Export Control Authorizations for AI Evaluations

August 20, 2026

The attached draft legislation was produced by the Law Reform Institute for discussion purposes. The Law Reform Institute intends to solicit feedback on this draft and revise it. Comments on this draft are invited and can be sent to tim@lawreforminstitute.org and joe@lawreforminstitute.org.

Background

As frontier artificial intelligence (AI) systems become more capable, evaluating whether those systems could facilitate serious harm becomes increasingly important, as does mitigating any identified risks. Responsible AI developers conduct—and often work with third-party experts to conduct—evaluations for a wide range of risks relevant to national security, in areas such as chemical, biological, radiological, nuclear, and explosives (CBRNE), cybersecurity, and others. Evaluating and mitigating these risks are essential for both development and deployment of frontier AI models and are increasingly expected by policymakers and the public. However, conducting these evaluations and mitigations may implicate U.S. export control laws in ways that increase legal uncertainty and create operational barriers for AI developers.

U.S. export controls restrict the transfer of controlled technology, software, and technical data to foreign persons, including such persons working in the United States. The Export Administration Regulations (EAR), 15 C.F.R. parts 730–774, administered by the Bureau of Industry and Security (BIS), control dual-use items. The International Traffic in Arms Regulations (ITAR), 22 C.F.R. parts 120–130, administered by the Directorate of Defense Trade Controls (DDTC), control defense articles, technical data, and defense services. Under the "deemed export" rule, a release of controlled technology or technical data to a foreign person in the United States is "deemed" to be an export to the foreign person's country of nationality and may require government authorization.[1] This framework was designed to prevent the transfer of sensitive technologies to foreign adversaries, but AI evaluations and mitigations may themselves involve transfers of the type of controlled information that triggers these restrictions.

AI developers conduct evaluations of frontier systems to assess whether their models could help users cause serious harm. These evaluations require personnel with specialized expertise to probe model capabilities, and many of these experts are foreign persons. Controlled information may be encountered at several points during the evaluation and mitigation process, including when sharing data sets, prompts, outputs, and evaluation results. If foreign-person employees or contractors participate in these evaluations and mitigations, a deemed export may occur.[2] Both the individuals and the company may face civil and criminal liability under the Arms Export Control Act (22 U.S.C. § 2778) and the Export Control Reform Act of 2018 (50 U.S.C. §§ 4801–4852). Parts of the AI industry have recognized this risk, and some have requested export control carveouts for testing in CBRNE and other sensitive domains.[3]

---

[1] *See* 15 C.F.R. § 734.13(a)(2) (EAR definition of "export" that includes deemed exports); 22 C.F.R. § 120.50(a)(2) (ITAR definition of "export" that includes deemed exports).

[2] For example, if a U.S. person employed at a third-party evaluator develops specialized prompts containing pathogen enhancement techniques to test a model's refusal mechanisms, sharing those prompts with a foreign person employed by the same evaluator in the United States could constitute a deemed export. Similarly, if the model generates controlled information in response to such a prompt, and the third-party evaluator emails the prompt and output to a foreign-person employee at the AI developer along with recommended mitigations, additional deemed exports may occur.

[3] *See* Memorandum from Christopher Lehane, Chief Glob. Affs. Officer, OpenAI, to Michael Kratsios, Exec. Dir., Off. of Sci. & Tech. Pol'y (Oct. 27, 2025), at 8-9, https://cdn.openai.com/pdf/21b88bb5-10a3-4566-919d-f9a6b9c3e632/openai-ostp-rfi-oct-27-2025.pdf; Letter from Courtney Lang, Vice President of Policy, Trust, Data & Tech., Info. Tech. Indus. Council to Michael Kratsios, Dir., Off. of Sci. & Tech. Pol'y (Oct. 27, 2025), at 5,

Existing regulatory authorizations do not adequately address this problem. While both the EAR and the ITAR include various license exceptions and exemptions, none were designed to facilitate evaluations of AI models.[4] Case-by-case licenses are also impractical. Industry competition and pressure for rapid model releases leave limited time for pre-deployment evaluations and mitigations, while EAR or ITAR licensing can take a month or more.

