

**AMENDMENT TO**  
**RULES COMMITTEE PRINT 119-33**  
**OFFERED BY MR. HUIZENGA OF MICHIGAN**

Add at the end the following:

1 **DIVISION E—DETECTING AMER-**  
2 **ICAN AI MODEL THEFT ACT**  
3 **OF 2026**

4 **SEC. 5001. SHORT TITLE.**

5 This division may be cited as “Detecting American  
6 AI Model Theft Act of 2026”.

7 **SEC. 5002. SENSE OF CONGRESS.**

8 It is the sense of Congress that—

9 (1) artificial intelligence (AI) models owned by  
10 United States private sector companies are essential  
11 for advancing United States economic and national  
12 security interests;

13 (2) many of the most advanced AI models  
14 owned by United States companies are “closed-  
15 source models” whose unique technical characteris-  
16 tics are not openly shared or published;

17 (3) the unauthorized acquisition of model capa-  
18 bilities, such as model weights, model architectures,  
19 and other technical characteristics of closed-source

1 AI models by entities of concern through model ex-  
2 traction attacks represents a threat to the national  
3 security and foreign policy interests of the United  
4 States, as well as the intellectual property rights and  
5 economic competitiveness of United States compa-  
6 nies;

7 (4) the United States Government, in coopera-  
8 tion with private owners of closed-source AI models,  
9 should take steps to identify, punish, and deter  
10 model extraction attacks on the protected capabili-  
11 ties of closed-source models by entities of concern;

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

15 (6) authorized model training practices that ad-  
16 here to the terms of service or are otherwise con-  
17 sistent with contractual terms set by the owners of  
18 closed-source AI models are a legitimate research  
19 method that play an important role in AI research  
20 and are fundamentally distinct from model extrac-  
21 tion attacks defined in this Act.

22 **SEC. 5003. DEFINITIONS.**

23 In this division:

1           (1) APPROPRIATE CONGRESSIONAL COMMIT-  
2           TEES.—The term “appropriate congressional com-  
3           mittees” means—

4                   (A) the Committee on Foreign Affairs of  
5                   the House of Representatives; and

6                   (B) the Committee on Banking, Housing,  
7                   and Urban Affairs in the Senate.

8           (2) CLOSED-SOURCE AI MODEL.—The term  
9           “closed-source AI model” means any artificial intel-  
10          ligence model with the following characteristics:

11                   (A) Proprietary key technical information  
12                   such as underlying model weights that are nec-  
13                   essary to reproduce and independently recreate  
14                   the model that are not willingly shared with  
15                   third parties or otherwise made publicly avail-  
16                   able by the owner of the model.

17                   (B) Access and use governed by terms of  
18                   service or contractual agreements that are es-  
19                   tablished by the owner of the model.

20                   (C) Access that is provided via an Applica-  
21                   tion Program Interface (API) or other con-  
22                   sumer-facing, owner-controlled interfaces with-  
23                   out enabling third parties to obtain, modify, or  
24                   host the closed-source AI model on their own  
25                   data servers or other technology unless specifi-

1 cally authorized by the owner of the closed-  
2 source AI model.

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

5 (A) the People’s Republic of China, includ-  
6 ing the Hong Kong and Macau Special Admin-  
7 istrative Regions;

8 (B) the Russian Federation; and

9 (C) any other foreign country—

10 (i) listed in Country Group D:5 under  
11 Supplement No. 1 to part 740 of the Ex-  
12 port Administration Regulations, as pub-  
13 lished on January 1, 2026, that is des-  
14 ignated by the Secretary of Commerce as  
15 a country of concern for purposes of this  
16 section and for which notice of such des-  
17 ignation has been published in the Federal  
18 Register; and

19 (ii) designated by the Secretary of  
20 Commerce pursuant to the assessment de-  
21 scribed in subsection (b) or (e) of section  
22 5004 of this Act.

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

1 (A) is located or headquartered in, or the  
2 ultimate parent company of which is  
3 headquartered in, a country of concern;

4 (B) is operating under the direction or  
5 control of any entity located or headquartered  
6 in, or the ultimate parent company of which is  
7 headquartered in, a country of concern; or

8 (C) is conducting or attempting to conduct  
9 a model extraction attack against closed-source  
10 AI models owned by United States persons and  
11 outside of authorized model training practices.

