SITUATIONAL REPORTS

Why Has the US Banned DeepSeek? China's AI Security Risks Explained

Author: CNAWS Research Team • **Published:** October 21, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

The United States has formally prohibited the use of artificial intelligence products developed by Chinese company DeepSeek across federal civilian executive branch information technology systems. The decision, published in the Federal Register on 20 October 2026, requires government agencies to remove DeepSeek-related products and services from their systems and excludes them from future procurement. Significantly, the restrictions also extend to third-party applications and services developed using DeepSeek implementations.[1] Although the announcement attracted international attention this week, the underlying directive was issued by the Department of Homeland Security (DHS) on 24 July 2026. Its publication has brought renewed scrutiny to the security implications of integrating foreign-developed artificial intelligence into government operations. Washington's concerns extend beyond conventional cybersecurity vulnerabilities. American authorities have identified potential risks involving the transfer of sensitive government information to China, the collection of intelligence on American officials and institutions, and vulnerabilities within AI applications and their supporting infrastructure. The decision does not constitute a nationwide prohibition on DeepSeek for American citizens or private companies. Instead, it represents a targeted government procurement and information-security measure. Nevertheless, its implications are broader, highlighting how artificial intelligence platforms are increasingly being evaluated as potential national security vulnerabilities rather than merely commercial software products.

What Has the United States Restricted?

The DHS order, designated Exclusion and Removal Order No. 2026-01, was issued under the Federal Acquisition Supply Chain Security Act of 2018 following a recommendation from the Federal Acquisition Security Council. The legislation allows federal authorities to restrict information technology products and services considered potentially harmful to government supply-chain security.

The directive identifies Hangzhou DeepSeek Artificial Intelligence Co., Ltd., its affiliated entities and third-party products incorporating DeepSeek implementations. Federal civilian executive agencies are required to exclude covered products from new procurement and remove existing implementations from their information technology environments.

The order also provides an exception mechanism through which agencies may seek permission to retain particular products or obtain additional time for compliance. Such requests must be justified and reviewed by DHS. [2]

Importantly, the directive applies to federal civilian executive agencies, with exclusions for specified national security and sensitive compartmented information systems that fall under separate authorities. The publicly available order does not establish a general prohibition across the American private sector.

Its coverage of third-party products is particularly significant. An American software provider using DeepSeek technology within its application could fall within the procurement restrictions even if the product itself is developed and distributed by an American company.

This reflects Washington's concern with the technological components embedded within software systems, rather than exclusively with the identity of the company selling the final product.

Why Does Washington Consider DeepSeek a Security Risk?

The American government's concerns can be understood through three interconnected dimensions involving data exposure, cybersecurity vulnerabilities and the potential intelligence value of AI interactions.

Data Collection and Chinese Jurisdiction

DeepSeek's own privacy policy, updated in February 2026, states that its services can collect user inputs, uploaded files, photographs, voice inputs, chat histories, account information and device-related data. The policy further explains that personal data is collected, processed and stored in the People's Republic of China. It also describes circumstances in which information may be shared with public authorities to comply with applicable legal obligations. [3]

For ordinary consumers, such data collection presents familiar privacy and confidentiality concerns associated with cloud-based AI services. For government employees, however, the potential consequences can be considerably greater.

An official using an AI chatbot to summarise internal correspondence, analyse an unpublished policy document or prepare an administrative assessment could inadvertently transfer sensitive information into infrastructure outside the government's direct control.

The DHS assessment specifically warns that DeepSeek-related data could be combined with publicly available information to generate actionable intelligence on American individuals and government programmes.

This does not establish that DeepSeek has systematically supplied American government information to Chinese intelligence agencies. Rather, Washington's assessment identifies a credible potential exposure arising from the location of data processing, applicable legal jurisdiction and the information collected through AI interactions.

Cybersecurity Vulnerabilities

The second concern involves weaknesses in DeepSeek applications and their supporting software.

In February 2025, mobile security company NowSecure published a technical assessment identifying multiple security and privacy weaknesses in the DeepSeek iOS application. Its researchers reported insecure transmission of certain device and registration data, weaknesses involving encryption keys and outdated cryptographic methods, insecure local storage and extensive device-fingerprinting capabilities. The investigation also documented communications with infrastructure associated with Chinese technology companies. ?

These findings provided concrete evidence that at least one version of the DeepSeek mobile application contained exploitable security weaknesses.

However, the February 2025 assessment should not be interpreted as proof that every subsequent DeepSeek application or model retained identical vulnerabilities. Nor does the presence of software vulnerabilities automatically establish deliberate espionage.

