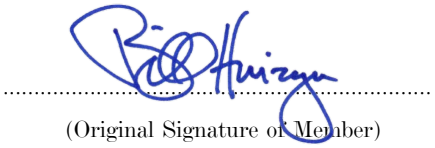

(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

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

Mr. HUIZENGA introduced the following bill; which was 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, American-owned artificial intelligence models, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as ''Deterring American AI Model Theft Act of 2026''.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

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

(2) many of the most advanced AI models owned by United States companies are ''closed-source models'' whose unique technical characteristics are not openly shared or published;

(3) the unauthorized acquisition of model capabilities, such as model weights, model architectures, and other technical characteristics of closed-source AI models by entities of concern through model extraction attacks represents a threat to the national security and foreign policy interests of the United States, as well as the intellectual property rights and economic competitiveness of United States companies;

(4) the United States Government, in cooperation with private owners of closed-source AI models, should take steps to identify, punish, and deter model extraction attacks on the protected capabilities of closed-source models by entities of concern;

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

(6) authorized model training practices that adhere to the terms of service or are otherwise consistent with contractual terms set by the owners of closed-source AI models are a legitimate research method that play an important role in AI research and are fundamentally distinct from model extraction attacks defined in this Act.

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

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

(2) CLOSED-SOURCE AI MODEL.—The term ''closed-source AI model'' means any artificial intelligence model with the following characteristics:

(A) Proprietary key technical information such as underlying model weights that are necessary to reproduce and independently recreate the model that are not willingly shared with third parties or otherwise made publicly available by the owner of the model.

(B) Access and use governed by terms of service or contractual agreements that are established by the owner of the model.

(C) Access that is provided via an Application Program Interface (API) or other consumer-facing, owner-controlled interfaces without enabling third parties to obtain, modify, or host the closed-source AI model on their own data servers or other technology unless specifically authorized by the owner of the closed-source AI model.

(3) COUNTRY OF CONCERN.—The term ''country of concern'' means—

(A) the People's Republic of China, including the Hong Kong and Macau Special Administrative Regions;

(B) the Russian Federation; and

(C) any other foreign country—

(i) listed in Country Group D:5 under Supplement No. 1 to part 740 of the Export Administration Regulations, as published on January 1, 2026, that is designated by the Secretary of State as a country of concern for purposes of this section and for which notice of such designa-

tion has been published in the Federal Register; and

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

(4) ENTITY OF CONCERN.—The term ''entity of concern'' means any foreign person or entity that—

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

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

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

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

(6) FOREIGN PERSON.—The term ''foreign person'' means a person that is not a United States person.

(7) FRAUDULENT ACCOUNT NETWORK PROVIDER.—

(A) IN GENERAL.—The term ''fraudulent account network provider'' means any foreign entity that knowingly and intentionally creates, obtains, maintains, sells, brokers, or otherwise provides access to accounts that allow entities of concern to access closed-source AI models that they would otherwise be prohibited from accessing due to location restrictions in the terms of service or contractual agreements created by the owner of the closed-source AI model.

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

(8) GOOD.—The term ''good'' has the meaning given that term in section 16 of the Export Administration Act of 1979 (50 U.S.C. App. 2415)(as con-

tinued in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.)).

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

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

(11) MODEL EXTRACTION ATTACK.—

(A) IN GENERAL.—The term ''model extraction attack'' means the unauthorized extracting of a closed-source AI model's capabilities to replicate, develop, train, or improve another AI model, where such querying—

(i) circumvents technical, contractual, or other access controls, identity verification requirements, or geographic access restrictions implemented by the model's owner;

(ii) is conducted through fraudulent, misrepresented, or unauthorized credentials; or

(iii) violates the terms, conditions, or restrictions governing access to or use of the model, as established by the owner or authorized provider, that specifically prohibit the use of model outputs or interactions to replicate, develop, train, or improve another AI model.

(B) INFERENCE OF PURPOSE.—For purposes of subparagraph (A), the purpose of querying may be inferred from the totality of circumstances, including—

(i) the volume, structure, pattern, coordination, or timing of the querying activity;

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

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

(iv) the correlation of querying activity within the development timeline of another AI model.

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

conducted within a permitted exception or the express authorization of the owner of the closed-source AI model, are not model extraction attacks.

(12) OPERATING COMMITTEE FOR EXPORT POLICY.— The term ''Operating Committee for Export Policy'' means the Operating Committee for Export Policy referred to in section 1763(c) of the Export Control Reform Act of 2018 (50 U.S.C. 4822(c)).

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

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

(B) is a United States person.

(14) REEXPORT.—The term ''reexport'' has the meaning given that term in section 1742(9) of the

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

SEC. 4. ASSESSMENT OF MODEL EXTRACTION ATTACKS AND FRAUDULENT ACCOUNT NETWORK PROVIDERS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State, in coordination with each agency that is a member of the Operating Committee for Export Policy, shall complete an assessment to determine—

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

(2) which, if any, entities of concern are fraudulent account network providers.

