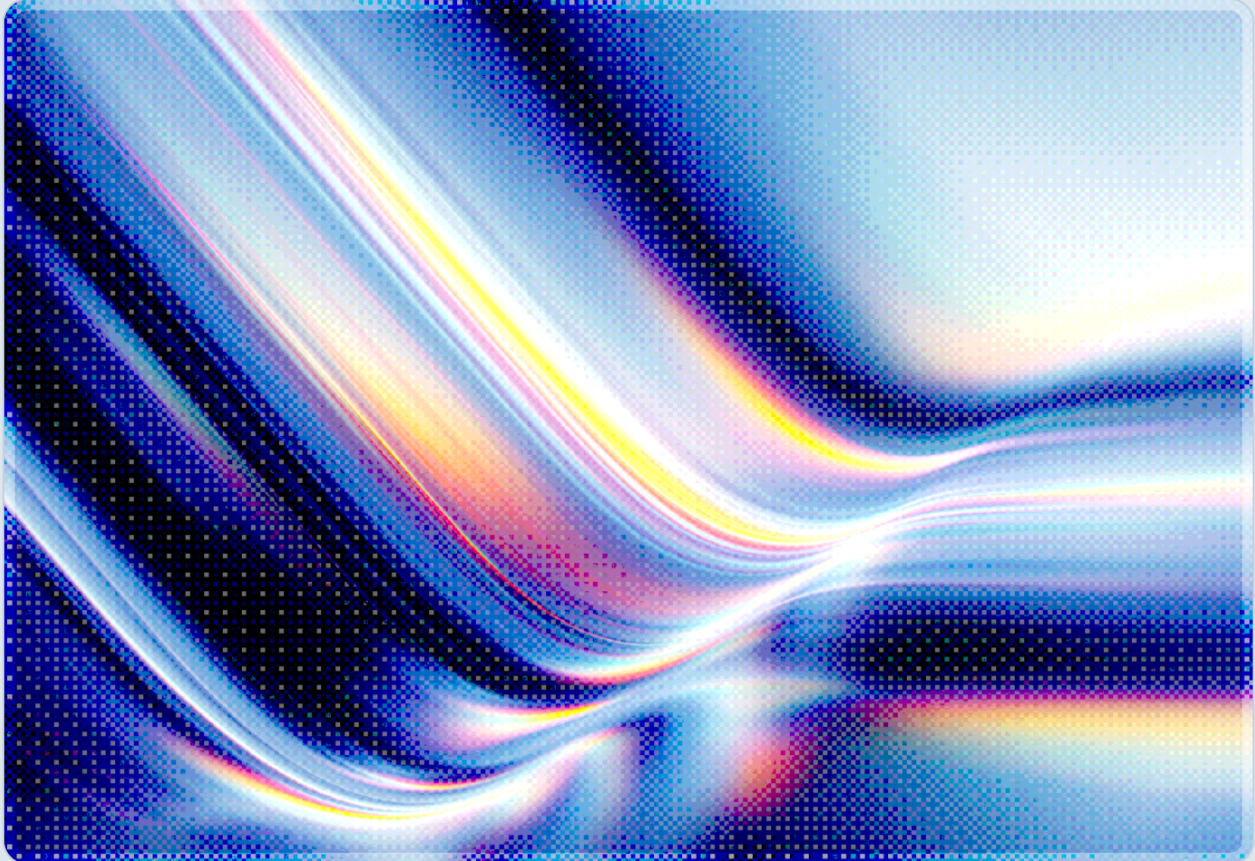


The DeepSeek FASCSA Exclusion Order: Security Implications and Guidance

Third-Party Implementations, Contractor Flow-Down, and the First Civilian Model-Provider Ban

2026-10-24

 AI-assisted Rapid Research



CSAI

cloud
security
alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

On October 20, 2026, the Department of Homeland Security published notice of an order under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA). The order excludes products and services of Hangzhou DeepSeek Artificial Intelligence Co., Ltd. and its affiliates from federal civilian procurements. It also requires removal of "all DeepSeek and DeepSeek-affiliate products, and third-party products and services developed using DeepSeek implementations" from civilian agency information technology [1]. Parallel orders from the Department of War (DoW) and the Director of National Intelligence (DNI) cover the defense and intelligence communities [2]. Together, the three orders are the first government-wide exclusion of an AI model provider under FASCSA, and the DHS order is the first FASCSA exclusion to reach civilian agencies [2][7].

