

119TH CONGRESS
2D SESSION

H. R. 9363

To amend the National Artificial Intelligence Initiative Act of 2020 to establish a center on artificial intelligence to ensure continued United States leadership in research, development, and evaluation of artificial intelligence systems, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 18, 2026

Mr. OBERNOLTE (for himself, Mrs. FOUSHEE, Mr. BABIN, Mr. MANN, and Mr. SCOTT FRANKLIN of Florida) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

A BILL

To amend the National Artificial Intelligence Initiative Act of 2020 to establish a center on artificial intelligence to ensure continued United States leadership in research, development, and evaluation of artificial intelligence systems, 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 “AI Security and Inno-
5 vation Act”.

1 **SEC. 2. ARTIFICIAL INTELLIGENCE ADVANCEMENT AND**
2 **RELIABILITY.**

3 (a) IN GENERAL.—The National Artificial Intel-
4 ligence Initiative Act of 2020 (enacted as division E of
5 the William M. (Mac) Thornberry National Defense Au-
6 thorization Act for Fiscal Year 2021; Public Law 116–
7 283) is amended—

8 (1) in section 5002 (15 U.S.C. 9401)—

9 (A) in paragraph (3)—

10 (i) in the heading, by striking “ARTI-
11 FICIAL” and inserting “AI; ARTIFICIAL”;

12 (ii) by striking “term ‘artificial intel-
13 ligence’ means” and inserting “terms ‘AI’
14 and ‘artificial intelligence’ mean”; and

15 (iii) by adding at the end the fol-
16 lowing new paragraphs:

17 “(4) ARTIFICIAL INTELLIGENCE MODEL.—The
18 term ‘artificial intelligence model’ means a compo-
19 nent of an artificial intelligence system that is—

20 “(A) derived using mathematical, computa-
21 tional, statistical, or machine-learning tech-
22 niques; and

23 “(B) used as part of an artificial intel-
24 ligence system to produce outputs or behaviors
25 from a defined set of inputs.

1 “(5) ARTIFICIAL INTELLIGENCE SYSTEM.—The
 2 term ‘artificial intelligence system’ means a data
 3 system, software, application, hardware, tool, service,
 4 or utility that operates in whole or in part using ar-
 5 tificial intelligence.”;

6 (B) by redesignating paragraphs (4), (5),
 7 (6), (7), (8), (9), (10), and (11) as paragraphs
 8 (6), (8), (9), (10), (11), (13), (14), and (15),
 9 respectively;

10 (C) by inserting after paragraph (6), as so
 11 redesignated, the following new paragraphs:

12 “(7) FOREIGN ADVERSARY.—The term ‘foreign
 13 adversary’ has the meaning given the term ‘covered
 14 nation’ in section 4872(f)(2) of title 10, United
 15 States Code.”; and

16 (D) by inserting after paragraph (11), as
 17 so redesignated, the following new paragraph:

18 “(12) INTELLIGENCE COMMUNITY.—The term
 19 ‘intelligence community’ has the meaning given such
 20 term in section 3(4) of the National Security Act of
 21 1947 (50 U.S.C. 3003(4)).”; and

22 (2) in title LIII (15 U.S.C. 9441 et seq.), by
 23 adding at the end the following new section:

24 **“SEC. 5304. CENTER FOR AI SECURITY AND INNOVATION.**

25 “(a) ESTABLISHMENT.—

1 “(1) IN GENERAL.—Not later than 60 days
2 after the date of the enactment of this section, the
3 Secretary of Commerce, acting through the Under
4 Secretary of Commerce for Standards and Innova-
5 tion (in this section referred to as the ‘Secretary’
6 and ‘Under Secretary’, respectively), shall establish
7 in the National Institute of Standards and Tech-
8 nology a center on artificial intelligence, to be known
9 as the ‘Center for AI Security and Innovation’ (in
10 this section referred to as the ‘Center’).

11 “(2) ACTIVITIES.—The Center shall carry out
12 the following:

13 “(A) Measure risks related to artificial in-
14 telligence systems, including national security
15 risks and economic security risks.

16 “(B) Support the exchange of information
17 between non-governmental entities and Federal
18 departments and agencies to facilitate mitiga-
19 tion related to any such risks.

