Sanctions and Export Control Responses to Adversarial Distillation

By Joe Khawam and Tim Schnabel

March 13, 2026
(updated March 26, 2026)

Comments on this draft paper are invited and can be sent to joe@lawreforminstitute.org.

I. Introduction

In early 2026, disclosures from the three leading U.S. AI developers revealed a coordinated pattern of industrial-scale distillation attacks against American frontier models. OpenAI informed the House Select Committee on China that employees of the Chinese AI laboratory DeepSeek developed methods to circumvent access restrictions and programmatically harvest outputs for distillation.[1] Google's Threat Intelligence Group documented similar extraction attempts against its Gemini models.[2] Anthropic's disclosure was more granular, identifying three Chinese AI laboratories—DeepSeek, Moonshot, and MiniMax—that used more than 24,000 fraudulent accounts and 16 million exchanges to extract Claude's reasoning capabilities, chain-of-thought processes, and agentic behaviors.[3] A senior U.S. official further noted that DeepSeek trained its latest model on smuggled Nvidia Blackwell chips, establishing a dual-channel circumvention strategy that includes stolen capabilities via distillation and stolen hardware via chip smuggling.[4]

This concept note examines the legal authorities available to the U.S. government to impose consequences on foreign entities engaged in adversarial distillation of U.S. frontier AI models. Government action would complement, not replace, the technical countermeasures that U.S. AI developers are independently employing.[5] The authorities discussed here are designed to impose consequences and alter incentives in a way that private-sector defensive measures alone cannot reach.[6] We assess four categories of tools in order of recommended priority.[7] For each,

[1] *See* Letter from OpenAI to House Select Comm. on the Chinese Communist Party (Feb. 12, 2026), https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rRmql_jJcxb4/v0.

[2] Google Threat Intelligence Group, GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use (Feb. 2026), https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use.

[3] Anthropic, Detecting and Preventing Distillation Attacks (Feb. 23, 2026), https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks.

[4] *See* Steve Holland et al., *Exclusive: China's DeepSeek Trained AI Model on Nvidia's Best Chip Despite US Ban, Official Says*, Reuters (Feb. 23, 2026), https://www.reuters.com/world/china/chinas-deepseek-trained-ai-model-nvidias-best-chip-despite-us-ban-official-says-2026-02-24/.

[5] Anthropic, for example, has announced enhanced detection systems and behavioral fingerprinting to identify distillation patterns, and other labs are strengthening their own defenses. *See* Anthropic, Detecting and Preventing Distillation Attacks (Feb. 23, 2026), https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks.

[6] A related policy approach would impose regulatory requirements on U.S. AI developers to implement anti-distillation measures industry-wide, addressing the collective action problem that makes unilateral investment insufficient. This paper focuses instead on imposing consequences on the foreign actors engaged in adversarial distillation, for two reasons. First, existing lab defenses have thus far proven insufficient against adversarial actors. *See, e.g.*, Letter from OpenAI to House Select Comm. on the Chinese Communist Party, *supra* note 1 (documenting "new, obfuscated methods" used to circumvent access restrictions, including through third-party routers masking query origins); Anthropic, Detecting and Preventing Distillation Attacks, *supra* note 5 (documenting use of more than 24,000 fraudulent accounts to evade platform safeguards). Second, output controls place compliance burdens on the victims of the conduct rather than on its perpetrators.

[7] A fifth category of authority—criminal statutes—warrants mention. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, may be a comparatively direct fit where actors use fraudulent credentials, false identities, or other evasive means to circumvent developer-imposed access restrictions on U.S. platforms. Trade-secret charges under section 1832 of the Economic Espionage Act are also conceivable, but they turn on the less-settled question, discussed in Section II.d., of whether systemically extracted model outputs qualify as trade secrets when outputs are commercially available. Extraterritorial jurisdiction under 18 U.S.C. § 1837 may attach to the EEA theory where the API queries targeted platforms operated by U.S.-headquartered companies. However, the criminal burden of proof,

we analyze legal feasibility, likely effectiveness, calibration of consequences, and potential pushback. We conclude with a recommended phased strategy that layers these authorities for escalating effect.

This analysis is premised on the factual record as reported by the affected U.S. AI developers. The applicability and strength of each authority discussed below will ultimately depend on the government's ability to build an independent evidentiary record consistent with those reports. We take no position on the sufficiency of the evidence currently available to the government.