The order's practical reach comes from the third-party clause, not from the DeepSeek brand. DeepSeek publishes its R1 and V3 models as open weights, so DeepSeek technology can sit inside commercial products, self-hosted inference stacks, fine-tuned derivatives, and developer tooling without any visible DeepSeek label [7]. The order does not define "developed using DeepSeek implementations" [2][3]. As a result, agencies and contractors cannot reliably answer the compliance question without model-level provenance data, such as base-model lineage, which is not yet routinely captured or exchanged across commercial AI supply chains [7].

Contractor obligations flow through FAR 52.204-30. Once the clause applies, the prime contractor must make a reasonable inquiry for covered articles and report any identified use, including use identified by subcontractors at any tier, to the contracting officer (or via DIBNet for defense contracts) within three business days, with mitigation details due within ten business days [4]. The clause must be flowed down to subcontracts at all tiers, including commercial ones [4]. Organizations that sell to federal agencies, or that sit anywhere in a federal contractor's AI supply chain, should therefore treat model inventory and model lineage as compliance artifacts with legal consequences.

Background

The FASCSA Authority

FASCSA created the Federal Acquisition Security Council (FASC), an interagency body that assesses supply chain risk in information and communications technology and recommends exclusion or removal actions. The statute gives order-issuing authority to three officials, each with a defined scope. The Secretary of Homeland Security covers federal civilian executive branch systems. The Secretary of Defense, now styled Secretary of War, covers defense systems. The Director of National Intelligence covers the Intelligence Community and sensitive compartmented information systems [4]. The FASC's recommendations are not published, but the resulting orders appear on SAM.gov and, for DHS orders, in the Federal Register [5].

The authority went unused for several years after enactment. The first public FASCSA exclusion and removal order came from ODNI in September 2025. It targeted the Swiss data-protection company Acronis AG, and its scope was limited to Intelligence Community systems [5]. In 2026 the Department of War used FASCSA's separate covered-procurement-action authority under 41 U.S.C. § 4713 against Anthropic. On September 25, 2026, the D.C. Circuit upheld that DoW-specific action and read "supply chain risk" broadly enough that it does not require hostile intent by the supplier [6]. The DeepSeek orders differ from both precedents. They are government-wide exclusion orders against an AI model developer, and the DHS order is the first FASCSA exclusion to bind the roughly 430 civilian departments, bureaus, and independent agencies [7].

The DeepSeek Orders

The DHS notice states that the Secretary acted "following review of the Federal Acquisition Security Council Recommendation and affiliated evidence." The order defines affiliated entities by reference to 48 CFR 2.101. The signed order is filed in docket DHS-2026-0628, and CISA's FASCSA Order Implementation Team is the point of contact [1]. Reporting on the signed order dates it to July 24, 2026, nearly three months before publication [7]. According to that reporting, the 60-day window for agencies to request exceptions, whether a scope limitation, delayed implementation, or an alternative safeguard, closed on September 22, 2026. That was four weeks before Federal Register publication; the order was filed for public inspection, and first reported, on October 19 [3][7]. Because the signed order is reproduced in the Federal Register only as page images, CSA has relied on secondary reporting for these dates. Readers should confirm them against the docket.

The three orders are not identical, and the differences matter for organizations that serve more than one part of government. The following table summarizes what has been publicly reported.

Dimension	DHS (civilian)	DoW (defense)	DNI (intelligence)
Publication	Federal Register, Oct. 20, 2026 [1]	SAM.gov FASCSA listing [2]	SAM.gov FASCSA listing [2]
Stated rationale	"Multiple threat vectors," PRC government access obligations, intelligence value of collected data [2][3]	None stated [2]	None stated [2]
Covered articles	DeepSeek and affiliate products, plus third-party products and services "developed using DeepSeek implementations" [1]	Applications and services that implement a DeepSeek model, regardless of hosting location [2]	Applications and services that implement a DeepSeek model, regardless of hosting location [2]
Excluded systems	National security systems and SCI facilities [7]	Not applicable (order scope is defense systems)	Not applicable (order scope is IC systems)
Contractor vehicle	FAR 52.204-30 [4]	FAR 52.204-30 (reports via DIBNet) [4]	FAR 52.204-30 [4]

All three orders reach contractors through the same clause. Where a solicitation uses Alternate I of FAR 52.204-30, however, the prohibition applies only to the order types (DHS, DoW, and/or DNI) that the contracting officer selects, so contractors should check which authorities their contracts invoke [4].

