119TH CONGRESS
2D SESSION

S. 5252

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

AUGUST 5, 2026

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 Banking, Housing, and Urban Affairs

---

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.

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 ''Blocking Large-scale Adversarial Distillation Efforts Act of 2026'' or ''BLADE Act''.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

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

(2) many of the most advanced artificial intelligence models owned by United States entities 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 artificial intelligence models, by persons 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 entities;

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

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

allow foreign adversaries a short cut to acquiring advanced artificial intelligence 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 artificial intelligence models are a legitimate research method that play an important role in artificial intelligence research and are fundamentally distinct from model extraction attacks addressed by 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 of the Senate.

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

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

essary to reproduce and independently recreate the model and 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 or another consumer-facing, owner-controlled interface without enabling third parties to obtain, modify, or host the closed-source artificial intelligence model on their own data servers or other technology unless specifically authorized by the owner of the 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 in Supplement No. 1 to part 740 of title 15, Code of Federal Regulations, as published

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

(ii) identified by the Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security, pursuant to an assessment required by subsection (a) or (e) of section 4.

(4) PERSON OF CONCERN.—The term ''person of concern'' means any foreign person 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 artificial intelligence models owned by United States persons and outside of authorized model training practices.

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

(6) FRAUDULENT ACCOUNT NETWORK PROVIDER.—

(A) IN GENERAL.—The term ''fraudulent account network provider'' means any foreign person that knowingly and intentionally creates, obtains, maintains, sells, brokers, or otherwise provides access to an account that allows a person of concern to access a closed-source artificial intelligence model that the entity would otherwise be prohibited from accessing as a result of location restrictions in the terms of service or a contractual agreement created by the owner of the model.

(B) EXCEPTION.—For purposes of subparagraph (A), 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, on the basis of that activity alone, a fraudulent account network provider.

(7) MODEL EXTRACTION ATTACK.—

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

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

(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, that specifically prohibit the use of model outputs or interactions to replicate, develop, train, or improve another artificial intelligence model.

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

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

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

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

(iv) the correlation of extraction activity within the development timeline of another artificial intelligence model.

(C) EXCLUSION.—For purposes of subparagraph (A), model training activities conducted in compliance with the terms, conditions, and restrictions governing access to and use of a closed-source artificial intelligence model, or otherwise conducted within a permitted exception or the express authorization of the owner of the model, are not model extraction attacks.

(8) 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)).

(9) OWNER.—The term ''owner'' means, with respect to a closed-source artificial intelligence model, the person 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 the model, or any version, instance, or deployment the model, whether such rights were obtained through development, acquisition, assignment, license, or otherwise; and

(B) is a United States person.

(10) PERSON.—The term ''person'' means individual or entity.

(11) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

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

(C) any person located in the United States.

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 Commerce, acting through the Under Secretary of Commerce for Industry and Security and in coordination with the head of each agency that is a member of the Operating Committee for Export Policy, shall complete an assessment to determine—

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

(2) which, if any, persons 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 persons 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 the countries, if any—

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

(B) in which 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 persons 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 offices and data centers of such providers; and

(B) a determination, to the extent possible, of the number of attempted model extraction attacks that occurred during the 2 calendar years preceding the date on which the Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security,

begins the assessment required by subsection (a).

(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 persons of concern that occurred during the 2 calendar years preceding the date on which the Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security, begins the assessment required by subsection (a).

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

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

(c) PUBLIC CONSULTATION.—

(1) IN GENERAL.—In conducting the assessment required by subsection (a), the Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security and in coordination with the head of each agency that is a member of the Operating Committee for Export Policy, shall consult with owners of closed-source artificial intelligence models that have been the targets or victims of model extraction attacks, academic experts, industry fora, and other appropriate entities—

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

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

(C) to develop best practices for identifying activities of fraudulent account network providers that facilitate model extraction attacks.

(2) VOLUNTARY PARTICIPATION.—The participation of owners of closed-source artificial intelligence models described in paragraph (1) in consultations under that paragraph shall be voluntary.

(d) REPORT.—

(1) IN GENERAL.—Not later than 210 days after the date of the enactment of this Act, the Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security and in coordination with the head of 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 required by subsection (a).

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

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

(e) ROUTINE ASSESSMENT.—The Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security and in coordination with the

head of 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 artificial intelligence models that occur after the date of completion of the assessment required by subsection (a);

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

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

(f) INDUSTRY COORDINATION.—The Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security and in coordination with the head of 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 artificial intelligence 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 Commerce, acting through the Under Secretary of Commerce for Industry and Security and in coordination with

the head of 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 persons of concern identified pursuant to an assessment required by subsection (a) or (e) as having conducted or directed model extraction attacks in the past year; and

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

(2) PROTECTION OF CONFIDENTIAL INFORMATION.—The Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security, may not, in publishing the list required by paragraph (1) on a publicly available website of the Department of Commerce, disclose confidential information provided by the owner of a closed-source artificial intelligence model without the express permission of the owner.

(h) PUBLIC GUIDANCE.—

(1) IN GENERAL.—Not later than 210 days after the date of the enactment of this Act, the Secretary of Commerce, acting through the Under Secretary of Commerce for Industry and Security and

in coordination with the head of 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.

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

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

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

(a) CONSIDERATION OF ADDITION TO ENTITY LIST.—

(1) IN GENERAL.—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 the head of each agency that is a member of the End-User Review Committee, shall add each entity described in paragraph (2) to the Entity List maintained by the Bureau of

Industry and Security and set forth in Supplement No. 4 to part 744 of title 15, Code of Federal Regulations, or any successor regulations.

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

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

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

(b) IMPOSITION OF SANCTIONS.—

(1) IN GENERAL.—The President shall, 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 each person of concern identified under subsections (a) 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 RELATING TO THE PROVISION OF HUMANITARIAN ASSISTANCE.—Sanctions under paragraph (1) 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; or

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

(B) 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) WAIVER.—

(A) IN GENERAL.—The President may, subject to subparagraph (B), waive the application of subsection (a) or (b) with respect to a person if, before issuing the waiver, the President submits to Congress—

(i) a certification in writing that the issuance of the waiver is in the national interests of the United States; and

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

(B) FORM OF REPORT.—Each report required by subparagraph (A) shall be submitted in unclassified form but may include a classified annex.

(4) 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.

○