

119TH CONGRESS
2D SESSION

S. _____

To prevent foreign adversaries from threatening the national security of the United States by extracting key technical features of closed-source, United States-owned artificial intelligence models, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. HAGERTY (for himself, Mr. KIM, Mr. SCOTT of South Carolina, and Ms. CORTEZ MASTO) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To prevent foreign adversaries from threatening the national security of the United States by extracting key technical features of closed-source, United States-owned artificial intelligence models, 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 “Blocking Large-scale Ad-
5 versarial Distillation Efforts Act of 2026” or “BLADE
6 Act”.

7 **SEC. 2. SENSE OF CONGRESS.**

8 It is the sense of Congress that—

1 (1) artificial intelligence models owned by
2 United States private sector entities are essential for
3 advancing economic and national security interests
4 of the United States;

5 (2) many of the most advanced artificial intel-
6 ligence models owned by United States entities are
7 “closed-source models” whose unique technical char-
8 acteristics are not openly shared or published;

9 (3) the unauthorized acquisition of model capa-
10 bilities, such as model weights, model architectures,
11 and other technical characteristics of closed-source
12 artificial intelligence models, by persons of concern
13 through model extraction attacks represents a threat
14 to the national security and foreign policy interests
15 of the United States, as well as the intellectual prop-
16 erty rights and economic competitiveness of United
17 States entities;

18 (4) the United States Government, in coopera-
19 tion with private owners of closed-source artificial
20 intelligence models, should take steps to identify,
21 punish, and deter model extraction attacks on the
22 protected capabilities of closed-source artificial intel-
23 ligence models by persons of concern;

24 (5) model extraction attacks against United
25 States closed-source artificial intelligence models

1 allow foreign adversaries a short cut to acquiring ad-
2 vanced artificial intelligence capabilities; and

3 (6) authorized model training practices that ad-
4 here to the terms of service or are otherwise con-
5 sistent with contractual terms set by the owners of
6 closed-source artificial intelligence models are a le-
7 gitimate research method that play an important
8 role in artificial intelligence research and are fun-
9 damentally distinct from model extraction attacks
10 addressed by this Act.

11 **SEC. 3. DEFINITIONS.**

12 In this Act:

13 (1) APPROPRIATE CONGRESSIONAL COMMIT-
14 TEES.—The term “appropriate congressional com-
15 mittees” means—

16 (A) the Committee on Foreign Affairs of
17 the House of Representatives; and

18 (B) the Committee on Banking, Housing,
19 and Urban Affairs of the Senate.

20 (2) CLOSED-SOURCE ARTIFICIAL INTELLIGENCE
21 MODEL.—The term “closed-source artificial intel-
22 ligence model” means any artificial intelligence
23 model with the following characteristics:

24 (A) Proprietary key technical information,
25 such as underlying model weights, that are nec-

1 essary to reproduce and independently recreate
2 the model and that are not willingly shared with
3 third parties or otherwise made publicly avail-
4 able by the owner of the model.

5 (B) Access and use governed by terms of
6 service or contractual agreements that are es-
7 tablished by the owner of the model.

8 (C) Access that is provided via an applica-
9 tion program interface or another consumer-
10 facing, owner-controlled interface without ena-
11 bling third parties to obtain, modify, or host the
12 closed-source artificial intelligence model on
13 their own data servers or other technology un-
14 less specifically authorized by the owner of the
15 model.

16 (3) COUNTRY OF CONCERN.—The term “coun-
17 try of concern” means—

18 (A) the People’s Republic of China, includ-
19 ing the Hong Kong and Macau Special Admin-
20 istrative Regions;

21 (B) the Russian Federation; and

22 (C) any other foreign country—

23 (i) listed in Country Group D:5 in
24 Supplement No. 1 to part 740 of title 15,
25 Code of Federal Regulations, as published

1 on January 1, 2026, that is designated by
2 the Secretary of Commerce as a country of
3 concern for purposes of this section and
4 for which notice of such designation has
5 been published in the Federal Register;
6 and

7 (ii) identified by the Secretary of
8 Commerce, acting through the Under Sec-
9 retary of Commerce for Industry and Secu-
10 rity, pursuant to an assessment required
11 by subsection (a) or (e) of section 4.

