

Exclusion and Removal Order #2026-01

Federal Acquisition Supply Chain Security Act Exclusion and Removal of DeepSeek Products and Services from Federal Civilian Executive Branch Information Technology Systems

Original Release Date: July 24, 2026

Applies To: Federal Civilian Executive Branch Agencies except for their national security systems and secure compartmented information systems

FROM: Markwayne Mullin 
Secretary, Department of Homeland Security

CC: Russell Vought
Director, Office of Management and Budget

The Federal Acquisition Supply Chain Security Act of 2018, 41 U.S.C. §§ 1321-1328, and implementing regulations at 41 C.F.R. part 201-1, authorize the Secretary of Homeland Security to issue exclusion and/or removal orders for purposes of safeguarding federal civilian information systems. Recommendations of the Council shall be reviewed by the Secretary of Homeland Security, who may issue exclusion and removal orders based upon such recommendations, to the extent not covered by the Department of Defense [Department of War] or the Intelligence Community. 41 U.S.C. §1323 (c)(5)(A). Section 201-1.304 of the Federal Acquisition Supply Chain Security Act Final Rule states that executive agencies shall comply with exclusion and removal orders issued pursuant to § 201-1.303.

Background:

Information and communications technology are vital to U.S. government systems. The Federal Acquisition Supply Chain Security Act of 2018 created the Federal Acquisition Security Council (FASC) to manage supply chain risks by recommending exclusion or removal of risky products or services from federal procurement and IT systems. The Secretary of Homeland Security can issue exclusion or removal orders for Federal civilian agency systems, except those under the Department of War and the Office of the Director of National Intelligence.

Summary of Risks from Source:

Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. (hereinafter DeepSeek), a foreign, privately-owned company, located in the People's Republic of China¹ (PRC) provides multiple artificial intelligence applications available widely and free of charge.² DeepSeek's models present multiple threat vectors. DeepSeek servers are located in the PRC,³

¹ "Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Company Profile." *exovera.com*, January 31, 2025, https://exovera.com/wp-content/uploads/2025/02/DeekSeek_Profile_2025_01_31-Final.pdf.

² "DeepSeek explained: Everything you need to know." *TechTarget*, August 25, 2025, <https://www.techtarget.com/WhatIs/feature/DeepSeek-explained-Everything-you-need-to-know>.

³ DeepSeek's Privacy Policy, available at <https://web.archive.org/web/-/20250306100653/https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html>; Charles Mok. "Taking Stock of the DeepSeek Shock." *Stanford Cyber Policy Center*, February 5, 2025. <https://cyber.fsi.stanford.edu/publication/taking-stock-deepseek-shock>.

and the PRC legal system permits extensive authority to government cyber and intelligence functions to access private company infrastructure.⁴ For DeepSeek-hosted instances of their models, DeepSeek’s account generation process collects personally identifiable information (PII) and may also track and digitally fingerprint users.⁵ DeepSeek’s most widely used applications function through a prompt-and-response process that requires presenting information to the model, and which may result in the transfer of sensitive data to the PRC if used by U.S. government employees or vendors.⁶ The transfer of the aforementioned information to the PRC, either independently or in combination with publicly available data, could produce actionable intelligence on U.S. persons and/or government programs. The models themselves may contain malware or other security vulnerabilities. Indeed, open-source security research has found that the DeepSeek iOS mobile application contains multiple critical vulnerabilities.⁷

Scope:

This Exclusion and Removal Order direct Federal civilian agencies⁸ to: (1) **exclude** DeepSeek, DeepSeek-affiliated entities⁹, and their products from civilian agency procurements,¹⁰ and (2) **remove** products provided by DeepSeek and DeepSeek entities, and third-party products and services developed using DeepSeek implementations, from civilian agency information technology systems.¹¹

⁴ “Data Security Business Advisory: Risks and Considerations for Businesses Using data services and equipment from firms linked to the PRC.” Department of Homeland Security, December 22, 2020. https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

⁵ DeepSeek’s Privacy Policy, p. 2 is available at <https://web.archive.org/web/-20250306100653/https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html>; *DeepSeek Unmasked: Exposing the CCP’s Latest Tool for Spying, Stealing, and Subverting U.S. Export Control Restrictions*. The Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, April 16, 2025, pp. 3 and n.13 and 14, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/DeepSeek%20Final.pdf>.

⁶ DeepSeek’s Privacy Policy, p. 2 is available at <https://web.archive.org/web/-20250306100653/https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html>.