The DHS rationale, as reported, has three parts. DHS cites technical vulnerabilities in DeepSeek's products, including a statement that the models "may contain malware or other security vulnerabilities." It cites the company's obligation to provide access to the People's Republic of China government. It also warns that data collected through DeepSeek applications and models "could produce actionable intelligence on U.S. persons and/or government agencies" [3]. Publicly documented incidents relevant to these concerns include Wiz Research's January 2025 discovery of an unauthenticated DeepSeek ClickHouse database that exposed more than one million log lines, including chat history and API keys [8].

They also include the House Select Committee on the CCP's April 2025 report alleging that DeepSeek routed U.S. user data to PRC-linked infrastructure [9]. Both incidents, however, concern DeepSeek's hosted services. CSA is not aware of public evidence of malicious code in the released open-weight model files, and the order's extension to self-hosted weights appears to rest on broader supply-chain and lineage concerns rather than on documented artifact-level compromise.

Security Analysis

"Implementations" Turns a Vendor Ban Into a Provenance Problem

A conventional vendor exclusion is mostly a procurement-hygiene exercise: identify contracts with the named company, stop buying, and uninstall its software. The DHS order's third-party clause changes the nature of the task. An agency that has never contracted with DeepSeek may still be running a commercial product whose summarization feature calls a DeepSeek-derived model hosted by a U.S. cloud provider. A contractor may be running an internal coding assistant on a quantized R1 distillation. Neither case involves a DeepSeek invoice, a DeepSeek domain, or a DeepSeek-branded binary. Network monitoring for outbound connections to DeepSeek infrastructure, which DHS reportedly directs as an interim measure [7], will not detect locally hosted weights.

Early legal and press commentary has begun to map the order's boundaries, but significant questions remain. Crowell & Moring reads the DoW and DNI definitions as reaching a DeepSeek model regardless of where it is hosted, including an open-weight instance integrated locally, and reads the DHS language as suggesting that products built with DeepSeek's coding assistant are also covered articles [2]. Tech Times reporting asserts that fine-tuning, distillation, and synthetic-data generation fall within "developed using" while leaving no detectable trace in the final product [7]. As of this writing, CISA has not published guidance on the "developed using" standard [7]. The table below sets out CSA's assessment of how likely common deployment patterns are to fall within scope. It is an interpretive judgment for planning purposes, not a statement of DHS's position.

Deployment pattern	Likely treatment (CSA interpretation)	Rationale
DeepSeek consumer app or hosted API	Covered	Named product of the excluded source

Deployment pattern	Likely treatment (CSA interpretation)	Rationale
Self-hosted DeepSeek open weights (any host)	Very likely covered	DoW/DNI text reportedly reaches models regardless of hosting location, including locally integrated open weights [2]; DHS text, which also covers third-party products "developed using" DeepSeek implementations [1], is broader
Fine-tuned, quantized, or merged DeepSeek derivatives	Likely covered	CSA reads derivatives as "implementations" of the underlying model; no published guidance addresses this
Third-party SaaS feature backed by a DeepSeek model	Likely covered	Fits the plain text of the third-party clause [1]
Models distilled from DeepSeek outputs	Uncertain	No published guidance; depends on how "developed using" is read, though reporting asserts distillation is reached [7]
Software written with assistance from DeepSeek tools	Uncertain	Counsel reads the DHS language as suggesting coverage [2]; most expansive reading, with no CISA guidance

The upper rows of this table describe exposures that organizations can find with existing tooling, provided they look at model artifacts and not just vendor names. The lower rows describe exposures that are hard to detect even in principle. There is currently no widely accepted, reliable method for detecting from weights alone that a model was distilled from DeepSeek outputs, and AI-assisted code is not typically labeled by the tool that produced it [7]. If DHS or CISA ultimately adopts the broader reading, compliance will depend on attestations from suppliers rather than on technical verification. That shift would put new weight on contractual representations about model lineage.