The draft legislation below is premised on the judgment that facilitating bona fide evaluations of AI models and mitigating any identified risks serve the national security and foreign policy interests of the United States. Appropriately structured authorizations, with meaningful safeguards, reporting, and enforcement mechanisms, can enable such evaluations and mitigations without undermining the core non-proliferation objectives of export control laws. Accordingly, the draft legislation directs the Secretaries of Commerce and State to establish the necessary authorizations and appropriate safeguards, thereby reconciling rigorous AI evaluations and mitigations with vital export controls.

Note: terms defined in section 2 (Definitions) are underlined when used elsewhere in the text.

https://www.itic.org/documents/artificial-intelligence/ITICommentsonOSTPAIInnovationRegStreamliningFINAL.pdf.

[4] *See* Doni Bloomfield, Joe Khawam & Tim Schnabel, *Application of U.S. Export Controls to AI Biosecurity Evaluations and Mitigations*, Law Reform Inst. (Oct. 14, 2025), https://lawreforminstitute.org/bio101425.pdf (analyzing the various license exceptions, exemptions, and exclusions that may apply to AI biosecurity evaluations); Doni Bloomfield, Joe Khawam,& Tim Schnabel, "How U.S. Export Controls Risk Undermining Biosecurity," *Lawfare* (Dec. 2, 2025), https://www.lawfaremedia.org/article/how-u.s.-export-controls-risk-undermining-biosecurity.

Draft Federal Legislation

A BILL

To direct the Department of Commerce and the Department of State to establish export-control authorizations for bona fide artificial intelligence evaluations and mitigations, and for other purposes.

SECTION 1. SHORT TITLE.

This Act may be cited as the "AI Evaluation Authorization Act".

SEC. 2. DEFINITIONS.

In this Act:

(1) the term "advanced artificial intelligence system" means an artificial intelligence model or system that meets criteria specified in the regulations required by section 3(c);

(2) the term "artificial intelligence" has the meaning given in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. § 2358 note);

(3) the term "appropriate committees of Congress" means the Committee on Banking, Housing, and Urban Affairs and the Committee on Foreign Relations of the Senate, and the Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives;

(4) the term "evaluation activities" means

(A) good-faith efforts to design, conduct, and interpret evaluations, such as red-teaming and controlled experiments, that are primarily intended to assess or reduce the risk that an advanced artificial intelligence system could enable or materially facilitate serious harm, including harm related to—

(i) chemical, biological, radiological, or nuclear weapons or related delivery systems;

(ii) explosives, improvised explosive devices, or mass-casualty weapons construction or use;

(iii) malicious cyber capabilities, including capabilities that could cause significant disruption to critical infrastructure, enable large-scale unauthorized access to information systems, or facilitate the development or deployment of malware development or exploitation tools;

(iv) the generation of technology or software described on the Commerce Control List, or technical data described on the United States Munitions List; and

(v) other severe-harm categories designated by the Secretary of Commerce and the Secretary of State by regulation;

(B) good-faith mitigation efforts, such as design, implementation, or verification of safeguards, that are primarily intended to address the risks covered by subparagraph (A); and

(C) good-faith assistance efforts, such as information-sharing, that are primarily intended to support the activities covered by subparagraphs (A) and (B).

Notes

This section establishes key definitions.

The definition of "appropriate committees of Congress" identifies the committees with primary jurisdiction over the EAR and ITAR, ensuring that the Section 9 report reaches the committees responsible for oversight of the underlying export control statutes.

The term "evaluation activities" is defined to encompass good-faith efforts to design, conduct, and support evaluations, including red-teaming and controlled experiments; good-faith mitigation efforts, including safeguard implementation and verification; and good-faith assistance to those undertaking activities in the first two categories (such as information sharing through industry consortia, standards bodies, or similar multi-stakeholder organizations that facilitate the development of shared evaluation methodologies, benchmarks, and best practices). The use of "good faith" signals that the authorization does not cover access to controlled information when the evaluation activities are pretextual.

SEC. 3. REQUIRED RULEMAKING FOR EVALUATION ACTIVITIES.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act—

(1) the Secretary of Commerce shall establish, by regulation, a license exception under the Export Administration Regulations to authorize releases and other transfers of controlled technology or software that are reasonably necessary to conduct evaluation activities; and

(2) the Secretary of State shall establish, by regulation, an exemption under the International Traffic in Arms Regulations to authorize releases and other transfers of controlled technical data and the provision of defense services that are reasonably necessary to conduct evaluation activities.

