



Australian Government

Department of Home Affairs
Protective Security Policy Framework

OFFICIAL

PSPF Direction 001-2024

Managing Foreign Ownership, Control or Influence Risks in Technology Assets

PSPF Direction 001-2024 requires Australian Government entities to identify indicators of Foreign Ownership, Control or Influence risk as they relate to procurement and maintenance of technology assets and appropriately manage and report those risks.

Foreign interference occurs when activity carried out by, or on behalf of, a foreign power, is coercive, corrupting, deceptive or clandestine, and contrary to Australia's sovereignty, values and national interests¹. Foreign Ownership, Control or Influence (FOCI) is an application of foreign interference.

Further information about FOCI as it relates to procurement is detailed in Policy Explanatory Note 01/24 – Managing Foreign Ownership, Control or Influence Risk in technology assets.

On advice from the Protective Security Board, there is a pressing need for Australian Government entities to appropriately manage the risks of foreign ownership, control and influence in technology assets to protect the Australian Government from unlawful activities.

By PSPF Reporting Period 2024-25 (June 2025) all entities **must**:

1. In accordance with Department of Home Affairs guidance, implement a process when undertaking procurement of technology assets² to identify and manage potential FOCI risks, calibrated to the entity's risk environment.
2. Conduct a risk assessment of potential FOCI risks identified during the procurement of technology assets process, using the security risk assessment process detailed in PSPF Policy 3: Security Planning and Risk Management.
3. Regularly monitor the entity's contracts relating to technology assets to ensure that FOCI risks do not materialise, in accordance with PSPF Policy 6: Security Governance for Contracted Goods and Service Providers, Requirement 3.

¹ [Countering the Insider Threat: A guide for Australian Government | Attorney-General's Department](#)

² For the purposes of this Direction, a technology asset is defined as *any hardware, software or information system, platform, mobile application or as-a-service offering, which stores, processes, transmits or transforms official or security classified information belonging to, or utilised by, the Australian Government.*

OFFICIAL

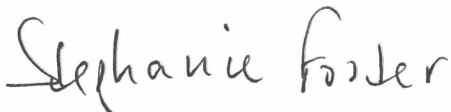
OFFICIAL

4. Report any potential or identified FOCI risks identified during procurement processes for technology assets to the Department of Home Affairs' Government Cyber and Protective Security Branch at PSPF@homeaffairs.gov.au or call 02 5127 9999 for advice on reporting above PROTECTED.

Entities **must** continue to report acts of foreign interference to the Australian Security Intelligence Organisation in accordance with PSPF Policy 5: Reporting on Security, Requirement 2.

Entities **must** continue to comply with the Commonwealth Procurement Rules (CPRs) and report non-compliance with the rules to the Department of Finance. For further information on the CPRs, contact procurementagencyadvice@finance.gov.au.

For further information, contact PSPF@homeaffairs.gov.au or 02 5127 9999.



Stephanie Foster PSM

Secretary

Department of Home Affairs

5 July 2024