The more significant lesson is that artificial intelligence services introduce several potential attack surfaces, including the mobile application, authentication systems, external servers, application programming interfaces and integrations with third-party software.

For government institutions handling confidential information, weaknesses at any of these levels can create opportunities for unauthorised access, surveillance or data compromise.

Intelligence Collection Through AI Interactions

The third concern is the intelligence value of information generated through routine interactions with AI systems.

Traditional cyber espionage generally involves gaining unauthorised access to devices, networks or stored information. AI services can create an additional collection opportunity because users voluntarily submit information to obtain assistance.

A single prompt may appear harmless. However, repeated interactions involving official responsibilities, internal documents, professional networks, technical problems or institutional decision-making could reveal patterns that are valuable for intelligence analysis.

Such information, if accessible to a hostile intelligence service, could potentially support profiling, identification of individuals handling sensitive responsibilities or the reconstruction of organisational activities.

This risk is not exclusive to Chinese AI platforms. It applies to externally hosted AI services whenever sensitive information is submitted without appropriate controls. The significance of DeepSeek's Chinese jurisdiction lies in the additional trust and legal-access concerns identified by Washington.

Does the Restriction Apply to DeepSeek's Open-Weight Models?

A critical distinction exists between accessing DeepSeek through its official cloud services and running independently deployed copies of its publicly available model weights.

When a user accesses DeepSeek's hosted services, data is processed according to the provider's infrastructure and applicable privacy policies. Conversely, an organisation operating model weights within a properly isolated domestic infrastructure can exercise greater control over data storage, network connectivity and access permissions.

Independent deployment therefore does not necessarily involve transmitting prompts to servers in China.

However, local deployment does not automatically eliminate security concerns. Organisations must still assess downloaded model files, software dependencies, external connections, model behaviour, update mechanisms and possible vulnerabilities in the surrounding applications.

The American order's inclusion of third-party DeepSeek implementations shows that the government's restriction is broader than simply blocking access to a Chinese-hosted chatbot.

For intelligence and defence institutions, this distinction is fundamental. The security of an AI system depends not only on where its data is stored but also on the provenance of its components, the integrity of the software environment and the ability to independently verify its behaviour.

China Rejects the American Restrictions

Beijing strongly criticised the decision on 20 October. China's Ministry of Commerce described the restrictions as discriminatory and accused Washington of undermining the interests of Chinese technology companies.

The ministry argued that the measure disregarded understandings reached between the American and Chinese leadership and urged the United States to reverse its decision. It also called for continued engagement through the existing China–US artificial intelligence dialogue mechanism. ?

The disagreement comes amid intensifying technological competition between the two countries. Washington has pursued restrictions involving advanced semiconductors and Chinese technology suppliers, while Beijing has increasingly emphasised technological self-reliance and control over strategically important technologies.

On 16 October, China separately proposed changes to its technology export-control catalogue covering advanced artificial intelligence and other sensitive technologies. Those proposals remained subject to consultation and should not be confused with the already-issued American DeepSeek order. ?

The emerging pattern suggests that competition over AI is extending beyond the development of more capable models. Governments are increasingly examining where AI systems originate, who operates their infrastructure, which jurisdictions govern the data and how technological dependencies might affect national security.

India Has Already Recognised the Risk

India faces similar considerations as artificial intelligence becomes increasingly integrated into government administration, research, commercial operations and security-related activities.

In January 2025, India's Ministry of Finance issued an internal advisory asking employees to avoid using AI tools, including DeepSeek and ChatGPT, for official purposes because of concerns surrounding the confidentiality of government documents and data. Reuters verified the advisory through ministry officials, although it could not establish whether equivalent instructions had been issued across all ministries. ?

The significance of the Indian advisory lies in its emphasis on the risks of unauthorised AI use, irrespective of whether the service originates in China or elsewhere.

The American decision provides a further illustration of the challenges confronting governments that seek to adopt powerful and inexpensive AI capabilities while protecting sensitive institutional information.

For India, such risks deserve particular attention in organisations dealing with defence procurement, intelligence assessments, critical infrastructure, strategic research and government decision-making.

A government employee or researcher using an externally hosted AI application to process confidential material could expose information without any conventional network intrusion taking place.

Therefore, a security framework based exclusively on blocking malicious websites or preventing unauthorised access to government networks may be insufficient. Institutions also require policies governing the classification of information submitted to AI models, approval of external AI services and the monitoring of third-party AI integrations.

Australia offers one relevant precedent. In February 2025, its government formally directed public-sector entities to prevent the installation or use of DeepSeek products and remove existing instances from government systems and devices. ?