12 (4) PERSON OF CONCERN.—The term “person
13 of concern” means any foreign person that—

14 (A) is located or headquartered in, or the
15 ultimate parent company of which is
16 headquartered in, a country of concern;

17 (B) is operating under the direction or
18 control of any entity located or headquartered
19 in, or the ultimate parent company of which is
20 headquartered in, a country of concern; or

21 (C) is conducting or attempting to conduct
22 a model extraction attack against closed-source
23 artificial intelligence models owned by United
24 States persons and outside of authorized model
25 training practices.

1 (5) FOREIGN PERSON.—The term “foreign per-
2 son” means a person that is not a United States
3 person.

4 (6) FRAUDULENT ACCOUNT NETWORK PRO-
5 VIDER.—

6 (A) IN GENERAL.—The term “fraudulent
7 account network provider” means any foreign
8 person that knowingly and intentionally creates,
9 obtains, maintains, sells, brokers, or otherwise
10 provides access to an account that allows a per-
11 son of concern to access a closed-source artifi-
12 cial intelligence model that the entity would
13 otherwise be prohibited from accessing as a re-
14 sult of location restrictions in the terms of serv-
15 ice or a contractual agreement created by the
16 owner of the model.

17 (B) EXCEPTION.—For purposes of sub-
18 paragraph (A), an entity that creates or trans-
19 mits location information to enable persons
20 within countries of concern to access the inter-
21 net for purposes of freedom of expression is
22 not, on the basis of that activity alone, a fraud-
23 ulent account network provider.

24 (7) MODEL EXTRACTION ATTACK.—

1 (A) IN GENERAL.—The term “model ex-
2 traction attack” means the unauthorized ex-
3 tracting of the capabilities of a closed-source ar-
4 tificial intelligence model to replicate, develop,
5 train, or improve another artificial intelligence
6 model, if such extraction—

7 (i) circumvents technical, contractual,
8 or other access controls, identity
9 verification requirements, or geographic ac-
10 cess restrictions implemented by the owner
11 of the model;

12 (ii) is conducted through fraudulent,
13 misrepresented, or unauthorized creden-
14 tials; or

15 (iii) violates the terms, conditions, or
16 restrictions governing access to or use of
17 the model, as established by the owner,
18 that specifically prohibit the use of model
19 outputs or interactions to replicate, de-
20 velop, train, or improve another artificial
21 intelligence model.

22 (B) INFERENCE OF PURPOSE.—For pur-
23 poses of subparagraph (A), the purpose of ex-
24 traction may be inferred from the totality of
25 circumstances, including—

1 (i) the volume, structure, pattern, co-
2 ordination, or timing of the extraction ac-
3 tivity;

4 (ii) the concentration of extractions on
5 specific model capabilities;

6 (iii) the use of multiple accounts in a
7 coordinated manner; or

8 (iv) the correlation of extraction activ-
9 ity within the development timeline of an-
10 other artificial intelligence model.

11 (C) EXCLUSION.—For purposes of sub-
12 paragraph (A), model training activities con-
13 ducted in compliance with the terms, conditions,
14 and restrictions governing access to and use of
15 a closed-source artificial intelligence model, or
16 otherwise conducted within a permitted excep-
17 tion or the express authorization of the owner
18 of the model, are not model extraction attacks.

19 (8) OPERATING COMMITTEE FOR EXPORT POL-
20 ICY.—The term “Operating Committee for Export
21 Policy” means the Operating Committee for Export
22 Policy referred to in section 1763(c) of the Export
23 Control Reform Act of 2018 (50 U.S.C. 4822(c)).

1 (9) OWNER.—The term “owner” means, with
2 respect to a closed-source artificial intelligence
3 model, the person that—

4 (A) holds intellectual property rights (in-
5 cluding trade secret, copyright, patent, or other
6 proprietary rights), contractual rights, or a
7 combination thereof, sufficient to authorize or
8 restrict third-party access to, use of, extraction
9 from, or reproduction of the model, or any
10 version, instance, or deployment the model,
11 whether such rights were obtained through de-
12 velopment, acquisition, assignment, license, or
13 otherwise; and

14 (B) is a United States person.

