

DHS Issues DeepSeek Exclusion and Removal Order Covering Third-Party Products Built With Its Technology

By Gregory Huh | October 23, 2026

RELATED PRACTICES Intellectual Property, AI and Technology, Privacy and Cybersecurity

The Department of Homeland Security (DHS) has published an order, signed by Secretary Markwayne Mullin under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA), that bars DeepSeek and its affiliates from federal civilian procurements.^{1, 2} The order also requires civilian agencies to remove DeepSeek products from their information technology, including “third-party products and services developed using DeepSeek implementations.” Exclusion and Removal Order #2026-01 appeared in the Federal Register on Oct. 20, 2026, nearly three months after its stated July 24 release date. Because the removal mandate covers third-party offerings, it reaches vendors’ products, not just DeepSeek’s own apps.^{1, 2}

Takeaways

- The removal mandate reaches third-party products developed using DeepSeek implementations but does not define that term. Practitioners advising civilian-agency vendors should consider mapping where DeepSeek models, or fine-tuned versions of them, sit in their offerings, including self-hosted, open-weight deployments and documenting the result.
- A FASCSA order can take effect and start its deadlines running well before it appears in the Federal Register. Here, the 60-day exception window, counted from the order’s July 24 release date, closed before publication. Practitioners should be prepared for operative dates that precede publication.
- FAR 52.204-30 turns an order aimed at agencies into inquiry and reporting obligations for contractors. That makes a model’s origin a diligence item in prime contracts and subcontracts.
- Affiliate status turns on the control test of 48 C.F.R. § 2.101, and the order names the company inconsistently. Ownership and control, not branding, decide whether a supplier’s products are covered.

Background

The notice (Docket No. DHS-2026-0628, 91 FR 66346-66350), signed by DHS General Counsel James H. Percival II, was filed for public inspection on Oct. 19 and attaches the signed order.² The order invokes 41 U.S.C. §§ 1321-1328 and 41 C.F.R. part 201-1 and follows the secretary’s review of a Federal Acquisition Security Council recommendation and related evidence. Citing 41 U.S.C. § 1323(c)(5)(A), it explains that the secretary of homeland security issues such orders for civilian agencies to the extent they are not covered by the secretary of defense or the director of national intelligence. It applies to federal civilian executive branch agencies, except for their national security systems and what it calls “secure compartmented information systems” (Federal Acquisition Regulation (FAR) 52.204-30 uses the term sensitive compartmented information systems).^{1, 2, 3}

According to the order's risk summary, DeepSeek's servers are in China, whose legal system gives government cyber and intelligence functions extensive authority to access private company infrastructure. For DeepSeek-hosted instances of the models, account sign-up collects personally identifiable information and may track and digitally fingerprint users. Prompts entered in DeepSeek's most widely used applications may send sensitive data to China if government employees or vendors use them. The models themselves may also contain malware or other vulnerabilities. The order cites research that found multiple critical flaws in DeepSeek's iOS app.^{1, 2}

Analysis

Removal Extends Past DeepSeek's Own Apps

The order does not define "DeepSeek implementation." Its footnotes say only that the procurement exclusion includes third-party DeepSeek implementations used to supply civilian agencies.^{1, 2} That gap matters because DeepSeek's models are open-weight: Their trained parameters are published, so anyone can run them on their own hardware without touching DeepSeek's servers. The order ties its account-data concern to DeepSeek-hosted instances and its malware concern to the models themselves. Its removal text, however, neither distinguishes DeepSeek-hosted from self-hosted deployments nor addresses fine-tuned versions (models further trained on narrower data).

The order is also inconsistent about the company's name. The notice names Hangzhou DeepSeek Artificial Intelligence Co., Ltd; the risk summary inserts "Basic Technology Research" into that name; and the affiliate footnotes, applying the control test of 48 C.F.R. § 2.101, refer to DeepSeek AG.^{1, 2}

Immediate Effect and an Exception Window That Closed Before Publication

Exclusion took effect immediately on issuance and extends to agency-approved product lists, service provider equipment lists and e-commerce markets. Removal is also immediate unless an agency seeks an exception.

Citing 41 C.F.R. § 201-1.304(b), the order lets agencies ask the DHS issuing official for exceptions, such as not applying the order to the agency or to certain actions, or delaying compliance. Requests must be made in writing within 60 days of issuance and must include a compelling justification and any alternative mitigations. Counted from the July 24 release date, that window closed on Sept. 22, 28 days before publication. The order is inconsistent on who reviews exception requests: One passage says the Cybersecurity and Infrastructure Security Agency (CISA), another says DHS. The notice lists CISA's FASCSA Order Implementation Team as its contact. The secretary will review the order within a year and annually thereafter.^{1, 2}

How the Order Reaches Contractors

The order's required actions are addressed to civilian agencies, and it does not mention the Federal Acquisition Regulation.^{1, 2} Contractors are instead bound through FAR 52.204-30, the clause that carries FASCSA orders into contracts; DHS orders govern all solicitations and contracts other than those of Department of Defense contracting offices. Absent a waiver, the clause bars contractors from providing or using, in contract performance, covered articles subject to applicable orders. It requires contractors to check SAM.gov for FASCSA orders at least every three months and imposes reasonable-inquiry and reporting duties, including a report to the contracting officer within three business days of identifying a covered article and a follow-up within 10 business days.

An order issued after the solicitation date applies to an existing contract only once it is added by amendment or modification (see FAR 4.2304(c)), although the clause's inquiry and reporting duties still run. The clause must also be flowed down to all subcontracts, including those for commercial products and services. Through that clause, the order can reach a vendor that built a DeepSeek model into its product, not just an agency using DeepSeek's app.³

Endnotes

1. Department of Homeland Security, Notice of Order Regarding Exclusion and Removal of DeepSeek Products From Federal Civilian Executive Branch Information Technology Systems and Procurements, 91 FR 66346-66350 (Oct. 20, 2026), Docket No. DHS-2026-0628, with appended Exclusion and Removal Order #2026-01, available at <https://www.federalregister.gov/documents/2026/10/20/2026-21447/notice-of-order-regarding-exclusion-and-removal-of-deepseek-products-from-federal-civilian-executive>.
2. FR Doc. 2026-21447, public inspection version (filed Oct. 19, 2026), available at <https://public-inspection.federalregister.gov/2026-21447.pdf>; see also the official GovInfo PDF, available at <https://www.govinfo.gov/content/pkg/FR-2026-10-20/pdf/2026-21447.pdf>, and the signed order in Docket No. DHS-2026-0628 at <https://www.regulations.gov>.
3. FAR 52.204-30, Federal Acquisition Supply Chain Security Act Orders—Prohibition (Dec. 2023), available at <https://www.acquisition.gov/far/52.204-30>.