

Background / Thematic Brief – Cyber UK and EU

Contents

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

Directions on DeepSeek, Kaspersky and TikTok 8

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

Directions on DeepSeek, Kaspersky and TikTok

Key points

- The Department considers risk and threat information from national security and intelligence agencies and has determined that certain applications, products and services pose an unacceptable security risk to Australian Government networks, data and information due to real and potential threats of foreign interference, espionage and sabotage. This is because they extensively collect user data which may be exposed to extrajudicial directions from a foreign government.
- Under the Protective Security Policy Framework (PSPF) the Department has issued three mandatory Directions on vendors of concern that extensively collect user data which may be exposed to extrajudicial directions from a foreign government, including:
 - Direction 001-2023 on the TikTok application – issued 4 April 2023.
 - Direction 001-2025 on DeepSeek Products, Applications and Web Services – issued 4 February 2025.
 - Direction 002-2025 on Kaspersky Lab, Inc. Products and Web Services – issued 21 February 2025.
- The Directions require non-corporate Commonwealth entities to:
 - Identify and remove existing instances of the products, applications and web services
 - Prevent the access, use or installation of the products, applications and web services on all Australian Government systems and mobile devices, and
 - Report completion of the Direction requirements to the Department of Home Affairs.
- The Australian Government continues to assess Australia's technology security policy settings to ensure they remain fit for purpose, including through the 2023-2030 Australian Cyber Security Strategy (the Strategy) and the finalisation of the Technology Vendor Review Framework.
- The Department of Home Affairs has also published the Foreign, Ownership, Control or Influence Risk Assessment Guidance to support public and private organisations assess technology vendor security risks in their supply chain and procurements.
- These measures are not targeted at any particular vendor or country, but rather, focus broadly on protecting the data integrity and security of Australian Government systems and devices.
- These initiatives also act as strong policy signals to critical infrastructure operators, other Australian governments including states and territories, and more broadly to Australian organisations and businesses.

Background

- DeepSeek's privacy policy outlines that it transmits and collects significant amounts of information from its users to train its AI model, with this information being stored in data centres owned and operated overseas.
- TikTok collects significant quantities of user data that is stored in overseas data centres that reside outside of Australia's protected technology estate and this extensive collection of data may be exposed extrajudicial directions from a foreign government.
- For Kaspersky Lab, Inc.'s applications and products to be effective as anti-virus software, they must be highly intrusive within a network so they can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction and this extensive collection of data may be exposed extrajudicial directions from a foreign government. The emergence of technologies like DeepSeek highlights the rapid pace of AI development. Australian companies are also demonstrating incredible innovation, harnessing the huge potential of AI.
 - The [National AI Capability Plan](#) will build on this Australian innovation and know-how and make sure we have the foundations for growth and to support our economic resilience.
- The Australian Government is engaging internationally to ensure the global governance of AI strengthens safe and responsible practices internationally, reflecting our democratic values and respect for human rights. This includes our work as part of the global network of AI Safety Institutes, our support for safe and responsible AI adoption in the region, and our contributions to advancing the international understanding of the science of AI safety through the International Scientific Report on the Safety of Advanced AI.

Background / Thematic Brief – Cyber UK and EU

This page has intentionally been left blank.

Directions on DeepSeek, Kaspersky and TikTok

Key points

- The Department considers risk and threat information from national security and intelligence agencies and has determined that certain applications, products and services pose an unacceptable security risk to Australian Government networks, data and information due to real and potential threats of foreign interference, espionage and sabotage. This is because they extensively collect user data which may be exposed to extrajudicial directions from a foreign government.
- Under the Protective Security Policy Framework (PSPF) the Department has issued three mandatory Directions on vendors of concern that extensively collect user data which may be exposed to extrajudicial directions from a foreign government, including:
 - Direction 001-2023 on the TikTok application – issued 4 April 2023.
 - Direction 001-2025 on DeepSeek Products, Applications and Web Services – issued 4 February 2025.
 - Direction 002-2025 on Kaspersky Lab, Inc. Products and Web Services – issued 21 February 2025.
- The Directions require non-corporate Commonwealth entities to:
 - Identify and remove existing instances of the products, applications and web services
 - Prevent the access, use or installation of the products, applications and web services on all Australian Government systems and mobile devices, and
 - Report completion of the Direction requirements to the Department of Home Affairs.
- The Australian Government continues to assess Australia's technology security policy settings to ensure they remain fit for purpose, including through the 2023-2030 Australian Cyber Security Strategy (the Strategy) and the finalisation of the Technology Vendor Review Framework.
- The Department of Home Affairs has also published the Foreign, Ownership, Control or Influence Risk Assessment Guidance to support public and private organisations assess technology vendor security risks in their supply chain and procurements.
- These measures are not targeted at any particular vendor or country, but rather, focus broadly on protecting the data integrity and security of Australian Government systems and devices.
- These initiatives also act as strong policy signals to critical infrastructure operators, other Australian governments including states and territories, and more broadly to Australian organisations and businesses.