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

(1) A determination of which entities of concern—

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

(B) are fraudulent account network providers.

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

(3) An identification of which, if any, agencies or instrumentalities of governments of countries of concern have provided or are providing material assistance to entities identified pursuant to paragraph (1).

(4) An analysis of the methods employed by entities of concern identified pursuant to paragraph (1), including—

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

(B) a determination, to the extent possible, of the number of attempted model extraction attacks that occurred in the previous two calendar years from the date on which the Secretary of State begins the assessment pursuant to subsection (a)(1).

(5) An examination of the strengths and weaknesses of various detection approaches that can be

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

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

(7) Steps detailing how the United States Government is assisting owners of closed-source AI models that have been the target or victim of model extraction attacks in detecting model extraction attacks, deterring future model extraction attacks, and punishing entities of concern that engage in model extraction attacks or are fraudulent account network providers.

(8) A diplomatic strategy to leverage United States allies and partners in detecting and preventing model extraction attacks by entities of concern.

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

have been the targets or victims of model extraction attacks, whose participation in this consultation shall be voluntary, other companies, academic experts, industry fora, and other appropriate entities to—

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

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

(3) develop best practices for identifying fraudulent account network provider activities that facilitate model extraction attacks.

(d) REPORT.—

(1) IN GENERAL.—Not later than 210 days after the date of the enactment of this Act, the Secretary of Commerce, in coordination with each agency that is a member of the Operating Committee for Export Policy, shall submit to the appropriate congressional committees a report that contains the findings of the assessment. The Secretary of Commerce shall, annually for 3 years, submit to the appropriate congressional committees an updated report with any additional entities of concern identified pursuant to subsection (b)(1).

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

(e) ROUTINE ASSESSMENT.—The Secretary of Commerce, in coordination with each agency that is a member of the Operating Committee for Export Policy, shall routinely assess for—

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

(2) fraudulent account network providers that facilitate model extraction attacks after the date of completion of the assessment required by this section; and

(3) any material changes related to other matters specified in subsection (b).

(f) INDUSTRY COORDINATION.—The Secretary of Commerce, in coordination with each agency that is a member of the Operating Committee for Export Policy, shall establish an information sharing mechanism that allows owners of closed-source AI models to voluntarily, quickly, and confidentially share information about model extraction attacks and fraudulent account network providers with the Department of Commerce.

(g) AI MODEL EXTRACTION ATTACKERS LIST.—

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

(A) maintain a list, to be known as the ''AI Model Extraction Attackers List'', that displays information about specific individuals and entities of concern, that the assessment required by subsection (a) and routine assessment described in subsection (e) identify as having conducted or directed model extraction attacks in the past year; and

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

(2) PROTECTION OF CONFIDENTIAL INFORMATION.—The Secretary of State may not, in publishing the list required by paragraph (1) on a publicly available website of the Department of State, disclose confidential information provided by owners of closed-source AI models without the express permission of said owner.

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

member of the Operating Committee for Export Policy, shall publish a report comprising of best practices to detect, prevent, and respond to model extraction attacks.

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

(2) PROTECTION OF CONFIDENTIAL INFORMATION.—In making the report required by this subsection publicly available, the Secretary of Commerce, in coordination with each agency that is a member of the Operating Committee for Export Policy, shall not disclose confidential information provided by owners of closed-source AI models without the express permission of said owner.

SEC. 5. DETERRING MODEL EXTRACTION ATTACKS AND FRAUDULENT ACCOUNT NETWORK PROVIDERS.

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

assessment required under section 4 of this Act (identified pursuant to subsection (e) of such section), or any affiliate of such entity (to be determined by ownership of 50 percent or more in the aggregate, directly or indirectly), should be added to the Entity List maintained by the Bureau of Industry and Security of the Department of Commerce under Supplement No. 4 to part 744 of title 15, Code of Federal Regulations, or any successor regulations.

(b) SANCTIONS DESCRIBED.—

(1) IN GENERAL.—The President, acting through the Secretary of State, may, pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), block and prohibit all transactions in all property and interests in property of entities of concern identified pursuant to subsections (b)(1) and (e) of section 4 if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) EXCEPTIONS.—

(A) EXCEPTION TO COMPLY WITH INTERNATIONAL OBLIGATIONS.—Sanctions under this subsection shall not apply with respect to the admission of an alien if admitting or paroling

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

(B) EXCEPTION RELATING TO THE PROVISION OF HUMANITARIAN ASSISTANCE.—Sanctions under this subsection may not be imposed with respect to transactions or the facilitation of transactions for—

(i) the sale of agricultural commodities, food, medicine, or medical devices;

(ii) the provision of humanitarian assistance;

(iii) financial transactions relating to humanitarian assistance; or

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

(C) EXCEPTION FOR INTELLIGENCE, LAW ENFORCEMENT, AND NATIONAL SECURITY ACTIVITIES.—Sanctions under this subsection

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

(3) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of this subsection or any regulation, license, or order issued to carry out that subsection shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.