15 (10) PERSON.—The term “person” means indi-
16 vidual or entity.

17 (11) UNITED STATES PERSON.—The term
18 “United States person” means—

19 (A) a United States citizen or an alien law-
20 fully admitted for permanent residence to the
21 United States;

22 (B) an entity organized under the laws of
23 the United States or any jurisdiction within the
24 United States, including a foreign branch of
25 such an entity; or

1 (C) any person located in the United
2 States.

3 **SEC. 4. ASSESSMENT OF MODEL EXTRACTION ATTACKS**
4 **AND FRAUDULENT ACCOUNT NETWORK PRO-**
5 **VIDERS.**

6 (a) IN GENERAL.—Not later than 180 days after the
7 date of the enactment of this Act, the Secretary of Com-
8 merce, acting through the Under Secretary of Commerce
9 for Industry and Security and in coordination with the
10 head of each agency that is a member of the Operating
11 Committee for Export Policy, shall complete an assess-
12 ment to determine—

13 (1) which, if any, persons of concern have con-
14 ducted or are currently conducting model extraction
15 attacks against closed-source artificial intelligence
16 models owned by United States persons; and

17 (2) which, if any, persons of concern are fraud-
18 ulent account network providers.

19 (b) MATTERS TO BE INCLUDED.—The assessment
20 required by subsection (a) shall include the following:

21 (1) A determination of which persons of con-
22 cern—

23 (A) have either previously or are currently
24 engaging in model extraction attacks; or

1 (B) are fraudulent account network pro-
2 viders.

3 (2) A determination of the countries, if any—

4 (A) from which model extraction attacks
5 have originated; and

6 (B) in which fraudulent account network
7 providers exist.

8 (3) An identification of which, if any, agencies
9 or instrumentalities of governments of countries of
10 concern have provided or are providing material as-
11 sistance to entities identified pursuant to paragraph
12 (1).

13 (4) An analysis of the methods employed by
14 persons of concern identified pursuant to paragraph
15 (1), including—

16 (A) the role of fraudulent account network
17 providers in model extraction attacks, including,
18 to the extent possible, the physical location of
19 offices and data centers of such providers; and

20 (B) a determination, to the extent possible,
21 of the number of attempted model extraction
22 attacks that occurred during the 2 calendar
23 years preceding the date on which the Secretary
24 of Commerce, acting through the Under Sec-
25 retary of Commerce for Industry and Security,

1 begins the assessment required by subsection
2 (a).

3 (5) An examination of the strengths and weak-
4 nesses of various detection approaches that can be
5 used to determine whether a model extraction attack
6 has occurred or is occurring.

7 (6) An assessment of the economic and national
8 security consequences of successful model extraction
9 attacks by persons of concern that occurred during
10 the 2 calendar years preceding the date on which the
11 Secretary of Commerce, acting through the Under
12 Secretary of Commerce for Industry and Security,
13 begins the assessment required by subsection (a).

14 (7) Steps detailing how the United States Gov-
15 ernment is assisting owners of closed-source artifi-
16 cial intelligence models that have been the target or
17 victim of model extraction attacks in detecting model
18 extraction attacks, deterring future model extraction
19 attacks, and punishing persons of concern that en-
20 gage in model extraction attacks or are fraudulent
21 account network providers.

22 (8) A diplomatic strategy to leverage allies and
23 partners of the United States in detecting and pre-
24 venting model extraction attacks by persons of con-
25 cern.

1 (c) PUBLIC CONSULTATION.—

2 (1) IN GENERAL.—In conducting the assess-
3 ment required by subsection (a), the Secretary of
4 Commerce, acting through the Under Secretary of
5 Commerce for Industry and Security and in coordi-
6 nation with the head of each agency that is a mem-
7 ber of the Operating Committee for Export Policy,
8 shall consult with owners of closed-source artificial
9 intelligence models that have been the targets or vic-
10 tims of model extraction attacks, academic experts,
11 industry fora, and other appropriate entities—

12 (A) to identify patterns of behavior and
13 methods of attackers to better inform efforts of
14 the United States Government and the private
15 sector to detect model extraction attacks;

16 (B) to develop best practices for defending
17 against model extraction attacks; and

18 (C) to develop best practices for identifying
19 activities of fraudulent account network pro-
20 viders that facilitate model extraction attacks.

