

119<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# H. R. 8283

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

---

## IN THE HOUSE OF REPRESENTATIVES

APRIL 15, 2026

Mr. HUIZENGA (for himself and Mr. MOOLENAAR) introduced the following bill; which was referred to the Committee on Foreign Affairs

---

## A BILL

To prevent foreign adversaries from threatening the national security of the United States by extracting key technical features of closed-source, American-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 “Deterring American AI  
5        Model Theft Act of 2026”.

6        **SEC. 2. SENSE OF CONGRESS.**

7        It is the sense of Congress that—

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

5           (2) many of the most advanced AI models  
6           owned by United States companies are “closed-  
7           source models” whose unique technical characteris-  
8           tics 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          AI models by entities of concern through model ex-  
13          traction attacks represents a threat to the national  
14          security and foreign policy interests of the United  
15          States, as well as the intellectual property rights and  
16          economic competitiveness of United States compa-  
17          nies;

18          (4) the United States Government, in coopera-  
19          tion with private owners of closed-source AI models,  
20          should take steps to identify, punish, and deter  
21          model extraction attacks on the protected capabili-  
22          ties of closed-source models by entities of concern;

23          (5) model extraction attacks against American  
24          closed-source AI models allow foreign adversaries a  
25          short cut to acquiring advanced AI capabilities; and

1           (6) authorized model training practices that ad-  
2 here to the terms of service or are otherwise con-  
3 sistent with contractual terms set by the owners of  
4 closed-source AI models are a legitimate research  
5 method that play an important role in AI research  
6 and are fundamentally distinct from model extrac-  
7 tion attacks defined in this Act.

8 **SEC. 3. DEFINITIONS.**

9 In this Act:

10           (1) **APPROPRIATE CONGRESSIONAL COMMIT-**  
11 **TEES.**—The term “appropriate congressional com-  
12 mittees” means—

13           (A) the Committee on Foreign Affairs of  
14 the House of Representatives; and

15           (B) the Committee on Banking, Housing,  
16 and Urban Affairs in the Senate.

17           (2) **CLOSED-SOURCE AI MODEL.**—The term  
18 “closed-source AI model” means any artificial intel-  
19 ligence model with the following characteristics:

20           (A) Proprietary key technical information  
21 such as underlying model weights that are nec-  
22 essary to reproduce and independently recreate  
23 the model that are not willingly shared with  
24 third parties or otherwise made publicly avail-  
25 able by the owner of the model.

1 (B) Access and use governed by terms of  
2 service or contractual agreements that are es-  
3 tablished by the owner of the model.

4 (C) Access that is provided via an Applica-  
5 tion Program Interface (API) or other con-  
6 sumer-facing, owner-controlled interfaces with-  
7 out enabling third parties to obtain, modify, or  
8 host the closed-source AI model on their own  
9 data servers or other technology unless specifi-  
10 cally authorized by the owner of the closed-  
11 source AI model.

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

14 (A) the People’s Republic of China, includ-  
15 ing the Hong Kong and Macau Special Admin-  
16 istrative Regions;

17 (B) the Russian Federation; and

18 (C) any other foreign country—

19 (i) listed in Country Group D:5 under  
20 Supplement No. 1 to part 740 of the Ex-  
21 port Administration Regulations, as pub-  
22 lished on January 1, 2026, that is des-  
23 ignated by the Secretary of State as a  
24 country of concern for purposes of this sec-  
25 tion and for which notice of such designa-

1           tion has been published in the Federal  
2           Register; and

3                   (ii) designated by the Secretary of  
4           State pursuant to the assessment described  
5           in subsection (b) or (e) of section 4 of this  
6           Act.

7           (4) ENTITY OF CONCERN.—The term “entity of  
8           concern” means any foreign person or entity that—

9                   (A) is located or headquartered in, or the  
10          ultimate parent company of which is  
11          headquartered in, a country of concern;

12                   (B) is operating under the direction or  
13          control of any entity located or headquartered  
14          in, or the ultimate parent company of which is  
15          headquartered in, a country of concern; or

16                   (C) is conducting or attempting to conduct  
17          a model extraction attack against closed-source  
18          AI models owned by United States persons and  
19          outside of authorized model training practices.

20           (5) EXPORT.—The term “export” has the  
21          meaning given that term in section 1742(3) of the  
22          Export Control Reform Act of 2018 (50 U.S.C.  
23          4801(3)).

