119TH CONGRESS
1ST SESSION

S. _____

To direct the Director of the National Security Agency to develop guidance to secure artificial intelligence related technologies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. YOUNG introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To direct the Director of the National Security Agency to develop guidance to secure artificial intelligence related technologies, 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 ''Advanced Artificial Intelligence Security Readiness Act of 2025''.

SEC. 2. ARTIFICIAL INTELLIGENCE SECURITY GUIDANCE.

(a) REQUIREMENT.—The Director of the National Security Agency, acting through the Artificial Intelligence Security Center (or successor office), shall develop and disseminate security guidance that identifies potential

vulnerabilities in covered artificial intelligence technologies and artificial intelligence supply chains, with a focus on cybersecurity risks and security challenges that are unique to protecting artificial intelligence systems, associated computing environments, or the wider artificial intelligence supply chain from theft or sabotage by foreign threat actors.

(b) ELEMENTS.—The guidance developed and disseminated under subsection (a) shall include the following:

(1) Identification of potential vulnerabilities and cybersecurity challenges that are unique to protecting covered artificial intelligence technologies and the artificial intelligence supply chain, such as threat vectors that are less common or severe in conventional information technology systems.

(2) Identification of elements of the artificial intelligence supply chain that, if accessed by threat actors, would meaningfully contribute to the actor's ability to develop covered artificial intelligence technologies or compromise the confidentiality, integrity, or availability of artificial intelligence systems or associated artificial intelligence supply chains.

(3) Strategies to identify, protect, detect, respond to, and recover from cyber threats posed by

threat actors targeting covered artificial intelligence technologies, including—

(A) procedures to protect model weights or other competitively sensitive model artifacts;

(B) ways to mitigate insider threats, including personnel vetting processes;

(C) network access control procedures;

(D) counterintelligence and anti-espionage measures; and

(E) other measures that can be used to reduce threats of technology theft or sabotage by foreign threat actors.

(c) FORM.—The guidance developed and disseminated under subsection (a) shall include—

(1) detailed best practices, principles, and guidelines in unclassified form, which may include a classified annex; and

(2) classified materials for conducting security briefings for service providers.

(d) ENGAGEMENT.—In developing the guidance required by subsection (a), the Director shall—

(1) engage with prominent artificial intelligence developers and researchers, as determined by the Director, to assess and anticipate the capabilities of

highly advanced artificial intelligence systems relevant to national security, including by—

(A) conducting a comprehensive review of publicly available industry documents pertaining to the security of artificial intelligence systems with respect to preparedness frameworks, scaling policies, risk management frameworks, and other matters;

(B) conducting interviews with subject matter experts;

(C) hosting roundtable discussions and expert panels; and

(D) visiting facilities used to develop artificial intelligence;

(2) leverage existing expertise and research, collaborate with relevant National Laboratories, university affiliated research centers, and any federally funded research and development center that has conducted research on strategies to secure artificial intelligence models from nation-state actors and other highly resourced actors; and

(3) consult, as appropriate, with other departments and agencies of the Federal Government as the Director determines relevant, including the Bureau of Industry and Security of the Department of

Commerce, the Center for Artificial Intelligence Standards and Innovation of the National Institute of Standards and Technology, the Department of Homeland Security, and the Department of Defense.

(e) REPORTS.—

(1) INITIAL REPORT.—Not later than 180 days after the date of the enactment of this Act, the Director shall submit to the congressional intelligence committees a report on the guidance required by subsection (a), including a summary of progress on the development of the guidance, an outline of remaining sections, and any relevant insights about artificial intelligence security.

(2) FINAL REPORT.—Not later than 365 days after the date of enactment of this Act, the Director shall submit to the congressional intelligence committees a report on the guidance required by subsection (a).

(3) FORM.—The report submitted under paragraph (2)—

(A) shall include—

(i) an unclassified version suitable for dissemination to relevant individuals, including in the private sector; and

(ii) a publicly available version; and

(B) may include a classified annex.

(f) DEFINITIONS.—In this section:

(1) The term ''artificial intelligence'' has the meaning given such term in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. note prec. 4061).

(2) The term ''*artificial intelligence* supply chain'' means artificial intelligence models computing environments for performing model training or inference tasks, training or test data, frameworks, or other components or model artifacts necessary for the training, management, or maintenance of any artificial intelligence system.

(3) The term ''congressional intelligence committees'' means the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

(4) The term ''covered *artificial intelligence* technologies'' means advanced artificial intelligence (whether developed by the private sector, the United States Government, or a public-private partnership) with critical capabilities that the Director determines would pose a grave national security threat if acquired or stolen by threat actors, such as artificial

intelligence systems that match or exceed human expert performance in chemical, biological, radiological, and nuclear matters, cyber offense, model autonomy, persuasion, research and development, and self-improvement.

(5) The term ''technology theft'' means any unauthorized acquisition, replication, or appropriation of covered artificial intelligence technologies or components of such technologies, including models, model weights, architectures, or core algorithmic insights, through any means, such as cyber attacks, insider threats, and side-channel attacks, or exploitation of public interfaces.

(6) The term ''threat actors'' means nation-state actors and other highly resourced actors capable of technology theft or sabotage.