.....

(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

To direct the Director of the National Security Agency to develop strategies to secure artificial intelligence related technologies.

IN THE HOUSE OF REPRESENTATIVES

Mr. LAHOOD introduced the following bill; which was referred to the Committee on _____

A BILL

To direct the Director of the National Security Agency to develop strategies to secure artificial intelligence related technologies.

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 AI Security Readiness Act''.

SEC. 2. AI SECURITY PLAYBOOK.

(a) REQUIREMENT.—The Director of the National Security Agency, acting through the Artificial Intelligence

Security Center (or successor office), shall develop strategies (in this section referred to as the ''AI Security Playbook'') to defend covered AI technologies from technology theft by threat actors.

(b) ELEMENTS.—The AI Security Playbook under subsection (a) shall include the following:

(1) Identification of potential vulnerabilities in advanced AI data centers and among advanced AI developers capable of producing covered AI technologies, with a focus on cybersecurity risks and other security challenges that are unique to protecting covered AI technologies and critical components of such technologies (such as threat vectors that do not typically arise, or are less severe, in the context of conventional information technology systems).

(2) Identification of components or information that, if accessed by threat actors, would meaningfully contribute to progress made by the actor with respect to developing covered AI technologies, including with respect to—

(A) AI models and key components of such models;

(B) core insights relating to the development of advanced AI systems, including with

respect to training such systems, the inferences made by such systems, and the engineering of such systems; and

(C) other related information.

(3) Strategies to detect, prevent, and respond to cyber threats by threat actors targeting covered AI technologies.

(4) Identification of the levels of security, if any, that would require substantial involvement by the United States Government in the development or oversight of highly advanced AI systems.

(5) Analysis of how the United States Government would be involved to achieve the levels of security identified in paragraph (4), including a description of a hypothetical initiative to build covered AI technology systems in a highly secure governmental environment, considering, at a minimum, cybersecurity protocols, provisions to protect model weights, efforts to mitigate insider threats (including personnel vetting and security clearance adjudication processes), access control procedures, counterintelligence and anti-espionage measures, contingency and emergency response plans, and other strategies that would be used to reduce threats of technology theft by threat actors.

(c) FORM.—The AI Security Playbook under subsection (a) shall include—

(1) detailed methodologies and intelligence assessments, which may be contained in a classified annex; and

(2) an unclassified portion with general guidelines and best practices suitable for dissemination to relevant individuals, including in the private sector.

(d) ENGAGEMENT.—

(1) IN GENERAL.—In developing the AI Security Playbook under subsection (a), the Director shall—

(A) engage with prominent AI developers and researchers, as determined by the Director, to assess and anticipate the capabilities of highly advanced AI systems relevant to national security, including by—

(i) conducting a comprehensive review of industry documents pertaining to the security of AI systems with respect to preparedness frameworks, scaling policies, risk management frameworks, and other matters;

(ii) conducting interviews with subject matter experts;

(iii) hosting roundtable discussions and expert panels; and

(iv) visiting facilities used to develop AI; and

(B) to leverage existing expertise and research, collaborate with a federally funded research and development center that has conducted research on strategies to secure AI models from nation-state actors and other highly resourced actors.

(2) NONAPPLICABILITY OF FACA.—None of the activities described in this subsection shall be construed to establish or use an advisory committee subject to chapter 10 of title 5, United States Code.

(e) REPORTS.—

(1) INITIAL REPORT.—Not later than 90 days after the date of the enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the AI Security Playbook under subsection (a), including a summary of progress on the development of Playbook, an outline of remaining sections, and any relevant insights about AI security.

(2) FINAL REPORT.—Not later than 270 days after the date of enactment of this Act, the Director

shall submit to the appropriate congressional committees a report on the Playbook.

(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) RULE OF CONSTRUCTION.—Nothing in subsection (b)(4) shall be construed to authorize or require any regulatory or enforcement action by the United States Government.

(g) DEFINITIONS.—In this section:

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

(2) The terms ''artificial intelligence'' and ''AI'' have the meaning given the term ''artificial intelligence'' 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).

(3) The term ''covered AI technologies'' means advanced AI (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 AI systems that match or exceed human expert performance in relating to chemical, biological, radiological, and nuclear matters, cyber offense, model autonomy, persuasion, research and development, and self-improvement.

(4) The term ''technology theft'' means any unauthorized acquisition, replication, or appropriation of covered AI 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.

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