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

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

6                   (A) IN GENERAL.—The term “fraudulent  
7                   account network provider” means any foreign  
8                   entity that knowingly and intentionally creates,  
9                   obtains, maintains, sells, brokers, or otherwise  
10                  provides access to accounts that allow entities  
11                  of concern to access closed-source AI models  
12                  that they would otherwise be prohibited from  
13                  accessing due to location restrictions in the  
14                  terms of service or contractual agreements cre-  
15                  ated by the owner of the closed-source AI  
16                  model.

17                   (B) EXCEPTION.—An entity that creates  
18                   or transmits location information to enable per-  
19                   sons within countries of concern to access the  
20                   internet for purposes of freedom of expression  
21                   is not considered, on the basis of this activity  
22                   alone, a fraudulent account network provider.

23           (8) GOOD.—The term “good” has the meaning  
24           given that term in section 16 of the Export Adminis-  
25           tration Act of 1979 (50 U.S.C. App. 2415)(as con-

1       tinued in effect pursuant to the International Emer-  
2       gency Economic Powers Act (50 U.S.C. 1701 et  
3       seq.)).

4           (9) IN-COUNTRY TRANSFER.—The term “in-  
5       country transfer” has the meaning given that term  
6       in section 1742(6) of the Export Control Reform Act  
7       of 2018 (50 U.S.C. 4801(6)).

8           (10) ITEM.—The term “item” has the meaning  
9       given that term in section 1742(7) of the Export  
10       Control Reform Act of 2018 (50 U.S.C. 4801(7)).

11          (11) MODEL EXTRACTION ATTACK.—

12           (A) IN GENERAL.—The term “model ex-  
13       traction attack” means the unauthorized ex-  
14       tracting of a closed-source AI model’s capabili-  
15       ties to replicate, develop, train, or improve an-  
16       other AI model, where such querying—

17                   (i) circumvents technical, contractual,  
18                   or other access controls, identity  
19                   verification requirements, or geographic ac-  
20                   cess restrictions implemented by the mod-  
21                   el’s owner;

22                   (ii) is conducted through fraudulent,  
23                   misrepresented, or unauthorized creden-  
24                   tials; or

1 (iii) violates the terms, conditions, or  
2 restrictions governing access to or use of  
3 the model, as established by the owner or  
4 authorized provider, that specifically pro-  
5 hibit the use of model outputs or inter-  
6 actions to replicate, develop, train, or im-  
7 prove another AI model.

8 (B) INFERENCE OF PURPOSE.—For pur-  
9 poses of subparagraph (A), the purpose of  
10 querying may be inferred from the totality of  
11 circumstances, including—

12 (i) the volume, structure, pattern, co-  
13 ordination, or timing of the querying activ-  
14 ity;

15 (ii) the concentration of queries on  
16 specific model capabilities;

17 (iii) the use of multiple accounts in a  
18 coordinated matter; or

19 (iv) the correlation of querying activ-  
20 ity within the development timeline of an-  
21 other AI model.

22 (C) EXCLUSION.—Model training activities  
23 conducted in compliance with the terms, condi-  
24 tions, and restrictions governing access to and  
25 use of the closed-source AI model, or otherwise

1 conducted within a permitted exception or the  
2 express authorization of the owner of the  
3 closed-source AI model, are not model extrac-  
4 tion attacks.

5 (12) OPERATING COMMITTEE FOR EXPORT POL-  
6 ICY.—The term “Operating Committee for Export  
7 Policy” means the Operating Committee for Export  
8 Policy referred to in section 1763(c) of the Export  
9 Control Reform Act of 2018 (50 U.S.C. 4822(c)).

10 (13) OWNER.—The term “owner” means, with  
11 respect to a closed-source AI model, the person or  
12 entity that—

13 (A) holds intellectual property rights (in-  
14 cluding trade secret, copyright, patent, or other  
15 proprietary rights), contractual rights, or a  
16 combination thereof, sufficient to authorize or  
17 restrict third-party access to, use of, extraction  
18 from, or reproduction of such closed-source AI  
19 model, or any version, instance, or deployment  
20 thereof, whether such rights were obtained  
21 through development, acquisition, assignment,  
22 license, or otherwise; and

23 (B) is a United States person.

24 (14) REEXPORT.—The term “reexport” has the  
25 meaning given that term in section 1742(9) of the

1 Export Control Reform Act of 2018 (50 U.S.C.  
2 4801(9)).

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 State,  
8 in coordination with each agency that is a member of the  
9 Operating Committee for Export Policy, shall complete an  
10 assessment to determine—

11 (1) which, if any, entities of concern have con-  
12 ducted or are currently conducting model extraction  
13 attacks against closed-source AI models owned by  
14 United States entities; and

15 (2) which, if any, entities of concern are fraud-  
16 ulent account network providers.