Flow-Down Reaches Into Commercial AI Supply Chains

FAR 52.204-30 is the mechanism that carries the order beyond agency networks. The clause prohibits contractors from providing or using covered articles "as part of the performance of the contract." It requires contractors to search SAM.gov for FASCSA orders at least once every three months. It also requires a reasonable inquiry when a new order could affect their supply chain [4]. The clause defines a reasonable inquiry as a search of information already in the contractor's possession and states that it does not require an internal or third-party audit [4]. That standard sounds modest. However, a contractor whose own AI bill of materials records model families and base models already possesses the relevant information, so a reasonable inquiry would be expected to surface any DeepSeek dependency it records.

The clause must be included in subcontracts at all tiers, including subcontracts for commercial products and services, although the quarterly SAM.gov review is excluded from flow-down [4]. In practice, a federal integrator's obligation becomes a question for every SaaS vendor, model-hosting platform, and AI feature provider in its delivery chain. Once a covered article is identified, whether by the prime contractor or through notification from a subcontractor at any tier, the contractor has three business days to report the contract, the order, and the product details to the contracting officer, or through DIBNet for defense work. Mitigation detail and steps to prevent recurrence are due within ten business days [4]. These timelines are short enough that organizations without a current model inventory are unlikely to meet them through ad hoc investigation.

Precedent Risk Extends Beyond DeepSeek

The order sets a template that is likely to be reused. The D.C. Circuit's Anthropic decision held that "supply chain risk" under FASCSA does not require malicious intent. As reported, it also accepted that the training methodology underlying a model could constrain DoW operations [6]. Taken together with the DeepSeek orders, this suggests that model developers of any nationality may now be subject to procurement-wide exclusion. The orders also show that exclusion can follow a model into downstream products. Organizations that build on a single foundation model family therefore carry a regulatory concentration risk alongside the familiar technical and commercial ones.

The question of notice deserves careful framing. The DoW and DNI orders give no published rationale [2], and the agency exception window reportedly closed before the order was public [7]. The statute does provide procedural protection for the named source: when the FASC issues a recommendation, it notifies affected parties, which have a 30-day period to respond [5]. Even that protection has limits, since the D.C. Circuit treated DoW's failure to follow FASCSA's pre-deprivation procedures in the Anthropic case

as harmless error [6]. Downstream vendors and contractors that merely embed the source's technology receive no comparable notice, and they should assume that future AI-related orders may become binding on them with little warning.

Recommendations

Immediate Actions

Federal agencies and contractors should begin by establishing whether they are already exposed, and most organizations can complete the first steps within days. The starting point is a SAM.gov search for "FASCSA order" to confirm which DeepSeek orders apply to each active contract, with the search date recorded as evidence of the required quarterly review [4]. That contractual baseline should be paired with an inventory of every AI model in use, including self-hosted weights in model registries, container images, and developer workstations. The inventory should record the base model family for each entry, not just the product name, because the third-party clause turns on lineage rather than branding.

Because much of the exposure sits with suppliers, organizations should also ask each AI-enabled SaaS vendor and model-hosting provider supporting federal work for a written statement of which base models power its features. In parallel, compliance teams should prepare the three-business-day report template now, so that any identified DeepSeek dependency can be reported on time [4]. Finally, security teams should block DeepSeek consumer applications and API endpoints at the network and mobile-device-management layers. This control is worth deploying quickly, but it does not address locally hosted weights and should not be treated as evidence of compliance on its own.

Short-Term Mitigations

Over the next one to three months, organizations should replace one-time searches with durable controls. Model provenance should become a required field in software and AI bills of materials. Procurement teams should add representations and warranties on base-model lineage, fine-tuning sources, and distillation sources to AI supplier contracts. These clauses should include a duty to notify when a supplier changes its underlying model. Model registries and artifact repositories should enforce admission policies that reject weights with unverified or excluded lineage. Where a DeepSeek-derived model is removed, teams should assess whether the replacement changes system behavior, evaluation results, or authorization boundaries. A model swap in a FedRAMP or agency-authorized system may itself require security review.

Strategic Considerations

Over the longer term, organizations should plan for a future in which government action, and not only vendor failure or technical compromise, can abruptly make a model unusable. Architectures that abstract the model layer behind a gateway, maintain evaluated fallback models from more than one provider, and keep prompts and fine-tuning data portable are likely to absorb these events at lower cost. Industry bodies and agencies would benefit from a shared, machine-readable convention for declaring model lineage. Without one, each FASCSA order touching AI is likely to trigger the same scramble for attestations. Finally, the unresolved scope of "developed using" deserves direct engagement. Contractors and trade associations should seek written CISA guidance on the scope of "developed using" before making removal decisions that rest on the broadest reading, because over-removal carries mission and cost consequences, including replacing embedded AI features, re-authorizing systems, and disrupting delivery.

