Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Removing PRC Artificial Intelligence Models from Federal Agencies

Updated October 27, 2026

On October 20, 2026, the U.S. Department of Homeland Security (DHS) issued a *Notice of Order Regarding Exclusion and Removal of DeepSeek Products from Federal Civilian Executive Branch Information Technology Systems and Procurements* in the *Federal Register*. This notice requires federal civilian executive branch (FCEB) departments and agencies to bar products made by DeepSeek—a firm headquartered in the People's Republic of China (PRC)—from their networks and to remove any DeepSeek products that may have already been deployed. The DHS order follows a similar action made by the Department of Defense (DOD, which is "using a secondary Department of War designation," under Executive Order 14347) on September 8, 2026. The Director of National Intelligence (DNI) issued a similar order concurrently with DHS. This In Focus discusses these actions and their implications related to supply chain security.

Overview of DeepSeek

Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. (DeepSeek) is an artificial intelligence (AI) company located in the PRC. DeepSeek develops open-weight large language models (LLM), such as (the eponymously named) DeepSeek and DeepSeek-R1.

DeepSeek's AI products have been noted for their general and cost efficiency. While their models are not as powerful as U.S. models, DeepSeek's models have cheaper token costs, can perform tasks quickly, and can be downloaded, hosted, and customized. Because of this price-to-performance advantage, some U.S. companies have adopted DeepSeek's (and other PRC AI) models.

The U.S. government issued warnings about the risks of PRC AI models and their adoption. The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) have said that DeepSeek and its peer companies have carried out large-scale distillation campaigns (e.g., the systemic querying of an AI model and using its responses without authorization to train another model) on U.S. models to develop their products. Further, the National Institute of Standards and Technology's (NIST's) Center for AI Standards and Innovation (CAISI) found that DeepSeek's AI models are more prone to *jailbreaking*, more likely to follow malicious commands than U.S. models, and more often provided users with narratives consistent with messaging from the Communist Party of China (CPC).

DeepSeek models are available to U.S. users through several pathways. They can be accessed directly from DeepSeek (e.g., from its mobile application) or through domestic cloud service providers and AI platforms, or it can be downloaded and run on a user's hardware.

Select Legislative Actions on DeepSeek

The National Defense Authorization Act for Fiscal Year 2026 (enacted December 18, 2025) requires that DOD issue an exclusion and removal order for DeepSeek technologies. That order was issued on September 8, 2026. The Department of the Air Force issued an exclusion and removal order on July 10, 2025.

The U.S. House of Representative's Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Select Committee on China) issued a report on risks from DeepSeek and the company's actions to subvert U.S. policy on April 16, 2025. The House Committee on Science Space and Technology held a hearing on DeepSeek on April 8, 2025.

Exclusion and Removal Order

The *Federal Register* notice for the DHS order on DeepSeek products includes a copy of *Exclusion and Removal Order #2026-01* from July 24, 2026. It states that DeepSeek poses risks to the United States for several reasons:

- The company is subject to PRC laws, including the 2017 cybersecurity law (which could allow the government to compel disclosure of sensitive information from DeepSeek).
- Signing up for a DeepSeek account would require the collection of personally identifiable information (PII).
- DeepSeek collects inputs and outputs, which could result in sensitive information being transmitted to U.S. adversaries.
- Any information leaked through DeepSeek could be used, or combined and used, with other information for actionable intelligence against the United States.

DHS also raises concerns that DeepSeek's applications (such as the aforementioned mobile application) are configured in ways that are insecure.

Because of these risks, federal departments and agencies are required to bar DeepSeek, its affiliated entities, and their products from procurements. Further, any previously acquired products must be immediately removed. This order extends to federal contractors and firms doing business with the prime contractor.

Agencies may petition CISA for an exception to this order. Further, CISA will assist agencies in implementing the order. The order suggests that it should be reviewed within a year and annually thereafter.

This is the first time that DHS has exercised its authority to issue exclusion and removal orders—a tool to mitigate supply chain risks at federal agencies.

Authority to Combat Technology Risks

The U.S. government has taken several actions since 2017 to address potential foreign cyber technology risks. In September 2017, DHS issued a Binding Operational Directive ordering the removal of Kaspersky-branded software products from federal agency use. In December 2017, Congress passed a statute codifying that directive.