12 (5) EXPORT.—The term “export” has the  
13 meaning given that term in section 1742(3) of the  
14 Export Control Reform Act of 2018 (50 U.S.C.  
15 4801(3)).

16 (6) FOREIGN PERSON.—The term “foreign per-  
17 son” means a person that is not a United States  
18 person.

19 (7) FRAUDULENT ACCOUNT NETWORK PRO-  
20 VIDER.—

21 (A) IN GENERAL.—The term “fraudulent  
22 account network provider” means any foreign  
23 entity that knowingly and intentionally creates,  
24 obtains, maintains, sells, brokers, or otherwise  
25 provides access to accounts that allow entities

1 of concern to access closed-source AI models  
2 that they would otherwise be prohibited from  
3 accessing due to location restrictions in the  
4 terms of service or contractual agreements cre-  
5 ated by the owner of the closed-source AI  
6 model.

7 (B) EXCEPTION.—An entity that creates  
8 or transmits location information to enable per-  
9 sons within countries of concern to access the  
10 internet for purposes of freedom of expression  
11 is not considered, on the basis of this activity  
12 alone, a fraudulent account network provider.

13 (8) GOOD.—The term “good” has the meaning  
14 given that term in section 16 of the Export Adminis-  
15 tration Act of 1979 (50 U.S.C. App. 2415)(as con-  
16 tinued in effect pursuant to the International Emer-  
17 gency Economic Powers Act (50 U.S.C. 1701 et  
18 seq.)).

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

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

1 (11) MODEL EXTRACTION ATTACK.—

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

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

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 or  
18 authorized provider, that specifically pro-  
19 hibit the use of model outputs or inter-  
20 actions to replicate, develop, train, or im-  
21 prove another AI model.

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

1 (i) the volume, structure, pattern, co-  
2 ordination, or timing of the querying activ-  
3 ity;

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

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

8 (iv) the correlation of querying activ-  
9 ity within the development timeline of an-  
10 other AI model.

11 (C) EXCLUSION.—Model training activities  
12 conducted in compliance with the terms, condi-  
13 tions, and restrictions governing access to and  
14 use of the closed-source AI model, or otherwise  
15 conducted within a permitted exception or the  
16 express authorization of the owner of the  
17 closed-source AI model, are not model extrac-  
18 tion attacks.

19 (12) 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 (13) OWNER.—The term “owner” means, with  
2 respect to a closed-source AI model, the person or  
3 entity 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 such closed-source AI  
10 model, or any version, instance, or deployment  
11 thereof, whether such rights were obtained  
12 through development, acquisition, assignment,  
13 license, or otherwise; and

14 (B) is a United States person.

15 (14) REEXPORT.—The term “reexport” has the  
16 meaning given that term in section 1742(9) of the  
17 Export Control Reform Act of 2018 (50 U.S.C.  
18 4801(9)).

19 **SEC. 5004. ASSESSMENT OF MODEL EXTRACTION ATTACKS**  
20 **AND FRAUDULENT ACCOUNT NETWORK PRO-**  
21 **VIDERS.**

22 (a) IN GENERAL.—Not later than 180 days after the  
23 date of the enactment of this Act, the Secretary of Com-  
24 merce, in coordination with each agency that is a member

1 of the Operating Committee for Export Policy, shall com-  
2 plete an assessment to determine—

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

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

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

11 (1) A determination of which entities of con-  
12 cern—

13 (A) have either previously or are currently  
14 engaging in model extraction attacks; or

15 (B) are fraudulent account network pro-  
16 viders.

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

20 (3) An identification of which, if any, agencies  
21 or instrumentalities of governments of countries of  
22 concern have provided or are providing material as-  
23 sistance to entities identified pursuant to paragraph  
24 (1).

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

4                   (A) the role of fraudulent account network  
5                   providers in model extraction attacks, including,  
6                   to the extent possible, the physical location of  
7                   fraudulent account network provider offices and  
8                   data centers; and

9                   (B) a determination, to the extent possible,  
10                  of the number of attempted model extraction  
11                  attacks that occurred in the previous two cal-  
12                  endar years from the date on which the Sec-  
13                  retary of Commerce begins the assessment pur-  
14                  suant to subsection (a)(1).

