Banking, Housing and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives a report on its gap in knowledge relating to artificial intelligence, including an analysis on—

(1) which tasks are most frequently being assisted or completed with artificial intelligence in the institutions the agency regulates;

(2) current governance standards in place for artificial intelligence use at the agency and current standards in place for artificial intelligence oversight by the agency;

(3) potentially additional regulatory authorities required by the agency to continue to successfully execute its mission;

(4) where artificial intelligence may lead to overlapping regulatory issues between agencies that require clarification;

(5) how the agency is currently using artificial intelligence, how the agency plans to use such artificial intelligence the next 3 years, and the expected impact, including fiscal and staffing, of those plans; and

(6) what resources, monetary or other resources, if any, the agency requires to both adapt to the changes that artificial intelligence will bring to the regulatory landscape and to adequately adopt and oversee the use of artificial intelligence across its operations described in paragraph (5).

(b) RULE OF CONSTRUCTION.—Nothing in this section may be construed to require an agency to include confidential supervisory information or pre-decisional or deliberative non-public information in a report under this section.

SEC. 4. ARTIFICIAL INTELLIGENCE BUG BOUNTY PROGRAMS.

(a) PROGRAM FOR FOUNDATIONAL ARTIFICIAL INTELLIGENCE PRODUCTS BEING INCORPORATED BY DEPARTMENT OF DEFENSE.—

(1) DEVELOPMENT REQUIRED.—Not later than 180 days after the date of the enactment of this Act and subject to the availability of appropriations, the Chief Data and Artificial Intelligence Officer of the Department of Defense shall develop a bug bounty program for foundational artificial intelligence models being integrated into Department of Defense missions and operations.

(2) COLLABORATION.—In developing the program required by paragraph (1), the Chief may collaborate with the heads of other government agencies that have expertise in cybersecurity and artificial intelligence.

(3) IMPLEMENTATION AUTHORIZED.—The Chief may carry out the program developed pursuant to subsection (a).

(4) CONTRACTS.—The Secretary of Defense shall ensure, as may be appropriate, that whenever the Department of Defense enters into any contract, the contract allows for participation in the bug bounty program developed pursuant to paragraph (1).

(5) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to require—

(A) the use of any foundational artificial intelligence model; or

(B) the implementation of the program developed pursuant to paragraph (1) in order for the Department to incorporate a foundational artificial intelligence model.

(b) BRIEFING.—Not later than one year after the date of the enactment of this Act, the Chief shall provide the congressional defense committees a briefing on—

(1) the development and implementation of bug bounty programs the Chief considers relevant to the matters covered by this section; and

(2) long-term plans of the Chief with respect to such bug bounty programs.

SEC. 5. VULNERABILITY ANALYSIS STUDY FOR ARTIFICIAL INTELLIGENCE-ENABLED MILITARY APPLICATIONS.

(a) STUDY REQUIRED.—Not later than one year after the date of the enactment of this Act, the Chief Digital and Artificial Intelligence Officer (CDAO) of the Department of Defense shall complete a study analyzing the vulnerabilities to the privacy, security, and accuracy of, and capacity to assess, artificial intelligence-enabled military applications, as well as research and development needs for such applications.

(b) ELEMENTS.—The study required by subsection (a) shall cover the following:

(1) Research and development needs and transition pathways to advance explainable and interpretable artificial intelligence-enabled military applications, including the capability to assess the underlying algorithms and data models of such applications.

(2) Assessing the potential risks to the privacy, security, and accuracy of underlying architectures and algorithms of artificial intelligence-enabled military applications, including the following:

(A) Individual foundational artificial intelligence models, including the adequacy of existing testing, training, and auditing for such

models to ensure models can be properly assessed over time.

(B) The interactions of multiple artificial intelligence-enabled military applications, and the ability to detect and assess new, complex, and emergent behavior amongst individual agents, as well as the collective impact, including how such changes may affect risk to privacy, security, and accuracy over time.

(C) The impact of increased agency in artificial intelligence-enabled military applications and how such increased agency may affect the ability to detect and assess new, complex, and emergent behavior, as well risks to the privacy, security, and accuracy of such applications over time.

(3) Assessing the survivability and traceability of decision support systems that are integrated with artificial intelligence-enabled military applications and used in a contested environment, including—

(A) potential benefits and risks to Department of Defense missions and operations of implementing such applications; and

(B) other technical or operational constraints to ensure such decision support sys-

tems that are integrated with artificial intelligence-enabled military applications are able to adhere to the Department of Defense Ethical Principles for Artificial Intelligence.

(4) Identification of existing artificial intelligence metrics, developmental, testing and audit capabilities, personnel, and infrastructure within the Department of Defense, including test and evaluation facilities, needed to enable ongoing identification and assessment under paragraphs (1) through (3), and other factors such as—

(A) implications for deterrence systems based on systems warfare; and

(B) vulnerability to systems confrontation on the system and system-of-systems level.

(5) Identification of gaps or research needs to sufficiently respond to the elements outlined in this subsection that are not currently, or not sufficiently, funded within the Department of Defense.

(c) COORDINATION.—In carrying out the study required by subsection (a), the Chief Digital and Artificial Intelligence Officer shall coordinate with the following:

(1) The Director of the Defense Advanced Research Projects Agency (DARPA).

(2) The Under Secretary of Defense for Research and Evaluation.

(3) The Under Secretary of Defense for Policy.

(4) The Director for Operational Test and Evaluation (DOT&E) of the Department.

(5) As the Chief Digital and Artificial Intelligence Officer considers appropriate, the following:

(A) The Secretary of Energy.

(B) The Director of the National Institute of Standards and Technology.

(C) The Director of the National Science Foundation.

(D) The head of the National Artificial Intelligence Initiative Office of the Office of Science and Technology Policy.

(E) Members and representatives of industry.

(F) Members and representatives of academia.

(d) INTERIM BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Chief Digital and Artificial Intelligence Officer shall provide the congressional defense committees a briefing on the interim findings of the Chief Digital and Artificial Intelligence Of-

ficer with respect to the study being conducted pursuant to subsection (a).

(e) FINAL REPORT.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Chief Digital and Artificial Intelligence Officer shall submit to the congressional defense committees a final report on the findings of the Chief Digital and Artificial Intelligence Officer with respect to the study conducted pursuant to subsection (a).

(2) FORM.—The final report submitted pursuant to paragraph (1) shall be submitted in unclassified for, but may include a classified annex.

SEC. 6. REPORT ON DATA SHARING AND COORDINATION.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report on ways to improve data sharing, interoperability, and quality, as may be appropriate, across the Department of Defense.

(b) CONTENTS.—The report submitted pursuant to subsection (a) shall include the following:

(1) A description of policies, practices, and cultural barriers that impede data sharing and inter-

operability, and lead to data quality issues, among components of the Department.

(2) The impact a lack of appropriate levels of data sharing, interoperability, and quality has on Departmental collaboration, efficiency, interoperability, and joint-decisionmaking.

(3) A review of current efforts to promote appropriate data sharing, including to centralize data management, such as the AVANA program.

(4) A description of near-, mid-, and long-term efforts that the Office of the Secretary of Defense plans to implement to promote data sharing and interoperability, including efforts to improve data quality.

(5) A detailed plan to implement a data sharing and interoperability strategy that supports effective development and employment of artificial intelligence-enabled military applications.

(6) A detailed assessment of the implementation of the Department of Defense Data Strategy issued in 2020, as well as the use of data decrees to improve management rigor in the Department when it comes to data sharing and interoperability.

(7) Any recommendations for Congress with respect to assisting the Department in these efforts.

○