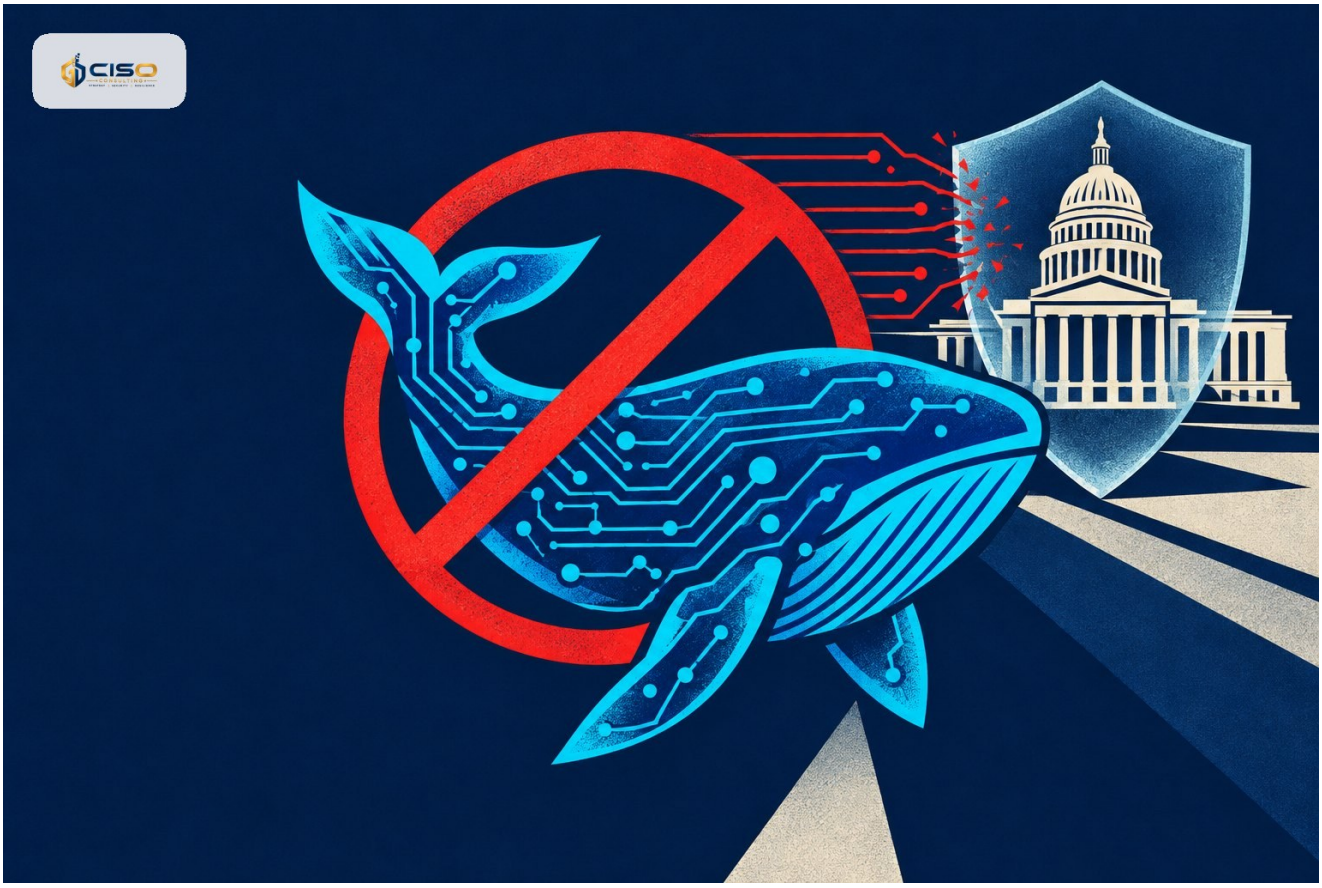
US DHS orders federal civilian agencies to remove DeepSeek products



DHS has ordered US federal civilian agencies to stop buying and using DeepSeek products, including affiliates' and derived third-party services, citing data-access and security concerns. The order is not a general ban on private use.

- Agencies must exclude DeepSeek products from procurement and remove them from IT systems, or request an exception.
- The scope includes affiliates' products and third-party services built on DeepSeek technology.
- Exception requests are due within 60 days; CISA will approve or deny them in writing.
- DHS cites concerns about Chinese government access, personal data collection and transfer of sensitive government data.
- The order applies to federal civilian agencies and is not a general ban on private or consumer use.

The US Department of Homeland Security (DHS) has issued an order requiring federal civilian agencies to stop using DeepSeek products and remove them from government systems. The order was published in the Federal Register.

What the order requires

Agencies must immediately exclude covered products from procurement, including approved-product lists and purchasing marketplaces. They must also remove them from IT systems or seek an exception. Exception requests are due within 60 days of issuance and must give a justification and proposed risk mitigations. CISA will review each request and respond in writing. Agencies that cannot comply because of internal capability limits can receive technical assistance from CISA.

Coverage extends beyond DeepSeek's own chatbot and API services. It also includes products from affiliates and third-party products or services built using DeepSeek technology.

Why DHS acted

DHS points to concerns that the Chinese government could access DeepSeek infrastructure, collect personal information, track users, and potentially receive sensitive government data. The order also raises the possibility of malware in DeepSeek models. It cites a February 2025 NowSecure report on the DeepSeek iOS app, which found unencrypted data transmissions, weak encryption, insecure local storage, user fingerprinting risks and data sharing with ByteDance.

The order applies only to federal civilian agencies under DHS authority. It is not a general ban on private or consumer use, and it does not bind Saudi organisations. It is nonetheless a useful reference point for how a government treats third-party AI services and the products built on them.

What to do now

1. Inventory AI tools, APIs and embedded models in use, including those staff adopt without approval, and identify any that rely on DeepSeek technology.
2. Check third-party and SaaS products for underlying DeepSeek models, and ask vendors to disclose the AI services they depend on.
3. Set a policy on external AI services that covers data classification, permitted data types and approval before use.
4. Assess where confidential or personal data could reach overseas AI services, and review this against PDPL cross-border transfer requirements.
5. Add AI service assessment to third-party risk reviews and procurement checks, in line with NCA ECC third-party requirements.