Australian Government
Department of Home Affairs

TechFIT
TECHNOLOGY FOREIGN INTERFERENCE TASKFORCE

Australian Government Due Diligence Resource Summary

This document provides a summary of existing Australian Government due diligence guidance on foreign interference and espionage-related matters, and guidance from other sectors with relevant insights applicable to Australia's technology sector. This list is at the **OFFICIAL** level and hence, non-exhaustive. Access to ASIO's **OFFICIAL: Sensitive** reporting is available by signing up to the Outreach portal.

Know Your Partner

Organisation	Resource	Purpose/Key Insights
Australian Securities and Investment Commission	ASIC Registers	• Tool for confirming a supplier's identity and ownership.
Australian Security Intelligence Organisation	ASIO Due Diligence Integrity Tool (ADDIT – available on request by emailing Outreach at outreach@asio.gov.au)	• Guidance for Australian institutions considering engaging with foreign entities. • Provides a framework to consider the security risks associated with foreign collaboration.
Australian Security Intelligence Organisation	ASIO's Security Treatment Advice for managing Procurement (STAMP – available on request by emailing Outreach at outreach@asio.gov.au)	• Due diligence framework focused on security risks and concerns associated with Defence procurement from private vendors. • Specifically aimed at Defence-related technology research and development sectors.
Australian Security Intelligence Organisation	Secure Your Success	• To raise awareness in the technology and research sectors on how foreign powers and proxies use cyber, human and technical means to steal intellectual property, harvest expertise and co-opt academic research. To advise on how these risks can be mitigated, research protected, and protocols for reporting suspicious incidents or behaviour.

Organisation	Resource	Purpose/Key Insights
Australian Tax Office	Australian Business Register	• Tool for confirming a supplier's identity and ownership.
Australian Transaction Reports and Analysis Centre	Politically exposes persons	• To identify customers that might be politically exposes persons (PEPs) and steps to deal with them. • Outlines PEP risks and indicators of suspicious behaviour associated with illicit activity.
Australian Transaction Reports and Analysis Centre	Beneficial owners	• To identify customers' beneficial owners and assessing the associated money laundering/terrorism financing risk. • Outlines the ways to determine beneficial owners when doing business with a non-individual customer (e.g. companies, trusts and associations).
Department of Home Affairs	Foreign Ownership, Control or Influence (FOCI) Risk Assessment Guidance	• Helps medium-to-large and mature small-sized organisations procuring technology products or services to assess a vendor's exposure to FOCI and correlating security risks. • Provides a repeatable methodology to identify, assess, recommend and implement mitigations commensurate to the risk posed by vendors operating in their supply chains.
Department of Foreign Affairs and Trade	Guidance – Considerations for Negotiating and Entering Foreign Arrangements	• Outlines general principles that should be considered when negotiating or entering foreign arrangements.

Sanctions Lists

Organisation	Resource	Purpose/Key Insights
Australian Sanctions Office, Department of Foreign Affairs and Trade	Consolidated List | Guidance Note – Dealing with assets owned or controlled by designated persons and entities	• Provides a list of all persons and entities listed under Australian sanctions laws. • Outlines obligations to freeze assets owned or controlled by designated persons or entities and the mandatory reporting to the Australian Sanctions Office and the Australian Federal Police.

Organisation	Resource	Purpose/Key Insights
Australian Sanctions Office, Department of Foreign Affairs and Trade	Guidance Note – Artificial intelligence and quantum technology sector	• Highlights the potential sanctions risks in the transfer of assets (including intangible assets) and the provision of a sanctioned service for the AI and quantum technology sectors.
Australian Sanctions Office, Department of Foreign Affairs and Trade	Guidance Note – Cyber sanctions | FAQs Cyber Sanctions and Ransomware Payments	• Outlines Australia's cyber sanctions framework, compliance obligations under autonomous sanctions law (including the need to undertake due diligence), and the risks associated with making or facilitating a ransomware payment to persons or entities subject to sanctions.
Australian Sanctions Office, Department of Foreign Affairs and Trade	Guidance Note – Fintech and the DeFi sector	• Provides a summary of sanctions laws relevant to Fintech (financial technology) and the DeFi (decentralised finance) sector.
Australian Sanctions Office, Department of Foreign Affairs and Trade	Sanctions Compliance Toolkit	• Provides guidance in navigating the complexities of Australian sanctions laws. Outlines key principles, risk management strategies and best practices for compliance at the organisational and activity-based levels.
Australian Sanctions Office, Department of Foreign Affairs and Trade	Sanctions Risk Assessment Tool	• Helps assess any given activity against Australian sanctions prohibitions by following a structured approach to determine if the activity has a connection to any sanctioned person, entity, or country.
Department of Defence	Export Controls Framework	• Regulates the responsible movement of Defence-related goods, technology and services both within and outside Australia. • For government, industry, higher education and research, and private individuals to meet their obligations under Australia's export control laws.
Department of Defence	Defence and Strategic Goods List (DSGL)	• Specifies goods, technology and software regulated under Australian export control laws. For any person or entity wishing to export, supply, publish or broker 'controlled' DSGL items. This includes the Dual-use List which contains commercial items with potential military and weapons of mass destruction application.

