

CYBER SECURITY - FOREIGN-OWNED TECHNOLOGY

HEADLINE

- The Government continues to assess Australia's technology security policy settings to ensure they remain fit for purpose and is bringing forward a range of measures under the 2023-2030 Australian Cyber Security Strategy.

KEY POINTS:

- The Australian Government is committed to keeping Australians safe and will make decisions based on our own interests and on the advice of our security agencies.
- On 4 February 2025, the Secretary of the Department of Home Affairs issued a mandatory Direction under the Protective Security Policy Framework to prevent the access, use or installation of DeepSeek products, applications and services from all Australian Government systems and devices.
- Based on risk and threat information from national security and intelligence agencies the Secretary determined that DeepSeek poses an unacceptable risk to the Australian Government's technology estate.
 - Like all digital systems, AI presents both opportunities and risks. DeepSeek retains significant amounts of data to train its AI model. This data is also subject to foreign control and influence risks.
- The Direction requires all non-corporate Commonwealth entities to:
 - Identify and remove all existing instances of DeepSeek products, applications and services on all Australian Government systems and mobile devices;
 - Prevent the access, use or installation of DeepSeek;
 - Report back on completion of these requirements.
- I encourage the community and Australian businesses to consider their own security arrangements to ensure they are engaging with AI in a safe and responsible way.
 - Advice can be found on [Cyber.gov.au](https://www.cyber.gov.au) and from the Office of the Australian Information Commissioner.
- The Australian Government has brought forward a range measures under the 2023-2030 Australian Cyber Security Strategy to strengthen the nation's resilience against technology-related harms.
 - s. 22(1)(a)(ii)

○ s. 22(1)(a)(ii)
○

• s. 22(1)(a)(ii)
•

s. 22(1)(a)(i)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s. 22(1)(a)(ii)

Restriction of DeepSeek and affiliated applications on Government-issued devices

- On 29 January 2025, the Department of Home Affairs issued policy advice to non-corporate Commonwealth entities reminding them of their PSPF obligations to appropriately manage the risks of foreign ownership, control and influence in technology assets to protect the Australian Government from unlawful activities.
- The Australian Government recognises the importance of AI to Australia's economy and is taking an integrated approach to mitigating the risks of AI while supporting innovations in its development and deployment.
 - The Department of Industry, Science and Resources leads efforts on safe and responsible use of AI across the economy.
 - In December, the Australian Government announced the development of a comprehensive National AI Capability Plan. This initiative aims to unlock the nation's full potential in AI, drive economic growth, address critical national priorities and position Australia as a global AI leader.

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

- 'DeepSeek poses security risk like Huawei and TikTok, Labor warned', *The Australian Financial Review*, 28 January 2025: Reports that Former Home Affairs Department secretary Michael Pezzullo and Strategic Analysis Australia director Michael Shoebridge have urged the Albanese government to impose stringent controls on the use of on DeepSeek.
- 'Be careful': Australian ministers urge caution over AI app DeepSeek', *SBS News*, 29 January 2025: Australia's science minister has raised privacy concerns over China's breakout AI chatbot DeepSeek, urging users to think carefully before downloading it.
- 'Ban is likely if new app is found to be unsafe', *The Australian*, 30 January 2025: Reports that the Australian government would follow a TikTok-style ban on DeepSeek and Special Envoy for Cyber Security Andrew Charlton is quoted.