21 (2) VOLUNTARY PARTICIPATION.—The partici-
22 pation of owners of closed-source artificial intel-
23 ligence models described in paragraph (1) in con-
24 sultations under that paragraph shall be voluntary.

25 (d) REPORT.—

1 (1) IN GENERAL.—Not later than 210 days
2 after the date of the enactment of this Act, the Sec-
3 retary of Commerce, acting through the Under Sec-
4 retary of Commerce for Industry and Security and
5 in coordination with the head of each agency that is
6 a member of the Operating Committee for Export
7 Policy, shall submit to the appropriate congressional
8 committees a report that contains the findings of the
9 assessment required by subsection (a).

10 (2) UPDATES.—Not later than one year after
11 submitting the report required by paragraph (1),
12 and annually thereafter for 3 years, the Secretary of
13 Commerce, acting through the Under Secretary of
14 Commerce for Industry and Security, shall submit to
15 the appropriate congressional committees an update
16 to the report listing any additional persons of con-
17 cern identified pursuant to subsection (a).

18 (3) FORM.—The report required by paragraph
19 (1), and each update required by paragraph (2),
20 shall be submitted in unclassified form, but may
21 contain a classified annex.

22 (e) ROUTINE ASSESSMENT.—The Secretary of Com-
23 merce, acting through the Under Secretary of Commerce
24 for Industry and Security and in coordination with the

1 head of each agency that is a member of the Operating
2 Committee for Export Policy, shall routinely assess for—

3 (1) model extraction attacks directed against
4 owners of closed-source artificial intelligence models
5 that occur after the date of completion of the assess-
6 ment required by subsection (a);

7 (2) fraudulent account network providers that
8 facilitate model extraction attacks after that date;
9 and

10 (3) any material changes related to other mat-
11 ters specified in subsection (b).

12 (f) INDUSTRY COORDINATION.—The Secretary of
13 Commerce, acting through the Under Secretary of Com-
14 merce for Industry and Security and in coordination with
15 the head of each agency that is a member of the Operating
16 Committee for Export Policy, shall establish an informa-
17 tion-sharing mechanism that allows owners of closed-
18 source artificial intelligence models to voluntarily, quickly,
19 and confidentially share information about model extrac-
20 tion attacks and fraudulent account network providers
21 with the Department of Commerce.

22 (g) AI MODEL EXTRACTION ATTACKERS LIST.—

23 (1) IN GENERAL.—The Secretary of Commerce,
24 acting through the Under Secretary of Commerce
25 for Industry and Security and in coordination with

1 the head of each agency that is a member of the Op-
2 erating Committee for Export Policy, shall—

3 (A) maintain a list, to be known as the
4 “AI Model Extraction Attackers List”, that dis-
5 plays information about specific persons of con-
6 cern identified pursuant to an assessment re-
7 quired by subsection (a) or (e) as having con-
8 ducted or directed model extraction attacks in
9 the past year; and

10 (B) publish the list on a publicly available
11 website of the Department of Commerce.

12 (2) PROTECTION OF CONFIDENTIAL INFORMA-
13 TION.—The Secretary of Commerce, acting through
14 the Under Secretary of Commerce for Industry and
15 Security, may not, in publishing the list required by
16 paragraph (1) on a publicly available website of the
17 Department of Commerce, disclose confidential in-
18 formation provided by the owner of a closed-source
19 artificial intelligence model without the express per-
20 mission of the owner.

21 (h) PUBLIC GUIDANCE.—

22 (1) IN GENERAL.—Not later than 210 days
23 after the date of the enactment of this Act, the Sec-
24 retary of Commerce, acting through the Under Sec-
25 retary of Commerce for Industry and Security and

1 in coordination with the head of each agency that is
2 a member of the Operating Committee for Export
3 Policy, shall publish a report comprising of best
4 practices to detect, prevent, and respond to model
5 extraction attacks.