II. Options

a. BIS Entity List

Legal authority and fit

The Entity List operates under Part 744 of the Export Administration Regulations. The legal standard requires "reasonable cause to believe, based on specific and articulable facts," that an entity has been involved in, or poses a significant risk of becoming involved in, activities contrary to U.S. national security or foreign policy interests.[8] This is a relatively low threshold. It is forward-looking, does not require proof of a completed violation, and explicitly encompasses risk-based assessments. The End-User Review Committee (Commerce, State, Defense, Energy, Treasury) votes on additions, and a majority is required to add an entity.[9]

The factual predicate here is almost certainly satisfied. BIS has already listed Chinese AI companies for advancing PRC military modernization through AI development (Zhipu AI, January 2025)[10] and for developing advanced AI with military-industrial ties (March 2025).[11] Adversarial distillation fits the same logic. Chinese labs systematically extracting frontier capabilities from U.S. models are advancing China's AI capabilities in ways that undermine U.S. national security, particularly given documented military-civil fusion strategy and the potential stripping of safety guardrails from distilled models.[12]

legal uncertainty at the margins of both theories, and the practical unenforceability of indictments against persons located in China make criminal prosecutions a less effective tool of deterrence than the national-security authorities analyzed here. A full treatment of the application of criminal laws to distillation is beyond the scope of this paper.

[8] 15 C.F.R. § 744.11 (2025).

[9] *See* 15 C.F.R. pt. 744, Supp. No. 5 (Procedures for End-User Review Committee Entity List and 'Military End User' (MEU) List Decisions).

[10] Addition of Entities to and Revision of Entry on the Entity List, 90 Fed. Reg. 4,617 (Jan. 16, 2025) (adding Zhipu AI entities).

[11] Bureau of Indus. & Sec., Commerce Further Restricts China's Artificial Intelligence and Advanced Computing Capabilities (Mar. 2025), https://www.bis.gov/press-release/commerce-further-restricts-chinas-artificial-intelligence-advanced-computing-capabilities.

[12] *See* Frontier Model Forum, Issue Brief: Adversarial Distillation (Feb. 2026), https://www.frontiermodelforum.org/issue-briefs/issue-brief-adversarial-distillation/.

Consequences and calibration

Entity List placement typically imposes license requirements for exports, reexports, or transfers of all items subject to the EAR to the listed entity. BIS can apply a presumption of denial to all such items—a posture that would override the more permissive case-by-case review established by the January 2026 final rule for H200, MI325X, and equivalent chips for exports from the United States to China.[13] That rule created a pathway through which Chinese AI labs could potentially acquire advanced U.S.-designed chips through licensed channels. Entity List designation with presumption of denial would override this pathway for designated entities, ensuring that the companies responsible for adversarial distillation cannot benefit from the relaxed AI chip review policy.

Entity List placement would address the hardware pipeline, but a significant gap remains around cloud computing services. Entity List designation alone does not restrict cloud providers from selling compute access to listed entities. The EAR provides supplemental mechanisms that could partially address this gap, but each carries limitations that make the authorities discussed below better suited for the problem.[14]

In addition to cloud computing access, Entity List designation faces practical enforcement limitations. Kharon documented that listed Chinese tech firms created new unrestricted subsidiaries within weeks of designation.[15] The BIS Affiliates Rule, currently suspended as part of the November 2025 U.S.-China trade arrangement but scheduled to go back into effect on November 10, 2026, would address this problem by automatically extending Entity List restrictions to any entity that is at least fifty percent owned, directly or indirectly, individually or in the aggregate, by one or more listed entities.[16] If reimposed, the Affiliates Rule would significantly complicate evasion through subsidiary creation, though it would also raise compliance costs for U.S. companies and others with U.S.-origin items in their supply chains.

[13] Revision to License Review Policy for Advanced Computing Commodities, 91 Fed. Reg. 1,684 (Jan. 15, 2026) (to be codified at 15 C.F.R. pts. 742, 744, 748); *see also* Bureau of Indus. & Sec., Department of Commerce Revises License Review Policy for Semiconductors Exported to China (Jan. 15, 2026), https://www.bis.gov/press-release/department-commerce-revises-license-review-policy-semiconductors-exported-china. Entity List placement can also, in certain cases (including where BIS applies an applicable foreign direct product rule or Entity List footnote designation), extend controls to certain foreign-produced items made using specified U.S.-origin technology. *See* 15 C.F.R. §§ 734.9, 744.21, 744.22.

[14] Conditions on AI chip export licenses can restrict downstream cloud use of foreign-located compute, but reach only chips exported through licensed channels. U.S. persons controls under 15 C.F.R. § 744.6 could prohibit U.S. cloud providers from furnishing compute to designated entities, but the authority is structurally designed for person-specific prohibitions on support for enumerated end-uses—requiring BIS to establish a WMD, military-intelligence, or similar nexus transaction by transaction rather than imposing a categorical prohibition—and runs through an enforcement architecture not designed for ongoing monitoring of cloud service transactions. An IEEPA-based program, by contrast, can prohibit specified services comprehensively through a single administrable framework, and derivative sanctions provisions can create pressure on non-U.S. providers that EAR-based tools cannot. *See infra* Section II.b.

[15] *See* Kharon, Weeks After BIS Listed These Chinese Tech Companies, They Spun Up Unrestricted Subsidiaries (2025), https://www.kharon.com/brief/bis-50-percent-rule-commerce-department-china-tech.