Recognizing that foreign adversaries may seek to use information and communications technology (ICT) supply chains to compromise organizations, Congress sought to create a repeatable process for restricting potentially dangerous ICT from federal agencies. A precursor bill was debated and passed in the Senate before being enacted as the Federal Acquisition Supply Chain Security Act of 2018 (Title II of the SECURE Technology Act of 2018). This act, among other actions, created the Federal Acquisition Security Council (FASC).

Federal Acquisition Security Council

The FASC is an interagency body that serves as a government-wide forum to identify, assess, and manage ICT supply chain risks to the federal government. It can recommend that federal agencies exclude particular entities and products from federal procurement because they pose an unacceptable risk to national security.

Per the FASC's implementing rule, a senior official from the Office of Management and Budget (OMB) chairs the FASC. Other members include the General Services Administration (GSA), DHS, CISA, the DNI, the National Counterintelligence and Security Center (NCSC), the Department of Justice (DOJ), the FBI, DOD, NSA, the Department of Commerce, and NIST. These agencies provide the council with procurement, cybersecurity, intelligence, law enforcement, national security, and technical expertise.

U.S. government agencies may refer cases to the FASC. The FASC may investigate such cases and coordinate across federal departments and agencies (not just FASC members) on the risk posed by the product or company, develop and recommend potential remedies to address those risks, and (if necessary) issue requirements for agencies to exclude certain vendors or products from federal networks and remove such vendors or products.

Exclusion and removal orders are issued by DHS for the FCEB, DOD for the military, and the DNI for the intelligence community (IC). All three agencies need not coordinate combined orders. The first exclusion and removal orders issued under this authority were by DNI and DOD (almost a year apart) for Acronis—a cybersecurity firm. DHS issued a similar order on October 27, 2026.

The recent orders against DeepSeek are the first time that all three agencies have issued similar orders in close succession and the first time that DHS has exercised this authority.

Considerations for Congress

The exclusion and removal orders issued by DOD, DNI, and CISA may spark interest among policymakers on what further actions Congress may take to combat the threat from DeepSeek, other PRC firms, and cyber supply chain risk management in both the public and private sectors.

Congress may seek to conduct oversight. The DeepSeek orders provide Congress a case study on the efficacy and utility of the FASC. Congress may choose to ask the Comptroller General (GAO), or the inspectors general for DHS, DOD, and the IC to evaluate the FASC's implementation of the DeepSeek order as well its broader operations, including processes for referrals, coordinating and evaluating risk across the interagency, and barriers to issuing orders. GAO has previously assessed the FASC's establishment and DOD's support.

The FASC limits federal procurement but does not restrict nongovernmental access to and use of DeepSeek. Congress may choose to consider the extent to which the Federal Acquisition Regulation's extension of prohibitions to contractors creates a broader disincentive for the private sector to adopt the barred companies. (For example, when Congress barred Huawei Technologies Company and ZTE Corporation telecommunications equipment from servicing the government, it served as a disincentive for wider adoption in the private sector.) Congress may also choose to consider whether a federal prohibition for a cloud service provider (CSP) that contracts with federal government extends to the nonfederal instances of the services that a CSP provides.

Relatedly, Congress might evaluate the risks that DHS, DOD, and the DNI determined regarding DeepSeek products and consider whether broader U.S. use restrictions are needed. Congress might also assess whether other PRC firms or technologies also merit scrutiny. While the FASC can create vendor prohibitions for the federal government, other departments and agencies can act broadly across the economy. For example, the Secure and Trusted Communications Networks Act of 2019 authorizes the Federal Communications Commission (FCC) to prevent communications equipment that poses national security risks from being deployed on U.S. networks. The FCC implements this through its Covered List. Congress may choose to examine the extent to which the FASC and other federal agencies have sufficient authority to combat transnational security risks from technology (e.g., AI).

While the FASC process seeks to protect the federal government against ICT supply chain threats through procurement policy, those same threats extend to state, local, tribal, and territorial governments; the private sector; academia; and other nongovernmental organizations. Congress could also assess whether new authorities are needed to ensure adequate identification, analysis, and mitigation of ICT supply chain risks across the nation and whether agencies can efficiently work on whole-of-government approaches to ICT supply chain security and threat mitigation.

Chris Jaikaran, Specialist in Cybersecurity Policy

IF13336

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.