CSA Resource Alignment

CSA's **AI Controls Matrix (AICM) v1.1** directly addresses the controls needed to operationalize compliance with this order [10]. Its Supply Chain Management, Transparency, and Accountability domain covers the inventory, supplier assessment, and contractual controls described in this note. Its shared-responsibility model distinguishes AI customers, application providers, and model providers, and that distinction aligns with the tiers that FAR 52.204-30 flow-down now reaches. Organizations can use AICM's implementation and auditing guidelines for each role to document a defensible reasonable inquiry.

CSA's **AI Model Risk Management Framework** describes model cards, data sheets, and risk cards as the core documentation of a model's origin and characteristics [11]. The DeepSeek order converts that documentation from good practice into compliance evidence. A model card that records base model, fine-tuning lineage, and distillation sources is a practical way to answer whether a product was "developed using DeepSeek implementations."

The CSA research note **AISI: Open-Weight Models Close Cyber Capability Gap** documents how quickly open-weight models are approaching closed frontier capability [12]. That trend, alongside permissive licensing and low inference cost, helps explain why open-weight families such as DeepSeek have spread widely into commercial and internal tooling, and why exclusion orders that follow open weights downstream will have broad effects.

Finally, **STAR for AI** provides a mechanism for AI suppliers to publish assessed control information, including supply chain and provenance controls, in a public registry [13]. Federal integrators trying to meet compressed reporting timelines across many vendors may find it useful to require or prefer STAR

for AI-listed suppliers, because it reduces the need for bespoke questionnaires after each new order.

References

- [1] U.S. Department of Homeland Security. "[Notice of Order Regarding Exclusion and Removal of DeepSeek Products From Federal Civilian Executive Branch Information Technology Systems and Procurements.](#)" Federal Register, Vol. 91, No. 201, FR Doc. 2026-21447, October 20, 2026. Also available at [federalregister.gov](https://www.federalregister.gov).
- [2] Crowell & Moring LLP. "[FASCSA Orders Require Exclusion and Removal of DeepSeek AI.](#)" Crowell Client Alert, October 21, 2026.
- [3] Riotta, Chris. "[DHS Bans DeepSeek From Federal Civilian Agencies.](#)" GovInfoSecurity, October 19, 2026.
- [4] Federal Acquisition Regulation (FAR) Council. "[FAR 52.204-30 Federal Acquisition Supply Chain Security Act Orders—Prohibition.](#)" Acquisition.gov, accessed October 24, 2026.
- [5] Mayer Brown. "[DNI Issues First FASCSA Exclusion and Removal Order Against Acronis AG.](#)" Mayer Brown, October 2, 2025.
- [6] Holland & Knight. "[D.C. Circuit Upholds Exclusion of Anthropic from DOW Supply Chain Under FASCSA.](#)" Holland & Knight Alert, September 29, 2026.
- [7] Hill, Terrence. "[DHS Filed DeepSeek Ban 28 Days After Agencies Lost Right to Request Exceptions.](#)" Tech Times, October 20, 2026.
- [8] Wiz Research. "[Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History.](#)" Wiz, January 29, 2025.
- [9] U.S. House Select Committee on the CCP. "[DeepSeek Unmasked: Exposing the CCP's Latest Tool for Spying, Stealing, and Subverting U.S. Export Control Restrictions.](#)" U.S. House of Representatives, April 16, 2025.
- [10] Cloud Security Alliance. "[AI Controls Matrix \(AICM\) v1.1.](#)" Cloud Security Alliance, June 22, 2026.
- [11] Cloud Security Alliance. "[AI Model Risk Management Framework.](#)" Cloud Security Alliance, July 23, 2024.
- [12] Cloud Security Alliance. "[AIS: Open-Weight Models Close Cyber Capability Gap.](#)" Cloud Security Alliance, August 9, 2026.

[13] Cloud Security Alliance. "[STAR for AI Overview](#)." Cloud Security Alliance, January 29, 2025.