[16] *See* Expansion of End-User Controls to Cover Affiliates of Certain Listed Entities, 90 Fed. Reg. 47201 (interim final rule Sept. 30, 2025) (adopting the Affiliates Rule); One Year Suspension of Expansion of End-User Controls for Affiliates of Certain Listed Entities, 90 Fed. Reg. 50857 (Nov. 12, 2025) (staying the Affiliates Rule until Nov. 10, 2026).

Chips lawfully exported to approved customers in China or third countries can also be diverted to listed entities after the initial sale,[17] a problem that the January 2026 rule's more permissive export policy may exacerbate by increasing the volume of advanced chips in Chinese commercial channels.

Potential pushback

Entity List designations of Chinese AI companies would likely draw opposition from U.S. semiconductor companies. Nvidia lobbied aggressively for the H200 policy shift and would likely view targeted designations as removing some of the largest prospective customers from the newly opened market. The industry may argue that targeted listings erode the predictability of the licensing environment and drive Chinese customers toward domestic alternatives. However, this opposition must be weighed against the fact that the entities in question are not ordinary commercial customers. They are engaged in systematic, adversarial extraction of U.S. intellectual property. Permitting them to purchase U.S. chips under a case-by-case review standard while they actively harm U.S. AI companies and U.S. national security interests would represent a significant policy incoherence.

The timing of any designation would also need to account for President Trump's rescheduled visit to Beijing on May 14–15, 2026.[18] Pre-summit action could establish these designations as a baseline policy response to documented adversarial conduct, but it could equally be perceived as creating additional bargaining chips to be traded away at the summit table. China may also respond to the Entity List designations through its Unreliable Entity List or Anti-Foreign Sanctions Law, or it may leverage critical minerals as a pressure point. The timing decision is ultimately a political judgment that falls outside the scope of this analysis, but policymakers should be aware that delay also carries risk. The longer the gap between public disclosure and government response, the weaker the signal that adversarial distillation carries meaningful consequences.

b. OFAC Sanctions Under Existing or New Authorities

Legal authority and fit

Two pathways could support sanctions action against the entities responsible for adversarial distillation. First, EO 13694, as amended,[19] authorizes blocking sanctions against foreign persons responsible for cyber-enabled activities that cause a misappropriation of, among other things, "intellectual property, proprietary or business confidential information" for

[17] *See, e.g.,* Steve Holland et al., *Exclusive: China's DeepSeek Trained AI Model on Nvidia's Best Chip Despite US Ban, Official Says*, Reuters (Feb. 23, 2026), https://www.reuters.com/world/china/chinas-deepseek-trained-ai-model-nvidias-best-chip-despite-us-ban-official-says-2026-02-24/.

[18] *See* Aamer Madhani, *Trump Will Travel to Beijing for Rescheduled China Trip May 14-15, After Delay Due to Iran War*, Associated Press (Mar. 25, 2026), https://apnews.com/article/trump-china-trip-iran-war-401c4c33a01b2acce72e96eb8058f8cc.

[19] Exec. Order No. 13,694 (Apr. 1, 2015); Exec. Order No. 13,757 (Dec. 28, 2016) (amending EO 13694); Exec. Order No. 13,984 (Jan. 19, 2021) (further amending EO 13694); Exec. Order No. 14,144 (Jan. 16, 2025) (further amending EO 13694); Exec. Order No. 14,306 (June 6, 2025) (further amending EO 13694).

"commercial or competitive advantage or private financial gain," where the misappropriation is reasonably likely to result in, or has materially contributed to, a threat to U.S. national security, foreign policy, or economic health or financial stability.[20] The operative language is significant because it reaches beyond the formal "trade secret" definition under 18 U.S.C. § 1839; the government can frame the harm as misappropriation of intellectual property or proprietary or business confidential information, a lower bar that the scale and nature of the extraction campaigns likely clear.

The remaining legal question is whether industrial-scale API extraction through fraudulent accounts constitutes "cyber-enabled" activity. EO 13694, as amended, defines the relevant conduct as activities "originating from, or directed by persons located, in whole or in substantial part, outside the United States."[21] The EO does not define "cyber-enabled," but OFAC guidance describes it as "any act primarily accomplished through or facilitated by computers or other electronic devices."[22] API-based extraction plainly involves computers at every stage, from the automated query generation to the systematic collection and processing of outputs. However, prior designations under this program have targeted traditional network intrusions, ransomware attacks, election interference, online fraud, and exploit trafficking—not extraction through a commercially available interface. Extending the program to adversarial distillation would require treating systematic abuse of authorized access channels, conducted through thousands of fraudulent accounts in deliberate circumvention of platform safeguards, as functionally equivalent to unauthorized network penetration. EO 13694, as amended, also provides an alternative basis through its unauthorized access prong, which covers activities "related to gaining or attempting to gain unauthorized access to a computer or network of computers of a United States person."[23] The use of fraudulent identities to circumvent developer-imposed access controls, including geographic restrictions, has a reasonable claim to constitute unauthorized access, though this application, too, would be novel.