20 “(C) Ensure continued leadership in the
21 United States with respect to research, develop-
22 ment, and evaluation of artificial intelligence
23 systems.

24 “(3) TRANSFER STUDY.—

1 “(A) IN GENERAL.—The Secretary may
2 conduct a study, as the Secretary determines
3 appropriate, that includes the following:

4 “(i) An assessment of the feasibility,
5 and the advantages and disadvantages, of
6 transferring the Center to an agency of the
7 Department of Commerce, or establishing
8 the Center as an agency of the Depart-
9 ment.

10 “(ii) Recommendations for Congress
11 related to the following:

12 “(I) Any additional authority the
13 Center should have.

14 “(II) Amounts of funding for the
15 Center.

16 “(B) CONGRESSIONAL REVIEW.—If the
17 Secretary conducts the study under subpara-
18 graph (A), the Secretary shall, not later than
19 30 days after so conducting such study, submit
20 to the Committee on Science, Space, and Tech-
21 nology of the House of Representatives and the
22 Committee on Commerce, Science, and Trans-
23 portation of the Senate such study for review.

24 “(b) DIRECTOR.—

1 “(1) IN GENERAL.—Not later than 3 months
2 after the date of the enactment of this section, the
3 Secretary, acting through the Under Secretary, shall
4 appoint a director for the Center (referred to in this
5 section as the ‘Director’).

6 “(2) EXPERIENCE.—The Secretary, acting
7 through the Under Secretary, shall ensure the Direc-
8 tor has the experience and is qualified to provide ad-
9 vice and leadership to carry out the duties under
10 subsection (c).

11 “(c) DUTIES.—

12 “(1) IN GENERAL.—The Director shall carry
13 out the following:

14 “(A) Evaluate and improve security meas-
15 ures with respect to artificial intelligence sys-
16 tems and seek to reduce any risk of misuse of
17 such systems, including the evaluation and im-
18 provement of security measures that address
19 threats relating to the following:

20 “(i) Model serialization attacks.

21 “(ii) Model tampering.

22 “(iii) Data leakage.

23 “(iv) Adversarial prompt injection.

24 “(v) Model extraction.

25 “(vi) Model jailbreaks.

1 “(vii) Supply chain attacks.

2 “(B) Establish a process for covered enti-
3 ties to enter into voluntary agreements with the
4 Director to develop or evaluate, as appropriate,
5 covered frontier systems to conduct classified
6 and unclassified evaluations of risks that such
7 systems may pose to national security or eco-
8 nomic security, including with respect to risks
9 related to cybersecurity or chemical, biological,
10 radiological, or nuclear threats.

11 “(C) Conduct evaluations and assessments
12 with respect to the following:

13 “(i) Covered frontier systems devel-
14 oped by covered entities located in the fol-
15 lowing:

16 “(I) The United States.

17 “(II) A foreign adversary.

18 “(ii) Any potential security vulner-
19 ability, flaw, or malign foreign activity that
20 results from artificial intelligence systems.

21 “(iii) Any relevant artificial intel-
22 ligence system, as determined by the Di-
23 rector.

24 “(D) Support the laboratories of the Na-
25 tional Institute of Standards and Technology in

1 the development and voluntary adoption of
2 standards, guidelines, and best practices relat-
3 ing to the following:

4 “(i) The testing and evaluation of cov-
5 ered frontier systems.

6 “(ii) Measuring and improving the se-
7 curity and reliability of artificial intel-
8 ligence systems, including in areas such as
9 robustness, interpretability of artificial in-
10 telligence, security relating to data centers
11 and hardware security mechanisms.

12 “(iii) Any other matter relating to a
13 covered frontier system, as determined ap-
14 propriate by the Director.

15 “(E) Publish any such standards, guide-
16 lines, and best practices.

17 “(F) Assess the following:

18 “(i) Whether covered frontier systems
19 are developing or voluntarily adopting any
20 such standards, guidelines, or best prac-
21 tices.

22 “(ii) Any barrier to such voluntary
23 adoption.