Background

- TikTok collected significant quantities of user data that is stored in overseas data centres that reside outside of Australia's protected technology estate and this extensive collection of data may be exposed extrajudicial directions from a foreign government.
- DeepSeek's privacy policy outlines that it transmits and collects significant amounts of information from its users to train its AI model, with this information being stored in data centres owned and operated overseas.

- For Kaspersky Lab, Inc.'s applications and products to be effective as anti-virus software, they must be highly intrusive within a network so they can identify and defeat malicious software. This includes transmitting information back to a host jurisdiction and this extensive collection of data may be exposed extrajudicial directions from a foreign government.
- The emergence of technologies like DeepSeek highlights the rapid pace of AI development. Australian companies are also demonstrating incredible innovation, harnessing the huge potential of AI.
 - The National AI Capability Plan will build on this Australian innovation and know-how and make sure we have the foundations for growth and to support our economic resilience.
- The Australian Government is engaging internationally to ensure the global governance of AI strengthens safe and responsible practices internationally, reflecting our democratic values and respect for human rights. This includes our work as part of the global network of AI Safety Institutes, our support for safe and responsible AI adoption in the region, and our contributions to advancing the international understanding of the science of AI safety through the International Scientific Report on the Safety of Advanced AI.

Point of contact

Directions on DeepSeek, Kaspersky and TikTok	s. 22(1)(a)(ii) Director, Protective Security Policy, Commonwealth Security Policy, Cyber and Technology Security Policy Division, s. 22(1)(a)(ii) s. 22(1)(a)(ii), Director, Critical & Emerging Technology Security Policy, Technology Security Policy Branch, Cyber and Technology Security Policy Division, s. 22(1)(a)(ii)
--	---



OFFICIAL

Meeting Brief: Oracle Government Executives

First Assistant Secretary: Peter Anstee

cc Assistant Secretary: Britt Ryan and Tim Neal

Meeting Date:	19 March 2025	Meeting Time:	04:00pm – 04:45pm
Venue:	Meeting Room: M2R41 Level: 2 No: 3 Molonglo Drive Brindabella Park		

Key issues

- You are meeting with **s. 47F(1)** Government Affairs VP at Oracle.
 - Oracle is a global leader in cloud computing, database management and enterprise software. Oracle is a key investment partner in the US Artificial Intelligence (AI) infrastructure project, 'Stargate', along with OpenAI, Softbank, investment firm MGX.
 - Oracle has requested to discuss topics of mutual concern including; AI, Stargate/DeepSeek, TikTok and sovereign operating models.

- s. 47G(1)(b)**

- s. 47G(1)(b)**

Talking points (you may wish to raise):

Artificial Intelligence

- 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 Home Affairs considers that AI will almost certainly exacerbate existing national security risks, with potential for new and unknown risks. This includes increased foreign interference activities (including misinformation and disinformation),

OFFICIAL

OFFICIAL

vulnerabilities relating to data security and integrity, increased volume and efficacy of cyber operations, and easier access to and production of potential illegal or harmful materials.

- As the lead on national security policy for critical technologies, including AI, the Department of Home Affairs is working hard to ensure Australians have access to safe and responsible AI systems. This includes through;
 - the establishment of a team focused on the development and provision of AI national security policy advice to government;
 - supporting work by the Department of Industry, Science and Resources on the design of mandatory guardrails for AI in High-Risk Settings; and
 - considering the potential impacts of AI on Australian Government systems through the Protective Security Policy Framework, including platforms such as DeepSeek.

Stargate

- Stargate represents a \$500 billion investment aimed at transforming AI infrastructure in the United States. This investment includes the construction of data centres and large-scale computing facilities to support next generation AI capabilities. A key focus of Stargate is the development of chip manufacturing plants in Texas strengthening its semiconductor supply chain and maintaining a competitive edge in AI innovation.
- Initiatives like Stargate are driving large-scale AI advancements, reinforcing the need for updated security measures and a clear regulatory framework to support its expansion. As AI capabilities scale, ensuring responsible deployment and risk mitigation will be key to maintain trust and alignment with national priorities.