Second, the President could issue a new Executive Order under IEEPA declaring a national emergency and establishing a new sanctions program.[24] A new EO would offer several advantages over designations under EO 13694. It could be drafted to address adversarial distillation, chip smuggling and diversion, and other conduct that undermines U.S. AI leadership within a single framework, rather than forcing each category of conduct through the "cyber-enabled" definitional requirements of the existing program. Critically, unlike EO 13694—whose designation architecture results in SDN designations—a purpose-built IEEPA EO can include targeted service prohibitions that stop short of full blocking, providing an intermediate tool that EO 13694 cannot offer. A purpose-built EO would also send a clearer policy signal, publicly identifying the specific behaviors the United States considers unacceptable and establishing the consequences for engaging in them. This messaging function should not be underestimated; a criticism of existing export control and sanctions authorities is that they address AI-related threats piecemeal across programs designed for other purposes. IEEPA authority is well-established, and a new program can be activated rapidly.

[20] EO 13694, § 1(a)(ii)(D), as amended by EO 14144, § 9.
[21] EO 13694, § 1(a)(ii), as amended by EO 14144, § 9.
[22] OFAC, Cyber-related Sanctions FAQs, https://ofac.treasury.gov/faqs/topic/1546.
[23] EO 13694, § 1(a)(iii)(B), as amended by EO 14144, § 9 (retaining a "significant threat" threshold for this prong).
[24] *See* 50 U.S.C. §§ 1701–1708.

Consequences and calibration

EO 13694 designations result in SDN designation with full blocking sanctions. The fifty-percent rule extends blocking to entities owned by designated persons, addressing the front company problem. A purpose-built IEEPA EO, however, need not default to blocking sanctions. Unlike EO 13694—whose designation architecture is fixed—a new EO can be designed from the outset to include a broad services prohibition or targeted service prohibitions as a distinct intermediate tool. Specifically, a targeted services prohibition could prohibit U.S. Infrastructure as a Service (IaaS) providers from furnishing AI training compute to Entity List designees without those entities becoming SDNs. This would close the U.S. cloud computing gap that Entity List designation alone cannot address. A services-focused prohibition is a partial exercise of IEEPA blocking authority rather than a novel extension of it; IEEPA clearly authorizes prohibiting all transactions with designated persons, and restricting a defined category of services is a less intrusive application of that same power.[25]

The service prohibition architecture, whether implemented through a targeted IEEPA provision or through full blocking, reaches only U.S.-origin cloud infrastructure. Non-U.S. IaaS providers, offshore cluster operators, and persons that divert U.S. AI semiconductors fall outside the reach of such a prohibition. Derivative sanctions provisions can partially address this gap by creating risk for non-U.S. cloud providers, cluster operators, and semiconductor diverters serving designated entities.[26]

Declaring a new national emergency also carries inherent escalation risk. However, the President retains control over how aggressively the authority is deployed. A new EO could be issued without immediate designations, establishing the framework and putting targets on notice while preserving flexibility. Alternatively, initial designations could target smaller actors, such as researchers, engineers, or executives at the labs who were directly involved in the campaigns, and proxy service operators that knowingly supplied the fraudulent-account infrastructure used in the campaigns, to demonstrate willingness to act without immediately confronting major Chinese AI labs. This graduated approach has precedent in other IEEPA-based programs where the declaration of emergency preceded substantive designations.

[25] IEEPA authorizes the President to "investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit" any transaction involving property in which a foreign country or national has an interest. 50 U.S.C. § 1702(a)(1)(B). Full blocking sanctions issued under IEEPA prohibit all transactions with designated persons, including the provision of services. A prohibition limited to all services or to specified services (e.g., the provision of AI training compute) is a partial exercise of that authority. OFAC's use of sector-specific transaction prohibitions that stop short of full blocking is well-established. The Russia sectoral sanctions program under EO 13662 (79 Fed. Reg. 16167, Mar. 24, 2014), for example, prohibited defined categories of financial transactions with designated entities without blocking those entities and prohibiting all U.S.-person dealings.

[26] Export control conditions on AI chip licenses may provide a complementary mechanism for reaching foreign-located compute operated by non-U.S. providers, as discussed above. The practical effectiveness of export control conditions as a mechanism for restricting foreign-located compute access, however, is complicated by documented evasion of existing chip export controls through smuggling and transshipment. *See supra* note 4 (confirming that DeepSeek trained on smuggled Nvidia Blackwell chips despite applicable export restrictions). Licensing conditions bind authorized users but cannot prevent designated entities from obtaining compute on chips that have already been diverted outside controlled channels.