(b) LIMITATIONS.—The Secretary of Commerce and the Secretary of State may impose limitations on the license exception and exemption required by this section based on the nationality or location of persons who would receive controlled technology, software, or technical data.

(c) COVERED SYSTEMS.—The regulations required by subsection (a) shall include criteria, developed jointly by the Secretary of Commerce and the Secretary of State, in consultation with other appropriate agencies, for identifying the advanced artificial intelligence systems for which evaluation activities are covered. Such criteria may relate to the technical characteristics of the systems themselves, the resources used to develop the systems, or their likely capabilities.

(d) RADIOLOGICAL AND NUCLEAR EVALUATIONS.—The license exception and exemption required by this section shall not authorize evaluation activities relating to radiological or nuclear weapons unless the Secretary of Energy and the Nuclear Regulatory Commission have concurred and, as applicable, have acted under section 7 to authorize such activities on terms consistent with the license exception and exemption.

Notes

This section establishes the core mechanism of the legislation by directing the Secretaries of Commerce and State to establish authorizations (a license exception under the EAR and an exemption under the ITAR) rather than having Congress directly carve out particular activities from export controls. This structure preserves executive branch flexibility to define the precise scope and conditions of the authorizations, allows for regulatory amendments as circumstances change, and respects the traditional division of authority in which Congress sets policy objectives while agencies implement technical regulations. The 180-day deadline creates urgency while providing adequate time for interagency coordination and notice-and-comment rulemaking.

Subsection (b) authorizes the Secretaries to impose nationality- or location-based limitations on the authorizations without mandating specific country restrictions in the statute. This approach gives the agencies flexibility to align the authorization with existing country-based frameworks under the EAR and ITAR, and to adjust those limitations as circumstances change. Persons who may receive controlled technology, software, or technical data under the authorizations are expected to include employees and contractors of AI developers and evaluators, as well as others reasonably necessary to conduct evaluation activities, whether located inside or outside the United States.

Subsection (c) directs the Secretaries to establish criteria for identifying which advanced artificial intelligence systems are covered by the authorization. The criteria are intentionally delegated to regulation rather than specified in statute, recognizing that appropriate thresholds will depend on technical factors that evolve and that agencies are better positioned than Congress to calibrate. The requirement for joint development by Commerce and State, in consultation with other appropriate agencies, ensures that the criteria reflect both dual-use and defense-related considerations and benefit from input across the federal government.

Finally, frontier AI developers routinely conduct CBRN evaluations—including radiological and nuclear components—as part of pre-deployment safety testing, and omitting these categories would leave a gap in the authorization's coverage. However, subsection (d) conditions the Commerce and State authorizations for radiological and nuclear-related evaluations on the concurrence of both DOE and NRC, with the applicable agency having acted under Section 7 on consistent terms. This ensures that both specialized nuclear agencies have visibility into any authorization of radiological- or nuclear-related AI evaluations, and that the agency whose regulations are implicated retains effective control over whether and under what conditions foreign persons may participate.

SEC. 4. SAFEGUARDS.

(a) SAFEGUARDS REQUIREMENT.—The regulations required by section 3 shall make the availability of the license exception and the exemption contingent on implementation of appropriate safeguards that are risk-based and proportionate to the sensitivity of the information controlled under the Export Administration Regulations or International Traffic in Arms Regulations and the nature of the evaluation activities.

(b) MINIMUM SAFEGUARDS.—The safeguards required by subsection (a) shall include, at a minimum, a requirement that any person relying on the license exception or exemption adopt and follow an effective compliance program, including a technology control plan.

Notes

This section establishes the compliance framework that persons relying on the license exception or exemption must satisfy, striking a balance between meaningful security requirements and operational flexibility. The "risk-based and proportionate" standard in subsection (a) recognizes that AI evaluations vary significantly in sensitivity and that safeguards should scale accordingly.