If asked about Australian Government investment in AI infrastructure

- On 16 December 2024, the Australian Government announced the development of a comprehensive National AI Capability Plan (the 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.
- The Plan will focus on four key areas for growing investment, strengthening AI capabilities, boosting AI skills and securing economic resilience.
- The Department of Industry, Science and Resources leads the Government's efforts on development of the Plan.

DeepSeek/TikTok

- The Department has determined that certain applications, products and services pose an unacceptable security risk to Australian Government networks, data and information due to real and potential threats of foreign interference, espionage and sabotage. This is because they extensively collect user data which may be exposed to extrajudicial directions from a foreign government.
 - The Department has issued three mandatory Directions under the Protective Security Policy Framework (PSPF) on vendors of concern, including TikTok, DeepSeek and Kaspersky:

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

OFFICIAL

- Direction 001-2023 on the TikTok application – issued 4 April 2023.
- Direction 001-2025 on DeepSeek Products, Applications and Web Services – issued 4 February 2025.
 - DeepSeek’s privacy policy outlines that it transmits and collects significant amounts of information from its users to train its AI model, with this information being stored in data centres owned and operated overseas.
- Direction 002-2025 on Kaspersky Lab, Inc. Products and Web Services – issued 21 February 2025.
- The Directions require non-corporate Commonwealth entities to:
 - Identify and remove all existing instances of the products, applications and web services
 - Prevent the access, use or installation of the products, applications and web services on all Australian Government systems and mobile devices, and
 - Report completion of the Direction requirements to the Department of Home Affairs.
- The Department acknowledges that Australia is a net technology importer, and that Australia’s economy relies heavily on the availability of overseas technology products and services to improve and expand productivity and business functionality for Australian Government entities, organisations and businesses.
- Many third-party vendors that are foreign owned, controlled or influenced (FOCI) do not present a threat to Australia’s interests, however, there is a potential for control or influence by foreign governments with interests which conflict with Australia’s.
- The PSPF Directions are part of a wider set of initiatives established by the Australian Government on third party and vendor risk management, including:
 - **Three PSPF Directions** on technology applications, products and web services supplied by vendors of concern.
 - **PSPF Release 2024**, which built upon existing requirements on managing third-party risks by including new requirements on managing FOCI risks in procurement, security risks associated with engaging with foreign partners, and implementing an insider threat program.
 - The **Technology Vendor Review Framework**, which provides guidance on technology vendor risks to inform public and private sector procurement decisions about the security of technology products and services.
 - The **Hosting Certification Framework**, which assists agencies in mitigating against supply chain and data centre ownership risks to enable them to identify and source appropriate hosting and related services.
- These measures are not targeted at any particular vendor or country, but rather, focus broadly on setting security policy within Government to address emerging risks.

- These initiatives also **act as strong policy signals** to critical infrastructure operators, other Australian governments including states and territories, and more broadly to Australian organisations and businesses.

Sovereign Operating Models

If asked: Is Australia developing a Sovereign AI Frontier Model?

- 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.

Background

- The three mandatory PSPF Directions refer to ‘devices’ which are defined in the PSPF section 9.3 - Minimum Protections and Handling Requirements and includes all mobile phones, handheld computers, tablets, laptops and personal digital assistants. This includes:
 - Government-issued mobile device – owned and issued by an Australian Government entity to access the entity’s systems and data and is approved by the relevant authority to process, store or communicate entity information of a specified protective marking or security classification.
 - Authorised non-government device – owned or issued by a non-government source that is managed, configured and encrypted in accordance with ASD standards and guidance, and the residual risk is accepted by the Commonwealth entity system risk owner to access, process, store or communicate OFFICIAL, OFFICIAL: Sensitive and PROTECTED Australian Government information.
- The **Technology Vendor Review Framework** (TVRF) was announced by the Minister for Home Affairs on 20 December 2024. The TVRF is a key measure under the 2023-2030 Australian Cyber Security Strategy.
-

Contact Officer:	s. 22(1)(a)(ii)
Author/Position:	s. 22(1)(a)(ii) A/g Senior Policy Officer, Protective Security Policy Commonwealth Security Policy Branch Cyber and Technology Security Policy Division s. 22(1)(a)(ii) Policy Officer, Critical & Emerging Securities Policy Technology Security Policy Branch Cyber and Technology Security Policy Division

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

OFFICIAL

Date: 14 March 2025

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

OFFICIAL