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

19           (6) An assessment of the economic and national  
20           security consequences of successful model extraction  
21           attacks by entities of concern that occurred in the  
22           previous two calendar years from the date on which  
23           the Secretary of Commerce begins the assessment  
24           pursuant to subsection (a)(1).

1           (7) Steps detailing how the United States Gov-  
2           ernment is assisting owners of closed-source AI mod-  
3           els that have been the target or victim of model ex-  
4           traction attacks in detecting model extraction at-  
5           tacks, deterring future model extraction attacks, and  
6           punishing entities of concern that engage in model  
7           extraction attacks or are fraudulent account network  
8           providers.

9           (8) A diplomatic strategy to leverage United  
10          States allies and partners in detecting and pre-  
11          venting model extraction attacks by entities of con-  
12          cern.

13          (c) PUBLIC CONSULTATION.—In conducting the as-  
14          sessment required by subsection (a), the Secretary of  
15          Commerce, in coordination with each agency that is a  
16          member of the Operating Committee for Export Policy,  
17          shall consult with owners of closed-source AI models that  
18          have been the targets or victims of model extraction at-  
19          tacks, whose participation in this consultation shall be vol-  
20          untary, other companies, academic experts, industry fora,  
21          and other appropriate entities to—

22                (1) identify patterns of attacker behavior and  
23                methods to better inform United States Government  
24                and private sector efforts to detect model extraction  
25                attacks;

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

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

6       (d) REPORT.—

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

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

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

1 (1) model extraction attacks directed against  
2 owners of closed-source AI models that occur after  
3 the date of completion of the assessment required by  
4 this section;

5 (2) fraudulent account network providers that  
6 facilitate model extraction attacks after the date of  
7 completion of the assessment required by this sec-  
8 tion; and

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

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

19 (g) AI MODEL EXTRACTION ATTACKERS LIST.—

20 (1) IN GENERAL.—The Secretary of Commerce,  
21 in coordination with each agency that is a member  
22 of the Operating Committee for Export Policy,  
23 shall—

24 (A) maintain a list, to be known as the  
25 “AI Model Extraction Attackers List”, that dis-

1 plays information about specific individuals and  
2 entities of concern, that the assessment re-  
3 quired by subsection (a) and routine assessment  
4 described in subsection (e) identify as having  
5 conducted or directed model extraction attacks  
6 in the past year; and

7 (B) publish such list on a publicly available  
8 website of the Department of Commerce for up  
9 to 5 years.

10 (2) PROTECTION OF CONFIDENTIAL INFORMA-  
11 TION.—The Secretary of Commerce may not, in  
12 publishing the list required by paragraph (1) on a  
13 publicly available website of the Department of Com-  
14 merce, disclose confidential information provided by  
15 owners of closed-source AI models without the ex-  
16 press permission of said owner.

17 (h) PUBLIC GUIDANCE.—Not later than 210 days  
18 after the date of the enactment of this Act, the Secretary  
19 of Commerce, in coordination with each agency that is a  
20 member of the Operating Committee for Export Policy,  
21 shall publish a report comprising of best practices to de-  
22 tect, prevent, and respond to model extraction attacks.

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

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

9   **SEC. 5005. DETERRING MODEL EXTRACTION ATTACKS AND**  
10                   **FRAUDULENT ACCOUNT NETWORK PRO-**  
11                   **VIDERS.**

12           (a) ADDITION CONSIDERATION FOR ENTITY LIST.—  
13           Not later than 210 days after the date of the enactment  
14           of this Act, the Under Secretary of Commerce for Industry  
15           and Security, in coordination with each agency that is a  
16           member of the End-User Review Committee, shall make  
17           a determination by majority vote of the Committee on  
18           whether entities identified as having conducted model ex-  
19           traction attacks or having facilitated them via fraudulent  
20           account networks after the date of the completion of the  
21           assessment required under section 5004 of this Act (iden-  
22           tified pursuant to subsection (e) of such section), or any  
23           affiliate of such entity (to be determined by ownership of  
24           50 percent or more in the aggregate, directly or indi-  
25           rectly), should be added to the Entity List maintained by

1 the Bureau of Industry and Security of the Department  
2 of Commerce under Supplement No. 4 to part 744 of title  
3 15, Code of Federal Regulations, or any successor regula-  
4 tions.