6 (2) PUBLIC ACCESS.—The report required by
7 paragraph (1) shall be publicly available.

8 (3) PROTECTION OF CONFIDENTIAL INFORMA-
9 TION.—In making the report required by paragraph
10 (1) publicly available, the Secretary may not disclose
11 confidential information provided by the owner of a
12 closed-source artificial intelligence model without the
13 express permission of the owner.

14 **SEC. 5. DETERRING MODEL EXTRACTION ATTACKS AND**
15 **FRAUDULENT ACCOUNT NETWORK PRO-**
16 **VIDERS.**

17 (a) CONSIDERATION OF ADDITION TO ENTITY
18 LIST.—

19 (1) IN GENERAL.—Not later than 210 days
20 after the date of the enactment of this Act, the
21 Under Secretary of Commerce for Industry and Se-
22 curity, in coordination with the head of each agency
23 that is a member of the End-User Review Com-
24 mittee, shall add each entity described in paragraph
25 (2) to the Entity List maintained by the Bureau of

1 Industry and Security and set forth in Supplement
2 No. 4 to part 744 of title 15, Code of Federal Regu-
3 lations, or any successor regulations.

4 (2) ENTITIES DESCRIBED.—An entity described
5 in this paragraph is—

6 (A) an entity that is a person of concern
7 identified, under subsection (a) or (e) of section
8 4, as having conducted model extraction attacks
9 or having facilitated such attacks via fraudulent
10 account networks; or

11 (B) a subsidiary of such an entity (to be
12 determined by ownership of 50 percent or more
13 in the aggregate, directly or indirectly).

14 (b) IMPOSITION OF SANCTIONS.—

15 (1) IN GENERAL.—The President shall, pursu-
16 ant to the International Emergency Economic Pow-
17 ers Act (50 U.S.C. 1701 et seq.), block and prohibit
18 all transactions in all property and interests in prop-
19 erty of each person of concern identified under sub-
20 sections (a) and (e) of section 4 if such property and
21 interests in property are in the United States, come
22 within the United States, or are or come within the
23 possession or control of a United States person.

24 (2) EXCEPTIONS.—

1 (A) EXCEPTION RELATING TO THE PROVI-
2 SION OF HUMANITARIAN ASSISTANCE.—Sanctions under paragraph (1) may not be imposed
3 with respect to transactions or the facilitation
4 of transactions for—
5

6 (i) the sale of agricultural commod-
7 ities, food, medicine, or medical devices;

8 (ii) the provision of humanitarian as-
9 sistance; or

10 (iii) transporting goods or services
11 that are necessary to carry out operations
12 relating to humanitarian assistance.

13 (B) EXCEPTION FOR INTELLIGENCE, LAW
14 ENFORCEMENT, AND NATIONAL SECURITY AC-
15 TIVITIES.—Sanctions under this subsection
16 shall not apply to any authorized intelligence,
17 law enforcement, or national security activities
18 of the United States.

19 (3) WAIVER.—

20 (A) IN GENERAL.—The President may,
21 subject to subparagraph (B), waive the applica-
22 tion of subsection (a) or (b) with respect to a
23 person if, before issuing the waiver, the Presi-
24 dent submits to Congress—

1 (i) a certification in writing that the
2 issuance of the waiver is in the national in-
3 terests of the United States; and

4 (ii) a report explaining the basis for
5 the certification.

6 (B) FORM OF REPORT.—Each report re-
7 quired by subparagraph (A) shall be submitted
8 in unclassified form but may include a classified
9 annex.

10 (4) PENALTIES.—A person that violates, at-
11 tempts to violate, conspires to violate, or causes a
12 violation of this subsection or any regulation, license,
13 or order issued to carry out that subsection shall be
14 subject to the penalties set forth in subsections (b)
15 and (c) of section 206 of the International Emer-
16 gency Economic Powers Act (50 U.S.C. 1705) to the
17 same extent as a person that commits an unlawful
18 act described in subsection (a) of that section.