Subsection (b) specifies a minimum safeguard that must be included regardless of risk levels—i.e., an effective compliance program that includes a technology control plan. This requirement draws on established export control compliance practices, including in guidelines published by BIS and DDTC.[5]

---

[5] *See* U.S. Dep't of State, Bureau of Pol.-Mil. Affs., Directorate of Def. Trade Controls, Off. of Def. Trade Controls Compliance, Int'l Traffic in Arms Regul. (ITAR) Compliance Program Guidelines (Version 1.1, Sept. 19, 2023), at 27-28, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=4f06583fdb78d300d0a370131f961913; U.S. Dep't of Com., Bureau of Indus. & Sec., Export Compliance Guidelines: The Elements of an Effective Export Compliance Program (Jan. 2017), at 21-22 https://www.bis.gov/sites/default/files/documents/ECP_0.pdf.

SEC. 5. REPORTING.

(a) REPORTING REQUIREMENTS.—The regulations required by section 3 shall require, in a form, manner, and frequency specified by such regulations, timely reporting from any person relying on the license exception or exemption.

(b) MINIMUM REPORTING.—The reporting required by subsection (a) shall include, at a minimum—

(1) a point of contact responsible for compliance;

(2) a description of the categories of evaluation activities conducted;

(3) the names of foreign persons who conducted evaluation activities during the reporting period, including their countries of citizenship and country of permanent residence; and

(4) a certification that the safeguards required under section 4 have been implemented.

(c) INCIDENT REPORTING.—The regulations shall also require that any person relying on the license exception or exemption promptly notify the Department of Commerce and the Department of State upon having reason to believe that—

(1) controlled information has been diverted or transferred without authorization; or

(2) a person receiving controlled information has used or is at significant risk of using such information to the detriment of the national security or foreign policy interests of the United States.

Notes

This section establishes reporting requirements designed to provide the Departments of Commerce and State with meaningful oversight of authorization usage without imposing the administrative burden and timing impediments of case-by-case licensing. This approach reflects the policy judgment that periodic, categorical reporting can provide sufficient visibility for compliance and enforcement purposes while preserving the operational benefits of a self-executing authorization.

The reporting obligations under this section are expected to run to the entity making releases under the authorization, not to individual employees acting within their organizational role. Where multiple entities rely on the authorization in connection with the same evaluation activities, such as an AI developer and a third-party evaluator, each entity would report on its own releases.

The minimum reporting categories specified in subsection (b) are tailored to this oversight purpose. A compliance point of contact is responsible for overall compliance with the authorization, including safeguards, reporting, recordkeeping, and other requirements, and this point of contact ensures agency access to responsible personnel; descriptions of evaluation categories provide insight into how the authorization is being used; foreign-person access records enable tracking of who is receiving controlled information and their nationalities; and compliance certifications create accountability for safeguard implementation.

Subsection (c) requires prompt incident reporting for diversions or unauthorized transfers under paragraph (1) and for situations where a recipient has used or poses a significant risk of using controlled information to the detriment of U.S. interest under paragraph (2). The latter may include circumstances such as discovering material misrepresentations, undisclosed foreign government affiliations, or a recipient's subsequent designation on a restricted party list. The "reason to believe" standard is designed to trigger reporting obligations when red flags emerge, without requiring certainty.

SEC. 6. RECORDKEEPING.

(a) RECORDKEEPING REQUIREMENTS.—The regulations required by section 3 shall specify reasonable recordkeeping requirements for any person relying on the license exception or exemption.

(b) LOGGING.— The recordkeeping required by subsection (a) shall include, at a minimum, a requirement that any person that relies on the license exception or exemption and that operates an <u>advanced artificial intelligence system</u> shall maintain logging and monitoring of internal use sufficient to identify when such systems generate controlled information and which individuals access such information.

Notes

This section establishes recordkeeping requirements, thereby creating the evidentiary foundation necessary for effective enforcement. Recordkeeping requirements are essential because license exceptions and exemptions depend on the government's ability to verify compliance after the fact, and records demonstrating adherence to authorization conditions and safeguards serve as the primary audit trail for enforcement purposes.

Subsection (b) addresses a challenge unique to AI models. Unlike traditional export scenarios where controlled items are identified in advance, AI systems may dynamically generate controlled information in ways that cannot be fully anticipated. The logging and monitoring requirement ensures that persons that relying on the authorization and that operate an advanced artificial intelligence system maintain sufficient visibility into when their internal use results in the generation of controlled information and which individuals access that information, enabling internal compliance, self-disclosures, and government oversight. Importantly, the logging and monitoring obligations are not limited to periods when formal evaluation activities are undertaken. Because AI developers continuously iterate on models and foreign persons may access internal systems at any time, logging and monitoring must be maintained on an ongoing basis to ensure there are no gaps in visibility.