24 “(G) Assess trends with respect to the de-
25 velopment of artificial intelligence in the United

1 States and in foreign adversaries, including
2 through comparative assessments of how the ca-
3 pabilities of artificial intelligence systems in the
4 U.S. and foreign adversaries differ with respect
5 to key artificial intelligence capabilities mile-
6 stones, as determined by the Director.

7 “(H) Any other action the Director deter-
8 mines necessary to carry out the activities of
9 the Center under subsection (a)(2).

10 “(2) CONSULTATION.—

11 “(A) IN GENERAL.—In carrying out para-
12 graph (1), the Director shall consult with the
13 following:

14 “(i) The Director of the Office of
15 Science and Technology Policy.

16 “(ii) The Secretary of Energy.

17 “(iii) The Secretary of Defense.

18 “(iv) The Secretary of Homeland Se-
19 curity.

20 “(v) Members of the intelligence com-
21 munity.

22 “(vi) The heads of any other relevant
23 Federal departments or agencies as the Di-
24 rector determines appropriate.

1 “(B) STANDARDS, GUIDELINES, AND BEST
2 PRACTICES.—Before the Director publishes any
3 standards, guidelines, or best practices pursu-
4 ant to paragraph (1)(E), the Director shall con-
5 sult with developers of artificial intelligence.

6 “(3) INTERAGENCY PARTICIPATION.—The Di-
7 rector shall be included in any interagency process
8 convened by the Executive Office of the President
9 relating to artificial intelligence policy, and may sub-
10 mit assessments and recommendations directly to
11 the National Security Council and the Office of
12 Science and Technology Policy on matters within the
13 scope of the duties described in paragraph (1).

14 “(4) DEFINING COVERED FRONTIER SYSTEM.—

15 “(A) IN GENERAL.—Not later than 180
16 days after the date of the enactment of this sec-
17 tion, the Under Secretary, acting through the
18 Director, shall publish, and update as the Di-
19 rector determines appropriate, a definition of
20 the term ‘covered frontier system’ that identi-
21 fies what capabilities and requirements an arti-
22 ficial intelligence system shall have to be consid-
23 ered such a ‘covered frontier system’.

24 “(B) ACTIVITIES.—In carrying out sub-
25 paragraph (A), the Under Secretary, acting

1 through the Director, in consultation with rel-
2 evant non-governmental entities (including de-
3 velopers of artificial intelligence), shall carry
4 out a program of measurement research to un-
5 derstand and benchmark the capabilities and
6 limitations of artificial intelligence systems over
7 time.

8 “(5) OPTIONAL PUBLICATION.—The Director
9 may make any evaluation or assessment conducted
10 under paragraph (1)(C) publicly available, as the Di-
11 rector determines appropriate.

12 “(d) CRITICAL TECHNICAL EXPERTS.—

13 “(1) IN GENERAL.—The Secretary may appoint
14 officers and employees for the Center as the Sec-
15 retary determines necessary.

16 “(2) HIRING CRITICAL TECHNICAL EXPERTS.—
17 Notwithstanding section 3104 of title 5, United
18 States Code, or the provisions of any other law relat-
19 ing to the appointment, number, classification, or
20 compensation of employees, the Secretary shall have
21 the authority to make appointments of scientific, en-
22 gineering, and professional personnel, and to fix the
23 basic pay of such personnel at a rate to be deter-
24 mined by the Secretary at rates not in excess of the
25 highest total annual compensation payable at the

1 rate determined under section 104 of title 3, United
2 States Code. The Secretary shall appoint not more
3 than 15 personnel under this subsection.

4 “(e) CONFIDENTIALITY OF RECORDS; LIMITATION.—
5 Any information shared with or provided to the Director
6 by a covered entity or the developer of a covered frontier
7 system to carry out subsection (c)—

8 “(1) shall be exempt from disclosure under sec-
9 tion 552(b)(3) of title 5, United States Code; and

10 “(2) may not—

11 “(A) be made public unless such covered
12 entity or developer provides the Director con-
13 sent for such information to be disclosed to the
14 public; and

15 “(B) be used by any Federal, State, local,
16 or Tribal government to regulate an activity of
17 such covered entity related to such information.