Potential pushback

OFAC sanctions remain the most escalatory option in principle, though the more limited IEEPA options and the graduated deployment strategies discussed above would moderate the initial impact. If the President designates major Chinese AI labs immediately, the retaliation risk is heightened. A services-related prohibition, a framework-only EO, or limited initial SDN designations targeting proxy service operators would mitigate this risk while preserving the option to escalate.

c. Complementary List-Based Designations: NS-CMIC and Section 1260H

Legal authority and fit

Two existing list-based authorities target different dimensions of designated entities' U.S. relationships—capital markets access and federal procurement—and warrant consideration as complementary tools in a phased strategy. The Non-SDN Chinese Military-Industrial Complex Companies (NS-CMIC) List is administered by OFAC under EO 13959, as amended by EO 14032.[27] Designation requires a finding that the entity operates in the defense and related materiel sector, the surveillance technology sector, or both, or is owned or controlled by (or owns or controls) such an entity.[28] The Section 1260H List is maintained by the Department of Defense under Section 1260H of the FY 2021 National Defense Authorization Act and identifies entities that qualify as "Chinese military companies" operating directly or indirectly in the United States under the criteria established in that provision.[29]

Neither authority was designed to specifically address the adversarial distillation scenario, and both require a military-company nexus that may not be straightforward for all the entities discussed in this note. The most viable path to designation runs through China's military-civil fusion policies and the documented integration of Chinese AI development into PRC national security objectives. BIS has already invoked that logic to list Chinese AI companies on the Entity List—for example, Zhipu AI-related entities were listed in January 2025 for advancing PRC military modernization through AI development—and the same factual predicate could potentially support NS-CMIC or 1260H designation for entities engaged in adversarial distillation.[30] Whether the government can sustain that nexus as to DeepSeek, Moonshot, and MiniMax specifically will depend on the evidentiary record available at the time of designation.

[27] EO 13959, *Addressing the Threat from Securities Investments That Finance Communist Chinese Military Companies*, 85 Fed. Reg. 73185 (Nov. 17, 2020), as amended by EO 14032, *Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China*, 86 Fed. Reg. 30145 (June 7, 2021). The amended order is implemented at 31 C.F.R. pt. 586.

[28] EO 13959, as amended by EO 14032, § 1(a), 86 Fed. Reg. 30145, 30146 (June 7, 2021).

[29] Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, § 1260H (2021) (codified at 10 U.S.C. § 113 note). Section 1260H requires the Secretary of Defense to publish the list annually until December 31, 2030.

[30] BIS added Zhipu AI (Beijing Zhipu Huazhang Technology Co., Ltd.) to the Entity List in January 2025 for advancing PRC military modernization through AI development. *See* Addition of Entities to and Revision of Entry on the Entity List, 90 Fed. Reg. 4,617 (Jan. 16, 2025).

Consequences and calibration

NS-CMIC designation prohibits U.S. persons from purchasing or selling publicly traded securities of designated entities, or any securities that are derivative of, or designed to provide investment exposure to, those securities. The restriction does not prohibit other commercial transactions, making it a capital markets tool.[31] Its practical impact is greatest for entities with U.S. investors, U.S.-listed securities, or ambitions to access U.S. capital markets.

Section 1260H designation carries a growing set of procurement-related restrictions. Section 805 of the FY 2024 NDAA prohibits DoD from entering into, renewing, or extending contracts with 1260H-listed entities (the Entity Prohibition, effective June 30, 2026) and from procuring, directly or indirectly, goods or services produced or developed by a listed entity or any entity under its control (the Goods and Services Prohibition, effective June 30, 2027).[32] Designation also creates secondary compliance pressure. BIS views 1260H listing as a red flag for Military End User status under the EAR, which can cause U.S. exporters and financial institutions to decline transactions even absent a strict legal prohibition.[33]

Beyond their direct legal effects, NS-CMIC and 1260H designations carry a distinct messaging value that the IEEPA EO's policy signal does not replicate. Formally characterizing DeepSeek, Moonshot, or MiniMax as Chinese military companies—or as operating in the defense and related materiel sector—undermines those entities' ability to present themselves as purely commercial actors in international markets and partnerships. That characterization may have downstream effects on third-country relationships, investment decisions, and academic collaborations that operate outside the formal reach of U.S. sanctions authority.

Potential pushback

The principal risk is legal and factual, not geopolitical. NS-CMIC and 1260H designations are lower in the escalation hierarchy than SDN listings. The government, however, must ensure the evidentiary basis for any designation under these authorities is sufficient to withstand legal scrutiny before proceeding.

[31] OFAC FAQ 905 (June 3, 2021) (clarifying that the prohibitions "apply only with respect to certain purchases or sales of publicly traded securities" and that the order does not prohibit "the purchase or sale of goods or services" with respect to CMIC entities or their subsidiaries).