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

19 (1) A determination of which entities of con-  
20 cern—

21 (A) have either previously or are currently  
22 engaging in model extraction attacks; or

23 (B) are fraudulent account network pro-  
24 viders.

1           (2) A determination of which, if any, countries  
2           model extraction attacks have originated from and  
3           where fraudulent account network providers exist.

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

9           (4) An analysis of the methods employed by en-  
10          tities of concern identified pursuant to paragraph  
11          (1), including—

12                   (A) the role of fraudulent account network  
13                   providers in model extraction attacks, including,  
14                   to the extent possible, the physical location of  
15                   fraudulent account network provider offices and  
16                   data centers; and

17                   (B) a determination, to the extent possible,  
18                   of the number of attempted model extraction  
19                   attacks that occurred in the previous two cal-  
20                   endar years from the date on which the Sec-  
21                   retary of State begins the assessment pursuant  
22                   to subsection (a)(1).

23          (5) An examination of the strengths and weak-  
24          nesses of various detection approaches that can be

1 used to determine whether a model extraction attack  
2 has occurred or is occurring.

3 (6) An assessment of the economic and national  
4 security consequences of successful model extraction  
5 attacks by entities of concern that occurred in the  
6 previous two calendar years from the date on which  
7 the Secretary of State begins the assessment pursu-  
8 ant to subsection (a)(1).

9 (7) Steps detailing how the United States Gov-  
10 ernment is assisting owners of closed-source AI mod-  
11 els that have been the target or victim of model ex-  
12 traction attacks in detecting model extraction at-  
13 tacks, deterring future model extraction attacks, and  
14 punishing entities of concern that engage in model  
15 extraction attacks or are fraudulent account network  
16 providers.

17 (8) A diplomatic strategy to leverage United  
18 States allies and partners in detecting and pre-  
19 venting model extraction attacks by entities of con-  
20 cern.

21 (c) PUBLIC CONSULTATION.—In conducting the as-  
22 sessment required by subsection (a), the Secretary of  
23 Commerce, in coordination with each agency that is a  
24 member of the Operating Committee for Export Policy,  
25 shall consult with owners of closed-source AI models that

1 have been the targets or victims of model extraction at-  
2 tacks, whose participation in this consultation shall be vol-  
3 untary, other companies, academic experts, industry fora,  
4 and other appropriate entities to—

5 (1) identify patterns of attacker behavior and  
6 methods to better inform United States Government  
7 and private sector efforts to detect model extraction  
8 attacks;

9 (2) develop best practices for defending against  
10 model extraction attacks; and

11 (3) develop best practices for identifying fraud-  
12 ulent account network provider activities that facili-  
13 tate model extraction attacks.

14 (d) REPORT.—

15 (1) IN GENERAL.—Not later than 210 days  
16 after the date of the enactment of this Act, the Sec-  
17 retary of Commerce, in coordination with each agen-  
18 cy that is a member of the Operating Committee for  
19 Export Policy, shall submit to the appropriate con-  
20 gressional committees a report that contains the  
21 findings of the assessment. The Secretary of Com-  
22 merce shall, annually for 3 years, submit to the ap-  
23 propriate congressional committees an updated re-  
24 port with any additional entities of concern identi-  
25 fied pursuant to subsection (b)(1).

1           (2) FORM.—The report required by this sub-  
2           section shall be submitted in unclassified form, but  
3           may contain a classified annex.

4           (e) ROUTINE ASSESSMENT.—The Secretary of Com-  
5           merce, in coordination with each agency that is a member  
6           of the Operating Committee for Export Policy, shall rou-  
7           tinely assess for—

8           (1) model extraction attacks directed against  
9           owners of closed-source AI models that occur after  
10          the date of completion of the assessment required by  
11          this section;

12          (2) fraudulent account network providers that  
13          facilitate model extraction attacks after the date of  
14          completion of the assessment required by this sec-  
15          tion; and

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

18          (f) INDUSTRY COORDINATION.—The Secretary of  
19          Commerce, in coordination with each agency that is a  
20          member of the Operating Committee for Export Policy,  
21          shall establish an information sharing mechanism that al-  
22          lows owners of closed-source AI models to voluntarily,  
23          quickly, and confidentially share information about model  
24          extraction attacks and fraudulent account network pro-  
25          viders with the Department of Commerce.