SEC. 7. COORDINATION WITH OTHER EXPORT-CONTROL REGIMES.

(a) DEPARTMENT OF ENERGY.—Not later than 180 days after enactment, the Secretary of Energy shall, as appropriate and consistent with the Atomic Energy Act of 1954, issue regulations, a general authorization, or guidance to ensure that Department of Energy controls applicable to assistance or transfers related to nuclear technology (including under 10 C.F.R. part 810, or successor provisions) do not unnecessarily impede evaluation activities, while maintaining appropriate safeguards, reporting, and recordkeeping.

(b) NUCLEAR REGULATORY COMMISSION.—Not later than 180 days after enactment, the Nuclear Regulatory Commission shall, as appropriate and consistent with the Atomic Energy Act of 1954 and NRC export regulations (including 10 C.F.R. part 110, or successor provisions), issue guidance or establish an appropriate authorization mechanism to ensure such controls do not unnecessarily impede evaluation activities, while maintaining appropriate safeguards, reporting, and recordkeeping.

(c) INTERAGENCY CONSULTATION.—In carrying out this section, the Secretary of Energy and the Nuclear Regulatory Commission shall consult with the Secretary of Commerce and the Secretary of State to develop consistent definitions, safeguards, reporting, and recordkeeping to the extent practicable.

Notes

This section recognizes that AI evaluations involving nuclear-related risks may implicate export controls administered by agencies beyond the Departments of Commerce and State. Specifically, the Department of Energy administers controls under 10 C.F.R. Part 810 governing assistance related to nuclear technology, while the Nuclear Regulatory Commission administers export licensing under 10 C.F.R. Part 110 for nuclear equipment and materials. Without coordination, AI developers conducting evaluation activities for nuclear-related risks could face conflicting or overlapping regulatory requirements.

This section directs DOE and the NRC to establish parallel authorization mechanisms consistent with their statutory authorities under the Atomic Energy Act of 1954. The interagency consultation requirement in subsection (c) is designed to promote harmonized definitions and safeguards across the export control system.

SEC. 8. RULE OF CONSTRUCTION; ENFORCEMENT.

(a) RULE OF CONSTRUCTION.—Nothing in this Act limits the authority of the United States to enforce export controls, sanctions, or criminal laws, or to deny, suspend, or revoke eligibility to use the authorization required under section 3.

(b) ENFORCEMENT.—Violations of regulations issued under section 3 shall be subject to the enforcement authorities and penalties available under the Export Control Reform Act of 2018 and the Arms Export Control Act, as applicable.

Notes

This section serves two essential functions. First, subsection (a) is a savings clause ensuring that nothing in the legislation limits existing authorities to enforce export controls, sanctions, or criminal laws, or to deny, suspend, or revoke authorization eligibility. Second, subsection (b) confirms that violations of the implementing regulations are subject to the full range of enforcement authorities and penalties available under the Export Control Reform Act of 2018 (for EAR violations) and the Arms Export Control Act (for ITAR violations), including civil penalties, criminal prosecution, denial of export privileges, and debarment. Together, these provisions make clear that the authorization is a conditional privilege that can be withdrawn and that violations carry serious consequences.

SEC. 9. REPORT TO CONGRESS.

Not later than one year after enactment, and annually thereafter, the Secretary of Commerce and the Secretary of State shall submit a joint report to the appropriate committees of Congress describing implementation of this Act, its utilization, compliance with its requirements, and recommendations for improvements.

Notes

This section establishes a congressional oversight mechanism by requiring an annual joint report from the Secretaries, starting one year after enactment. The report's required contents (implementation, utilization, compliance, and recommendations for improvements) are designed to inform congressional judgment about whether the authorization is achieving its intended purpose of facilitating legitimate evaluation activities, whether safeguards are adequate, and whether legislative modifications are warranted.

Directing the report to "appropriate committees of Congress" encompasses the committees with jurisdiction over export controls, including the Senate Committee on Banking, Housing, and Urban Affairs, the Senate Committee on Foreign Relations, the House Committee on Foreign Affairs, and the House Committee on Financial Services, ensuring that the committees responsible for oversight of the EAR and ITAR receive the information necessary to evaluate this legislation's effectiveness.