18 “(f) AVOIDING DUPLICATION.—In carrying out this
19 section, the Director shall take such actions as may be
20 necessary to ensure no unnecessary duplication with ac-
21 tivities carried out pursuant to section 22A of the National
22 Institute of Standards and Technology Act (15 U.S.C.
23 278h-1).

24 “(g) INTERNATIONAL ENGAGEMENT.—

1 “(1) IN GENERAL.—Except as provided in para-
2 graph (2), the Director may share information, col-
3 laborate, and participate in talent exchanges with a
4 center or institute similar to the Center that is lo-
5 cated in another country.

6 “(2) EXCEPTION.—Paragraph (1) does not
7 apply with respect to a center or institute similar to
8 the Center that is located in a foreign adversary.

9 “(h) REPORT.—For each fiscal year beginning with
10 fiscal year 2027, not later than 90 days after the Presi-
11 dent submits a budget for such fiscal year pursuant to
12 section 1105 of title 31, United States Code, the Secretary
13 shall submit to the Committee on Science, Space, and
14 Technology of the House of Representatives and the Com-
15 mittee on Commerce, Science, and Transportation of the
16 Senate a report that includes the following:

17 “(1) The budget of the Center for such fiscal
18 year.

19 “(2) Information relating to the consultation re-
20 quired by subsection (c)(2).

21 “(3) A description of any goals, priorities, and
22 metrics for guiding and evaluating any activities of
23 the Center under subsection (a)(2).

24 “(4) An assessment of the following:

1 “(A) The state of international competition
2 relating to artificial intelligence, including a
3 comparison between the capabilities of artificial
4 intelligence systems developed by entities in the
5 United States and foreign adversaries.

6 “(B) Any talent or personnel gaps affect-
7 ing the ability of the Director to carry out sub-
8 section (c), and any recommendations relating
9 to the recruitment and retention of personnel
10 through temporary rotational assignments of
11 personnel from other Federal departments or
12 agencies or non-governmental entities, fellow-
13 ship programs, or any other means of utilizing
14 specialized technical expertise from non-govern-
15 mental entities.

16 “(C) Any new or emerging capabilities that
17 may impact the national or economic security of
18 the United States that artificial intelligence sys-
19 tems currently possess or that the Director ex-
20 pects such systems to plausibly possess in the
21 upcoming years, with a focus on any such capa-
22 bilities that are most critical or relevant for the
23 national security of the United States.

1 “(i) PROHIBITION ON REGULATIONS.—This section
2 does not confer upon the Director any regulatory, rule-
3 making, or enforcement authority.

4 “(j) AUTHORIZATION OF APPROPRIATIONS.—There
5 is to be authorized to be appropriated to the Secretary
6 to carry out this section \$20,000,000 for each of fiscal
7 years 2027 through 2032.

8 “(k) SUNSET.—This section shall terminate on the
9 date that is 5 years after the date of the enactment of
10 this section.

11 “(l) RULES OF CONSTRUCTION.—Nothing in this sec-
12 tion may be construed to carry out any of the following:

13 “(1) Provide the Director, Secretary, or Under
14 Secretary any enforcement authority that was not in
15 effect on the day before the date of the enactment
16 of this section.

17 “(2) Confer any regulatory authority to any
18 Federal, State, local, or Tribal department or agen-
19 cy.

20 “(3) Modify any regulatory requirement to re-
21 port or submit information to a Federal, State, local,
22 or Tribal department or agency.

23 “(m) DEFINITIONS.—In this section:

24 “(1) COVERED ENTITY.—The term ‘covered en-
25 tity’ means an entity or consortium of entities with

1 a demonstrated ability to develop or evaluate, as the
2 case may be, a covered frontier system.

3 “(2) COVERED FRONTIER SYSTEM.—The term
4 ‘covered frontier system’ has the meaning deter-
5 mined by the Director pursuant to subsection
6 (c)(4).”.

7 (b) CLERICAL AMENDMENT.—The tables of contents
8 in section 2(b) and title LIII of division E of the William
9 M. (Mac) Thornberry National Defense Authorization Act
10 for Fiscal Year 2021 are amended by inserting after the
11 items relating to section 5303 the following new item:

“Sec. 5304. Center for AI Standards and Innovation.”.