For India, the policy objective should be to distinguish legitimate AI adoption from uncontrolled exposure of sensitive information. Developing and deploying domestically governed AI infrastructure, verifying foreign models before integration and maintaining clear data-handling rules would strengthen institutional resilience without requiring an indiscriminate rejection of foreign technology.

Strategic Assessment

The United States' restrictions on DeepSeek reflect a wider shift in the perception of artificial intelligence from a productivity tool to a potential component of the intelligence and cybersecurity threat environment.

Three developments are particularly significant.

First, AI platforms are becoming potential repositories of strategically valuable information. Unlike traditional databases, these systems can accumulate detailed contextual information about users, their responsibilities, institutional activities and documents through seemingly routine interactions. The intelligence value of such information may emerge through aggregation rather than any individual disclosure.

Second, the restriction of third-party DeepSeek implementations indicates that governments are beginning to examine AI supply-chain exposure at the model level. An application may be developed domestically while relying on foreign-origin models, external infrastructure or software components. Its national security implications therefore cannot be determined solely by the nationality of the final software provider.

Third, the decision illustrates the increasing importance of technological sovereignty. Countries seeking to integrate AI into sensitive government functions must consider not only model capability and cost but also the jurisdiction governing data processing, the transparency of software components and the feasibility of secure independent deployment.

CNAWS assesses with high confidence that the American restrictions represent a substantive expansion of government AI supply-chain controls. The legal scope and procurement requirements are directly established by the published order.

However, the publicly available evidence does not demonstrate that DeepSeek has conducted a systematic intelligence collection operation against American federal agencies. The potential for Chinese state access, together with documented application vulnerabilities and data-governance concerns, forms the basis of Washington's preventive security assessment.

The distinction is important. A product may present an unacceptable exposure for sensitive government operations without there being public evidence that it has already been used for state-directed espionage.

Outlook and Indicators to Monitor

The next phase will depend on the practical implementation of the order and the extent to which federal agencies identify DeepSeek technology embedded within existing software.

The most relevant indicators include the granting of exceptions, the removal of third-party implementations, new federal procurement restrictions affecting other foreign-origin AI models and additional technical findings concerning DeepSeek's security architecture.

International responses will also be important. Further restrictions by governments in Europe and the Indo-Pacific could indicate a broader movement towards more tightly controlled public-sector AI ecosystems.

For India, the immediate requirement is to assess how externally developed AI systems are being used across sensitive institutional environments and whether existing approval and data-handling procedures adequately address model-level and third-party risks.

CNAWS Assessment

The DeepSeek restrictions are not simply another episode in the commercial rivalry between American and Chinese technology companies. They reveal a fundamental challenge for governments entering the age of widespread artificial intelligence adoption.

AI services can improve administrative efficiency and analytical capacity while simultaneously creating new pathways through which confidential information, institutional knowledge and user behaviour become accessible outside established security boundaries.

The central national security question is no longer merely whether an AI model is accurate, inexpensive or technologically advanced. It is whether the state can independently control, verify and secure the system through which sensitive information is processed.

For India, this challenge is particularly relevant as artificial intelligence becomes increasingly embedded in public administration, strategic research and defence-related decision-making.

CNAWS assesses that establishing secure AI procurement standards, verified model deployment environments and institutional data-protection protocols will become an increasingly important component of national security planning.

The American decision demonstrates that AI sovereignty is no longer determined solely by the ability to develop indigenous models. It also depends on maintaining effective control over the infrastructure, software components and data flows underpinning their use.

Endnotes

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* 91, no. 201 (October 20, 2026): 66346–66350. Official Federal Register.

2. U.S. Department of Homeland Security, “Exclusion and Removal Order No. 2026-01,” July 24, 2026, appendix to the notice published October 20, 2026. Official Order PDF.

3. Hangzhou DeepSeek Artificial Intelligence Co., Ltd., “DeepSeek Privacy Policy,” updated February 10, 2026. DeepSeek.

4. Andrew Hoog, “NowSecure Uncovers Multiple Security and Privacy Flaws in DeepSeek iOS Mobile App,” *NowSecure*, February 6, 2025. NowSecure.

5. Reuters, “China Says US' DeepSeek Ban Disregards Xi-Trump Consensus,” October 20, 2026. Reuters.

6. Reuters, “Beijing Seeks Tighter Grip on AI Exports amid US Rivalry,” October 16, 2026. Reuters.

7. Sarita Chaganti Singh and Nikunj Ohri, “India's Finance Ministry Asks Employees to Avoid AI Tools Like ChatGPT, DeepSeek,” *Reuters*, February 5, 2025. Reuters.

8. Australian Government, Protective Security Policy Framework, “Direction 001-2025 on DeepSeek Products, Applications and Web Services,” February 4, 2025. Australian Government.