[32] The direct and indirect procurement prohibitions derive from Section 805 of the National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, § 805 (2023). Section 805's Entity Prohibition takes effect on June 30, 2026, and its Goods and Services Prohibition takes effect on June 30, 2027.

[33] *See* Hogan Lovells, US Department of Defense Issues Updated Section 1260H Chinese Military Companies List (Jan. 17, 2025), https://www.hoganlovells.com/en/publications/us-department-of-defense-issues-updated-section-1260h-chinese-military-companies-list-. This creates a secondary compliance pressure. U.S. exporters and financial institutions may decline to transact with 1260H-listed entities even absent a strict legal prohibition, amplifying the practical consequences of designation beyond the formal procurement restrictions.

d. The PAIP Act

Legal authority and fit

The Protecting American Intellectual Property (PAIP) Act of 2022 requires the President to identify foreign persons that have "knowingly engaged in, or benefitted from, significant theft of trade secrets of United States persons" where the theft is "reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."[34] Once identified, sanctions are mandatory. The President must impose at least five from a menu of twelve, which include OFAC blocking, Entity List placement, Export-Import Bank restrictions, investment prohibitions, and visa denials.[35] The statute also covers entities that have "benefitted from" trade secret theft and those providing "significant financial, material, or technological support,"[36] potentially reaching the entire distillation chain.

The statute uses the broad definition of "trade secret" from the Economic Espionage Act, which covers all forms of business, scientific, technical, or engineering information from which the owner derives independent economic value and takes reasonable measures to keep secret.[37] Applying this definition to adversarial distillation requires confronting the threshold question of whether the outputs of frontier AI models can constitute trade secrets when any authorized user can obtain such outputs through ordinary API access.

Any individual API response is available to any paying customer and, standing alone, would not satisfy the statutory requirement that trade secret information not be "generally known" or "readily ascertainable through proper means."[38] But adversarial distillation does not target individual outputs. It targets the model's embedded reasoning capabilities, training methodology artifacts, and capability distributions, which are reflected across millions of structured exchanges designed to systematically reconstruct those capabilities in a competing model. On this theory, the trade secret is the aggregate of learned representations that required billions of dollars in compute, proprietary training data, and years of research to develop, and that the owner has chosen to make available only through controlled inference access rather than by releasing model weights. That DeepSeek and others required 24,000 fraudulent accounts to carry out the distillation campaign is evidence both that protective measures existed and that

[34] Protecting American Intellectual Property Act of 2022, Pub. L. No. 117-336, 136 Stat. 6147 (enacted Jan. 5, 2023) (codified at 50 U.S.C. § 1709).
[35] 50 U.S.C. § 1709(b) (mandatory sanctions menu).
[36] 50 U.S.C. § 1709(a)(1)(A)(i)–(ii).
[37] 18 U.S.C. § 1839(3) (defining "trade secret" as "all forms and types of financial, business, scientific, technical, economic, or engineering information" that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information" and is subject to "reasonable measures to keep such information secret").
[38] *See* 18 U.S.C. § 1839(3)(B).

improper means were used to circumvent them[39]—a factual pattern that is now the subject of analogous litigation in federal court.[40]

The theory is plausible, but it is not certain to prevail. A skeptic could conclude that making outputs commercially available through an API is fundamentally incompatible with trade secret protection, regardless of scale. Whether the government can sustain the argument that the trade secret resides not in any individual output but in the aggregate of learned representations is the central legal question that any PAIP Act designation in this context would need to answer.

The PAIP Act requires no judicial finding that a trade secret theft has occurred before sanctions can be imposed. The President makes the determination and reports it to Congress.[41] This lowers the threshold for action but does not insulate the designation from review. A designated entity could challenge the designation in federal court under the Administrative Procedure Act. Courts reviewing IEEPA-based sanctions designations have applied the "arbitrary and capricious" standard of 5 U.S.C. § 706(2)(A), with significant but not unlimited national security deference.[42] Under that standard, the government must demonstrate that the administrative record provides a rational basis for the designation.

The evidentiary record may prove to be the easier part of that showing. The scale of the documented conduct—thousands of fraudulent accounts, millions of structured queries, and a resulting model that closely mirrors the capabilities of the original—could provide a substantial factual basis for a presidential determination. The harder question is whether a reviewing court would accept that systemic API-based distillation constitutes "significant theft of trade secrets" within the meaning of the statute. Even under a deferential standard, the court must accept the legal theory, not merely the factual predicate. A designation that fails on these grounds would not merely unwind a single action but could cast doubt on the PAIP Act's utility as a tool for addressing AI-related intellectual property threats more broadly.

Consequences and calibration

The requirement to impose at least five sanctions from a menu of twelve gives the President meaningful flexibility to calibrate the response to the severity of the conduct. The available sanctions range from substantial economic isolation to relatively modest restrictions, and the selection will determine whether the designation functions primarily as a punitive measure or as leverage to change behavior.