5 (b) SANCTIONS DESCRIBED.—

6 (1) IN GENERAL.—The President may, pursu-  
7 ant to the International Emergency Economic Pow-  
8 ers Act (50 U.S.C. 1701 et seq.), block and prohibit  
9 all transactions in all property and interests in prop-  
10 erty of entities of concern identified pursuant to sub-  
11 sections (b)(1) and (e) of section 5004 if such prop-  
12 erty and interests in property are in the United  
13 States, come within the United States, or are or  
14 come within the possession or control of a United  
15 States person.

16 (2) EXCEPTIONS.—

17 (A) EXCEPTION TO COMPLY WITH INTER-  
18 NATIONAL OBLIGATIONS.—Sanctions under this  
19 subsection shall not apply with respect to the  
20 admission of an alien if admitting or paroling  
21 the alien into the United States is necessary to  
22 permit the United States to comply with the  
23 Agreement regarding the Headquarters of the  
24 United Nations, signed at Lake Success June  
25 26, 1947, and entered into force November 21,

1           1947, between the United Nations and the  
2           United States, or other applicable international  
3           obligations.

4           (B) EXCEPTION RELATING TO THE PROVI-  
5           SION OF HUMANITARIAN ASSISTANCE.—San-  
6           ctions under this subsection may not be imposed  
7           with respect to transactions or the facilitation  
8           of transactions for—

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

11                  (ii) the provision of humanitarian as-  
12                  sistance;

13                  (iii) financial transactions relating to  
14                  humanitarian assistance; or

15                  (iv) transporting goods or services  
16                  that are necessary to carry out operations  
17                  relating to humanitarian assistance.

18           (C) EXCEPTION FOR INTELLIGENCE, LAW  
19           ENFORCEMENT, AND NATIONAL SECURITY AC-  
20           TIVITIES.—Sanctions under this subsection  
21           shall not apply to any authorized intelligence,  
22           law enforcement, or national security activities  
23           of the United States.

24           (3) PENALTIES.—A person that violates, at-  
25           tempts to violate, conspires to violate, or causes a

1 violation of this subsection or any regulation, license,  
2 or order issued to carry out that subsection shall be  
3 subject to the penalties set forth in subsections (b)  
4 and (c) of section 206 of the International Emer-  
5 gency Economic Powers Act (50 U.S.C. 1705) to the  
6 same extent as a person that commits an unlawful  
7 act described in subsection (a) of that section.

8 (c) EXCEPTION WITH RESPECT TO THE IMPORTA-  
9 TION OF GOODS.—

10 (1) IN GENERAL.—The authorities and require-  
11 ments under this section shall not include the au-  
12 thority or any requirement to impose sanctions on  
13 the importation of goods.

14 (2) GOOD DEFINED.—In this section, the term  
15 “good” means any article, natural or man made sub-  
16 stance, material, supply, or manufactured product,  
17 including inspection and test equipment, and exclud-  
18 ing technical data.

19 **SEC. 5006. ASSESSMENT OF PEOPLE’S REPUBLIC OF CHI-**  
20 **NA’S MILITARY USE OF ARTIFICIAL INTEL-**  
21 **LIGENCE.**

22 (a) IN GENERAL.—Not later than 180 days after the  
23 date of the enactment of this Act, and annually thereafter,  
24 the Secretary of Defense shall submit to the Committee  
25 on Armed Services and the Committee on Foreign Affairs

1 of the House of Representatives and the Committee on  
2 Armed Services and the Committee on Foreign Relations  
3 of the Senate a report on the People's Liberation Army  
4 Cyberspace Force use of artificial intelligence.

5 (b) CONTENTS.—The report required by this section  
6 shall detail how the People's Liberation Army Cyberspace  
7 Force is using artificial intelligence for its modernization  
8 efforts and force posture in the Western Pacific. This shall  
9 include how the People's Liberation Army Cyberspace  
10 Force is exploiting access to United States and allied ad-  
11 vanced semiconductor technologies and artificial intel-  
12 ligence.

13 (c) FORM.—The report require by this section shall  
14 be submitted in unclassified form but may include a classi-  
15 fied annex.