⁷ Andrew Hoog, “NowSecure Uncovers Multiple Security and Privacy Flaws in DeepSeek iOS Mobile App.” *NowSecure*, February 6, 2025. <https://www.nowsecure.com/blog/2025/02/06/nowsecure-uncovers-multiple-security-and-privacy-flaws-in-deepseek-ios-mobile-app/>

⁸ The Secretary of Homeland Security’s authority to issue exclusion and removal orders is applicable to civilian agencies, to the extent not covered by the authority of the Secretary of Defense and Director of National Intelligence, as defined by 41 U.S.C. § 1323(5)(A)(ii) or (iii).

(ii)The Secretary of Defense, for exclusion and removal orders applicable to the Department of Defense and national security systems other than sensitive compartmented information systems.

(iii)The Director of National Intelligence, for exclusion and removal orders applicable to the intelligence community and sensitive compartmented information systems, to the extent not covered by clause (ii).

⁹ For purposes of this Order, an individual or business is an “affiliated entity” or “affiliate” of DeepSeek AG if, directly or indirectly, either one controls or can control the other; or a third party controls or can control both. *See* 48 C.F.R. § 2.101 (definition of “affiliates”).

¹⁰ To include third party implementations of DeepSeek used to provide products and services civilian agencies.

¹¹ Pursuant to 41 U.S.C. § 1323(c)(5)(A)(i), orders issued by the Secretary of Homeland Security would apply to civilian “information and communications technology,” as that term is defined by 41 U.S.C. § 1321(5).

Required Actions:

All civilian agencies are required to:

1. **Exclude** DeepSeek, DeepSeek-affiliated entities,¹² and their products from civilian agency procurements,¹³ effective immediately after issuance of this Order, to include agency-approved products lists, service provider equipment lists, e-commerce markets, and other similar functions that facilitate the procurement of information technology hardware, software, and services.
2. **Remove products provided by** DeepSeek, DeepSeek-affiliated entities, and third-party products and services developed using DeepSeek implementations, from civilian agency information technology systems¹⁴ immediately after the issuance of the Order, or seek an Exception, as described below.

Exceptions:

Executive agencies may request an exception from the DHS Issuing Official under 41 C.F.R. § 201-1.304(b), such as asking that the order not apply to the agency, certain actions, or for a delay in compliance.

Executive agency requests for exceptions must be **submitted in writing within 60 days** of the issuance of this order and include all necessary information for the issuing official to review and evaluate it, including:

1. Identification of the applicable exclusion order or removal order;
2. A description of the exception sought, including, if limited to only a portion of the order, a description of the order provisions from which an exception is sought;
3. The name or a description sufficient to identify the covered article or the product or service provided by a source that is subject to the order from which an exception is sought;
4. Compelling justification for why an exception should be granted, such as the impact of the order on the agency's ability to fulfill its mission-critical functions, or considerations related to the national interest, including national security reviews, national security investigations, or national security agreements; and
5. Any alternative mitigations to be undertaken to reduce the risks addressed by the exclusion or removal order.

CISA will review requests for exceptions and provide a written approval or disapproval. Please submit any exception requests to FASCSA.Orders@cisa.dhs.gov.

Interim Cybersecurity Measures:

¹² For purposes of this Order, an individual or business is an "affiliated entity" or "affiliate" of DeepSeek AG if, directly or indirectly, either one controls or can control the other; or a third party controls or can control both. *See* 48 C.F.R. § 2.101 (definition of "affiliates").

¹³ To include third party implementations of DeepSeek used to provide products and services to civilian agencies.

¹⁴ Pursuant to 41 U.S.C. § 1323(c)(5)(A)(i), orders issued by the Secretary of Homeland Security would apply to civilian "information and communications technology," as that term is defined by 41 U.S.C. § 1321(5).

During the period between the issuance of this order and full removal of covered articles from agency systems, federal agencies are encouraged to take steps to address risks to their systems, such as monitoring the flow of traffic in and out of the agency, implementing enhanced logging and controls on data exfiltration for the relevant systems, and detecting and flagging anomalous activity.

Actions by DHS and its Cybersecurity and Infrastructure Security Agency (CISA):

1. CISA may provide technical assistance to agencies that are without internal capabilities sufficient to comply with this Order.
2. DHS will review requests for exceptions and provide written approval or disapproval for the department.
3. The Secretary of Homeland Security will review this order as required by the Federal Acquisition Supply Chain Security Act within one year and annually thereafter.

Additional Information:

Contact FASCSA.Orders@cisa.dhs.gov for additional information, assistance, and reporting.