At the severe end, selecting blocking sanctions would prohibit all U.S. persons from engaging in any transactions involving the property or interests in property of the designated

[39] *Cf.* Anthropic, Detecting and Preventing Distillation Attacks (Feb. 23, 2026), https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks.
[40] Complaint, *OpenEvidence, Inc. v. Pathway Med., Inc.*, No. 1:25-cv-10471-MJJ (D. Mass. Feb. 26, 2025) (alleging defendants used stolen credentials and "prompt injection" attacks—i.e., malicious inputs designed to bypass safeguards—to induce plaintiff's AI system to divulge proprietary information, including system prompts and instructions).
[41] *See* 50 U.S.C. § 1709(a)–(b).
[42] *See, e.g.*, *Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156 (D.C. Cir. 2003); *Al-Haramain Islamic Found., Inc. v. U.S. Dep't of the Treasury*, 686 F.3d 965 (9th Cir. 2012).

entity. Unlike Entity List restrictions, which reach only items subject to the EAR, blocking sanctions reach all U.S.-person dealings, including cloud computing services, financial transactions, and commercial partnerships. This would limit the cloud computing gap identified above and extend to categories of conduct that the EAR framework cannot reach. OFAC's fifty-percent rule would also likely apply, automatically extending blocking to any entity owned fifty percent or more by a designated person, providing a more comprehensive response to the front company problem than BIS's current approach to newly created subsidiaries. Combining blocking with the investment prohibition and banking transaction restrictions would effectively sever the designated entity from the U.S. financial system.

At the other end of the spectrum, a package built around Export-Import Bank restrictions, procurement bans, and opposition to international financial institution loans would signal disapproval without imposing crippling consequences, potentially leaving room for negotiated behavioral changes. Regardless of which five sanctions the President selects for entities, the statute also mandates additional sanctions for any alien identified in the report (including blocking and visa-related consequences) and authorizes sanctions on principal executive officers.

Potential pushback

A PAIP Act designation in this context would face two categories of risk: legal exposure inherent in extending the statute to a novel and untested theory, and geopolitical blowback that would intensify with the severity of the sanctions selected.

The legal risk is structural. The first PAIP Act designations involved conventional theft of cyber tools subsequently sold to a Russian exploit broker.[43] Extending the statute to API-based distillation would be a materially more difficult application, and the evidentiary case must be robust enough to withstand public and judicial scrutiny even under a deferential standard of review. As discussed above, the central vulnerability is not the factual record but the untested legal theory on which the designation would rest. A failed challenge would set an unfavorable precedent.

The geopolitical risk is calibration-dependent. A package of sanctions from the menu that initially avoids blocking may reduce the diplomatic and retaliatory costs while still imposing meaningful consequences and sending a clear message. The calibration question is therefore about managing escalation risk.

e. Addressing the Hypocrisy Argument

Any government action will face the criticism that U.S. AI labs trained their own models on copyrighted internet content—often by scraping websites in ways that may themselves violate those sites' Terms of Service—making it hypocritical to punish Chinese labs for distillation. This argument carries some weight, and policymakers would need to account for it when selecting and calibrating a response. It is also true that distillation is a legitimate and widely used technique

[43] Press Release, U.S. Dep't of State, Protecting Americans from Intellectual Property Theft (Feb. 24, 2026), https://www.state.gov/releases/office-of-the-spokesperson/2026/02/protecting-americans-from-intellectual-property-theft.

across the AI industry; frontier labs routinely distill their own models to create smaller, cheaper versions, and researchers use competitor model outputs for evaluation and benchmarking. But the adversarial distillation documented in early 2026 differs in both scale and character from these practices. The campaign involved deliberate, coordinated efforts by commercial competitors in a foreign adversary nation to extract proprietary capabilities of U.S. frontier models through thousands of fraudulent accounts, false identities, and active evasion of geographic access restrictions. The U.S. government has independent national security and geopolitical interests in responding to that conduct on its own terms, even as the broader questions surrounding AI training practices continue to be resolved through litigation and legislation.

III. Recommendation

The authorities analyzed above should be deployed in a phased escalation strategy that layers consequences for increasing effect while preserving diplomatic flexibility. Each phase builds on the preceding one and is designed to be independently justifiable. The decision to move from one phase to the next, and the calibration of consequences within each phase, should be driven by the designated entities' response and by broader diplomatic and policy conditions, not by a predetermined timeline.

Phase 1: Entity List Designation. BIS should add DeepSeek, Moonshot, and MiniMax to the Entity List under Part 744, with license requirements for all items subject to the EAR and a presumption of denial.[44] The legal standard is well-established, the factual predicate is strong, and the designation process is familiar to the interagency. Designation would ensure that the companies responsible for adversarial distillation cannot benefit from the January 2026 final rule's more permissive case-by-case review policy for advanced chips. The timing of Phase 1 action should account for the President's rescheduled visit to Beijing on May 14–15, balancing the value of a prompt response to documented adversarial attack against the diplomatic considerations discussed in Section II.a. Entity List designation addresses the hardware pipeline but leaves a significant gap around cloud computing services, which are not controlled as items subject to the EAR.

