

119TH CONGRESS  
1ST SESSION

# H. R. 3919

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

---

## IN THE HOUSE OF REPRESENTATIVES

JUNE 11, 2025

Mr. LAHOOD (for himself, Mr. MOOLENAAR, Mr. GOTTHEIMER, and Mr. KRISHNAMOORTHY) introduced the following bill; which was referred to the Permanent Select Committee on Intelligence

---

## A BILL

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

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Advanced AI Security  
5 Readiness Act”.

6 **SEC. 2. AI SECURITY PLAYBOOK.**

7 (a) REQUIREMENT.—The Director of the National  
8 Security Agency, acting through the Artificial Intelligence  
9 Security Center (or successor office), shall develop strate-

1 gies (in this section referred to as the “AI Security Play-  
2 book”) to defend covered AI technologies from technology  
3 theft by threat actors.

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

6 (1) Identification of potential vulnerabilities in  
7 advanced AI data centers and among advanced AI  
8 developers capable of producing covered AI tech-  
9 nologies, with a focus on cybersecurity risks and  
10 other security challenges that are unique to pro-  
11 tecting covered AI technologies and critical compo-  
12 nents of such technologies (such as threat vectors  
13 that do not typically arise, or are less severe, in the  
14 context of conventional information technology sys-  
15 tems).

16 (2) Identification of components or information  
17 that, if accessed by threat actors, would meaning-  
18 fully contribute to progress made by the actor with  
19 respect to developing covered AI technologies, in-  
20 cluding with respect to—

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

23 (B) core insights relating to the develop-  
24 ment of advanced AI systems, including with  
25 respect to training such systems, the inferences

1           made by such systems, and the engineering of  
2           such systems; and

3           (C) other related information.

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

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

11          (5) Analysis of how the United States Govern-  
12          ment would be involved to achieve the levels of secu-  
13          rity identified in paragraph (4), including a descrip-  
14          tion of a hypothetical initiative to build covered AI  
15          technology systems in a highly secure governmental  
16          environment, considering, at a minimum, cybersecu-  
17          rity protocols, provisions to protect model weights,  
18          efforts to mitigate insider threats (including per-  
19          sonnel vetting and security clearance adjudication  
20          processes), access control procedures, counterintel-  
21          ligence and anti-espionage measures, contingency  
22          and emergency response plans, and other strategies  
23          that would be used to reduce threats of technology  
24          theft by threat actors.

1 (c) FORM.—The AI Security Playbook under sub-  
2 section (a) shall include—

3 (1) detailed methodologies and intelligence as-  
4 sements, which may be contained in a classified  
5 annex; and

6 (2) an unclassified portion with general guide-  
7 lines and best practices suitable for dissemination to  
8 relevant individuals, including in the private sector.

9 (d) ENGAGEMENT.—

10 (1) IN GENERAL.—In developing the AI Secu-  
11 rity Playbook under subsection (a), the Director  
12 shall—

13 (A) engage with prominent AI developers  
14 and researchers, as determined by the Director,  
15 to assess and anticipate the capabilities of high-  
16 ly advanced AI systems relevant to national se-  
17 curity, including by—

18 (i) conducting a comprehensive review  
19 of industry documents pertaining to the se-  
20 curity of AI systems with respect to pre-  
21 paredness frameworks, scaling policies, risk  
22 management frameworks, and other mat-  
23 ters;

24 (ii) conducting interviews with subject  
25 matter experts;

1 (iii) hosting roundtable discussions  
2 and expert panels; and

3 (iv) visiting facilities used to develop  
4 AI; and

5 (B) to leverage existing expertise and re-  
6 search, collaborate with a federally funded re-  
7 search and development center that has con-  
8 ducted research on strategies to secure AI mod-  
9 els from nation-state actors and other highly  
10 resourced actors.

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

15 (e) REPORTS.—

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

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

1 shall submit to the appropriate congressional com-  
2 mittees a report on the Playbook.

3 (3) FORM.—The report submitted under para-  
4 graph (2)—

5 (A) shall include—

6 (i) an unclassified version suitable for  
7 dissemination to relevant individuals, in-  
8 cluding in the private sector; and

9 (ii) a publicly available version; and

10 (B) may include a classified annex.

11 (f) RULE OF CONSTRUCTION.—Nothing in subsection  
12 (b)(4) shall be construed to authorize or require any regu-  
13 latory or enforcement action by the United States Govern-  
14 ment.

15 (g) DEFINITIONS.—In this section:

16 (1) The term “appropriate congressional com-  
17 mittees” means the Permanent Select Committee on  
18 Intelligence of the House of Representatives and the  
19 Select Committee on Intelligence of the Senate.

20 (2) The terms “artificial intelligence” and “AI”  
21 have the meaning given the term “artificial intel-  
22 ligence” in section 238(g) of the John S. McCain  
23 National Defense Authorization Act for Fiscal Year  
24 2019 (Public Law 115–232; 10 U.S.C. note prec.  
25 4061).

1           (3) The term “covered AI technologies” means  
2           advanced AI (whether developed by the private sec-  
3           tor, the United States Government, or a public-pri-  
4           vate partnership) with critical capabilities that the  
5           Director determines would pose a grave national se-  
6           curity threat if acquired or stolen by threat actors,  
7           such as AI systems that match or exceed human ex-  
8           pert performance in relating to chemical, biological,  
9           radiological, and nuclear matters, cyber offense,  
10          model autonomy, persuasion, research and develop-  
11          ment, and self-improvement.

12          (4) The term “technology theft” means any un-  
13          authorized acquisition, replication, or appropriation  
14          of covered AI technologies or components of such  
15          technologies, including models, model weights, archi-  
16          tectures, or core algorithmic insights, through any  
17          means, such as cyber attacks, insider threats, and  
18          side-channel attacks, or exploitation of public inter-  
19          faces.

20          (5) The term “threat actors” means nation-  
21          state actors and other highly resourced actors capa-  
22          ble of technology theft.

○