1 (g) AI MODEL EXTRACTION ATTACKERS LIST.—

2 (1) IN GENERAL.—The Secretary of State, in  
3 coordination with each agency that is a member of  
4 the Operating Committee for Export Policy, shall—

5 (A) maintain a list, to be known as the  
6 “AI Model Extraction Attackers List”, that dis-  
7 plays information about specific individuals and  
8 entities of concern, that the assessment re-  
9 quired by subsection (a) and routine assessment  
10 described in subsection (e) identify as having  
11 conducted or directed model extraction attacks  
12 in the past year; and

13 (B) publish such list on a publicly available  
14 website of the Department of State for up to 5  
15 years.

16 (2) PROTECTION OF CONFIDENTIAL INFORMA-  
17 TION.—The Secretary of State may not, in pub-  
18 lishing the list required by paragraph (1) on a pub-  
19 licly available website of the Department of State,  
20 disclose confidential information provided by owners  
21 of closed-source AI models without the express per-  
22 mission of said owner.

23 (h) PUBLIC GUIDANCE.—Not later than 210 days  
24 after the date of the enactment of this Act, the Secretary  
25 of Commerce, in coordination with each agency that is a

1 member of the Operating Committee for Export Policy,  
2 shall publish a report comprising of best practices to de-  
3 tect, prevent, and respond to model extraction attacks.

4 (1) PUBLIC ACCESS.—The report required by  
5 this subsection shall be publicly available.

6 (2) PROTECTION OF CONFIDENTIAL INFORMA-  
7 TION.—In making the report required by this sub-  
8 section publicly available, the Secretary of Com-  
9 merce, in coordination with each agency that is a  
10 member of the Operating Committee for Export Pol-  
11 icy, shall not disclose confidential information pro-  
12 vided by owners of closed-source AI models without  
13 the express permission of said owner.

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

17 (a) ADDITION CONSIDERATION FOR ENTITY LIST.—  
18 Not later than 210 days after the date of the enactment  
19 of this Act, the Under Secretary of Commerce for Industry  
20 and Security, in coordination with each agency that is a  
21 member of the End-User Review Committee, shall make  
22 a determination by majority vote of the Committee on  
23 whether entities identified as having conducted model ex-  
24 traction attacks or having facilitated them via fraudulent  
25 account networks after the date of the completion of the

1 assessment required under section 4 of this Act (identified  
2 pursuant to subsection (e) of such section), or any affiliate  
3 of such entity (to be determined by ownership of 50 per-  
4 cent or more in the aggregate, directly or indirectly),  
5 should be added to the Entity List maintained by the Bu-  
6 reau of Industry and Security of the Department of Com-  
7 merce under Supplement No. 4 to part 744 of title 15,  
8 Code of Federal Regulations, or any successor regulations.

9 (b) SANCTIONS DESCRIBED.—

10 (1) IN GENERAL.—The President, acting  
11 through the Secretary of State, may, pursuant to  
12 the International Emergency Economic Powers Act  
13 (50 U.S.C. 1701 et seq.), block and prohibit all  
14 transactions in all property and interests in property  
15 of entities of concern identified pursuant to sub-  
16 sections (b)(1) and (e) of section 4 if such property  
17 and interests in property are in the United States,  
18 come within the United States, or are or come with-  
19 in the possession or control of a United States per-  
20 son.

21 (2) EXCEPTIONS.—

22 (A) EXCEPTION TO COMPLY WITH INTER-  
23 NATIONAL OBLIGATIONS.—Sanctions under this  
24 subsection shall not apply with respect to the  
25 admission of an alien if admitting or paroling

1 the alien into the United States is necessary to  
2 permit the United States to comply with the  
3 Agreement regarding the Headquarters of the  
4 United Nations, signed at Lake Success June  
5 26, 1947, and entered into force November 21,  
6 1947, between the United Nations and the  
7 United States, or other applicable international  
8 obligations.

9 (B) EXCEPTION RELATING TO THE PROVI-  
10 SION OF HUMANITARIAN ASSISTANCE.—Sanctions  
11 under this subsection may not be imposed  
12 with respect to transactions or the facilitation  
13 of transactions for—

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

16 (ii) the provision of humanitarian as-  
17 sistance;

18 (iii) financial transactions relating to  
19 humanitarian assistance; or

20 (iv) transporting goods or services  
21 that are necessary to carry out operations  
22 relating to humanitarian assistance.

23 (C) EXCEPTION FOR INTELLIGENCE, LAW  
24 ENFORCEMENT, AND NATIONAL SECURITY AC-  
25 TIVITIES.—Sanctions under this subsection

1           shall not apply to any authorized intelligence,  
2           law enforcement, or national security activities  
3           of the United States.

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

○