Phase 2: IEEPA Framing and Complementary Designations. The President should issue a new Executive Order under IEEPA declaring a national emergency with respect to foreign threats to U.S. AI leadership. The EO should establish a comprehensive sanctions framework—including full blocking authority, targeted service prohibitions, and derivative sanctions provisions—that can be activated in graduated fashion across Phases 2 and 3. A purpose-built program would avoid the definitional risks associated with the "cyber-enabled" requirement, could address adversarial distillation, chip smuggling, and related conduct within a single coherent framework, and would allow the government to define the sanctionable conduct in terms that match the facts.

[44] Entity List designation should include an express carve-out allowing U.S. persons to engage with the designated entities in AI safety and risk dialogues, analogous to the exception established for standards-related activities under 15 C.F.R. § 734.10. *See* Standards-Related Activities and the Export Administration Regulations, 89 Fed. Reg. 58,265 (July 18, 2024) (establishing that certain standards-setting activities with Entity List parties do not constitute a licensable export or transfer under the EAR, to avoid ceding standards development to PRC-aligned entities).

In Phase 2, the intermediate and complementary tools should be activated first. Specifically, Phase 2 activation would include a prohibition on U.S. IaaS providers furnishing AI training compute to Entity List designees, without those entities becoming SDNs, which would close the cloud computing gap for U.S.-origin infrastructure.[45] Consistent with the graduated approach, Phase 2 should also impose initial blocking sanctions on proxy service operators that knowingly provided the fraudulent-account infrastructure used in the distillation campaigns and on researchers, engineers, or executives involved in them. Blocking of the major Chinese AI labs and activation of derivative sanctions against foreign cloud providers, offshore cluster operators, and semiconductor diverters serving them should be reserved for Phase 3, preserving diplomatic flexibility while the intermediate architecture imposes costs. The EO could be issued concurrently with or shortly after Phase 1 to establish the framework and put targets on notice. If the administration opts against a new EO, EO 13694 could support blocking sanctions in Phase 3, but its fixed designation architecture—which defaults to blocking sanctions and does not accommodate the intermediate service prohibitions—makes it a less suitable vehicle for the graduated approach recommended here.

In addition, policymakers should pursue NS-CMIC and Section 1260H designations for the entities responsible for adversarial distillation. NS-CMIC designation would impose targeted capital markets restrictions; inclusion on the 1260H List would trigger procurement-related restrictions taking effect in 2026 and 2027. Both listings require a military-company nexus that must be sustained on the evidentiary record.

Together with the IEEPA intermediate tools, these designations would layer additional consequences across capital markets and procurement while preserving the option to escalate to Phase 3. Formally characterizing these entities as Chinese military companies also carries a distinct messaging value independent of the legal consequences: it undermines their ability to present themselves as purely commercial actors in international markets and partnerships, with potential downstream effects on third-country investment decisions, academic collaborations, and commercial relationships that operate outside the formal reach of U.S. sanctions authority.

Phase 3: Blocking Sanctions and PAIP Act Designation. If the designated entities do not meaningfully alter their conduct, the President should impose blocking sanctions on major Chinese AI labs under the IEEPA program established in Phase 2. Blocking sanctions would sever all U.S.-person dealings, carrying criminal penalties for willful violations. The fifty-percent rule would automatically extend blocking to subsidiaries. With the major labs now SDNs, the derivative sanctions provisions established in Phase 2 would be activated, forcing foreign cloud providers, offshore cluster operators, and semiconductor diverters serving them to choose between business with the designated labs and the risk of designation.

[45] Export control conditions on AI chip licenses may provide a complementary mechanism for reaching foreign-located compute operated by non-U.S. providers. The practical effectiveness of such conditions, however, is complicated by documented evasion of existing chip export controls through smuggling and transshipment. *See supra* note 4. Derivative sanctions provisions activated in Phase 3 provide an additional lever against non-U.S. providers with meaningful U.S. market exposure.

The PAIP Act also remains available as a parallel authority in this phase, though the IEEPA framework is the preferred vehicle given its stronger legal footing. PAIP Act designations could add incremental value by anchoring the response in a statute expressly aimed at trade secret theft, but such designations would likely turn on the untested theory that trade secrets can reside in aggregate model behavior extracted via API access.

* * *

The phased strategy is designed to change behavior, not solely to punish. Each phase should be accompanied by clear signaling of the conditions under which pressure would be reduced, including verifiable commitments that the designated entities have ceased adversarial distillation campaigns, dismantled the fraudulent account infrastructure used to conduct them, and will not incorporate capabilities obtained through prior distillation into future model development.