

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

_____ (legislative day, _____), _____
Mr. YOUNG (for himself and Mr. KELLY) 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.

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 Artificial
5 Intelligence Security Readiness Act of 2025”.

6 **SEC. 2. ARTIFICIAL INTELLIGENCE SECURITY GUIDANCE.**

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

1 vulnerabilities in covered artificial intelligence technologies
2 and artificial intelligence supply chains, with a focus on
3 cybersecurity risks and security challenges that are unique
4 to protecting artificial intelligence systems, associated
5 computing environments, or the wider artificial intel-
6 ligence supply chain from theft or sabotage by foreign
7 threat actors.

8 (b) ELEMENTS.—The guidance developed and dis-
9 seminated under subsection (a) shall include the following:

10 (1) Identification of potential vulnerabilities and
11 cybersecurity challenges that are unique to pro-
12 tecting covered artificial intelligence technologies and
13 the artificial intelligence supply chain, such as threat
14 vectors that are less common or severe in conven-
15 tional information technology systems.

16 (2) Identification of elements of the artificial
17 intelligence supply chain that, if accessed by threat
18 actors, would meaningfully contribute to the actor's
19 ability to develop covered artificial intelligence tech-
20 nologies or compromise the confidentiality, integrity,
21 or availability of artificial intelligence systems or as-
22 sociated artificial intelligence supply chains.

23 (3) Strategies to identify, protect, detect, re-
24 spond to, and recover from cyber threats posed by

1 threat actors targeting covered artificial intelligence
2 technologies, including—

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

5 (B) ways to mitigate insider threats, in-
6 cluding personnel vetting processes;

7 (C) network access control procedures;

8 (D) counterintelligence and anti-espionage
9 measures; and

10 (E) other measures that can be used to re-
11 duce threats of technology theft or sabotage by
12 foreign threat actors.

13 (c) FORM.—The guidance developed and dissemi-
14 nated under subsection (a) shall include—

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

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

20 (d) ENGAGEMENT.—In developing the guidance re-
21 quired by subsection (a), the Director shall—

22 (1) engage with prominent artificial intelligence
23 developers and researchers, as determined by the Di-
24 rector, to assess and anticipate the capabilities of

1 highly advanced artificial intelligence systems rel-
2 evant to national security, including by—

3 (A) conducting a comprehensive review of
4 publicly available industry documents pertaining
5 to the security of artificial intelligence systems
6 with respect to preparedness frameworks, scal-
7 ing policies, risk management frameworks, and
8 other matters;

9 (B) conducting interviews with subject
10 matter experts;

11 (C) hosting roundtable discussions and ex-
12 pert panels; and

13 (D) visiting facilities used to develop artifi-
14 cial intelligence;

15 (2) leverage existing expertise and research, col-
16 laborate with relevant National Laboratories, univer-
17 sity affiliated research centers, and any federally
18 funded research and development center that has
19 conducted research on strategies to secure artificial
20 intelligence models from nation-state actors and
21 other highly resourced actors; and

22 (3) consult, as appropriate, with other depart-
23 ments and agencies of the Federal Government as
24 the Director determines relevant, including the Bu-
25 reau of Industry and Security of the Department of

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

5 (e) REPORTS.—

6 (1) INITIAL REPORT.—Not later than 180 days
7 after the date of the enactment of this Act, the Di-
8 rector shall submit to the congressional intelligence
9 committees a report on the guidance required by
10 subsection (a), including a summary of progress on
11 the development of the guidance, an outline of re-
12 maining sections, and any relevant insights about ar-
13 tificial intelligence security.

14 (2) FINAL REPORT.—Not later than 365 days
15 after the date of enactment of this Act, the Director
16 shall submit to the congressional intelligence com-
17 mittees a report on the guidance required by sub-
18 section (a).

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

21 (A) shall include—

22 (i) an unclassified version suitable for
23 dissemination to relevant individuals, in-
24 cluding in the private sector; and

25 (ii) a publicly available version; and

1 (B) may include a classified annex.

2 (f) DEFINITIONS.—In this section:

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

8 (2) The term “*artificial intelligence* supply
9 chain” means artificial intelligence models com-
10 puting environments for performing model training
11 or inference tasks, training or test data, frameworks,
12 or other components or model artifacts necessary for
13 the training, management, or maintenance of any
14 artificial intelligence system.

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

19 (4) The term “covered *artificial intelligence*
20 technologies” means advanced artificial intelligence
21 (whether developed by the private sector, the United
22 States Government, or a public-private partnership)
23 with critical capabilities that the Director determines
24 would pose a grave national security threat if ac-
25 quired or stolen by threat actors, such as artificial

1 intelligence systems that match or exceed human ex-
2 pert performance in chemical, biological, radiological,
3 and nuclear matters, cyber offense, model autonomy,
4 persuasion, research and development, and self-im-
5 provement.

6 (5) The term “technology theft” means any un-
7 authorized acquisition, replication, or appropriation
8 of covered artificial intelligence technologies or com-
9 ponents of such technologies, including models,
10 model weights, architectures, or core algorithmic in-
11 sights, through any means, such as cyber attacks,
12 insider threats, and side-channel attacks, or exploi-
13 tation of public interfaces.

14 (6) The term “threat actors” means nation-
15 state actors and other highly resourced actors capa-
16 ble of technology theft or sabotage.