Recruitment / Personnel

Organisation	Resource	Purpose/Key Insights
Attorney-General's Department	Countering the Insider Threat: A guide for Australian Government	• Supports government entities to establish and maintain an organisational culture resistant to insider threats. • Provides transferrable guidance for industry on the associated risks and factors, and offers practical measures to assist mitigation.
Australian Security Intelligence Organisation	Countering the insider threat	• Advises government and industry security managers on how to protect workplaces from insider threats.
Department of Foreign Affairs and Trade	Guidance Note – Employment with designated people or entities	• Outlines how Australian sanctions laws apply to Australian citizens and foreign residents living in Australia considering employment with designated persons or entities.

Security Maturity and Protective Security

Organisation	Resource	Purpose/Key Insights
Australian Security Intelligence Organisation	Protective Security Top Ten	• Outlines the essential components of a complete security framework to protect people, places, technology and information.
Australian Security Intelligence Organisation	Secure innovation	• Outlines five key principles to support the technology sector's innovation and collaboration in a way that keeps organisations safe and secure.
Australian Signals Directorate	Cyber Security Partnership Program	• Enables Australian organisations and individuals to engage with the Australian Signals Directorate's Australian Cyber Security Centre and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy.
Australian Signals Directorate	Essential Eight Maturity Model	• Advises on how to protect internet-connected information technology networks used by small and medium businesses, large organisations and infrastructure, and government.

Organisation	Resource	Purpose/Key Insights
Department of Home Affairs	Protective Security Policy Framework	• Prescribes the actions government entities must take to protect their people, information and resources from security risks. • Guidance is transferrable to uplift security culture, policies and procedures in a non-government context.

University/Research Sector-Specific

Organisation	Resource	Purpose/Key Insights
Attorney-General's Department	Foreign Influence Transparency Scheme Factsheet – Information for university students and student associations	• Assists university students and student associations to determine whether they are required to register under the Foreign Influence Transparency Scheme.
Australian Research Council (ARC)	Countering Foreign Interference Framework	• Articulates the ARC's processes to help protect the research it funds from misuse, including the roles and responsibilities of the ARC, universities, researchers and other government agencies in relation to ARC grants and grant processes. • Outlines counter foreign interference considerations informing funding assessment.
Australian Sanctions Office, Department of Foreign Affairs and Trade	Guidance Note – Sanctions compliance for universities	• Outlines key sanctions risks across the various activities conducted by Australian universities and offers guidance on how to comply with Australian sanctions laws.
Australian Security Intelligence Organisation	Protect your research	• Raises awareness on how foreign powers and proxies target Australian academic and research institutions, and advises on ways to protect individuals and institutions, and manage visitors and delegations from overseas.
Commonwealth Scientific and Industrial Research Organisation (CSIRO)	The Research Engagement Sensitivities Tool (REST) (Available on request by emailing CSIRO at CSIROsecurity@csiro.au)	• A decision-support tool developed by CSIRO as its key foreign interference risk-assessment process. It helps identify and mitigate risks to activities, including research security, in a consistent and proportionate way across the different circumstances of each research unit.

Organisation	Resource	Purpose/Key Insights
Department of Education / Department of Home Affairs	Case Studies – • Cybersecurity • Due diligence, risk assessments and management • Governance and risk frameworks Transnational Education	• Assists universities to understand how they might consider the *Guidelines to Counter Foreign Interference in the Australian University Sector* in the transnational education environment, in their due diligence and risk assessment processes, in their cybersecurity practices, and in their governance and risk frameworks.
Department of Education / Department of Home Affairs	Countering Foreign Interference in the Australian University Sector	• Central hub for university foreign interference support. • Relevant resources include: o Due Diligence Assistance Framework o Report and resolve foreign interference (responsibility matrix) o Factsheet – Open source information o Transnational Education Guidance Note on Due Diligence
Department of Education / Department of Home Affairs	Guidance Notes – • Communication, education and knowledge sharing • Cybersecurity • Due diligence, risk assessments and management • Governance and risk frameworks	• Assists universities to develop and implement communication, education, and knowledge sharing; cyber security; due diligence, risk assessments and management processes; and governance and risk frameworks practices in accordance with the *Guidelines to Counter Foreign Interference in the Australian University Sector.*
Department of Education / Department of Home Affairs	• Guidelines to Counter Foreign Interference in the Australian University Sector	• Assists the university sector to manage and engage with risk to deepen resilience against foreign interference in the university sector.

Organisation	Resource	Purpose/Key Insights
Department of Education / Department of Home Affairs	Self-Evaluations – • Communication, education and knowledge sharing • Due diligence, risk assessments and management • Governance and risk frameworks	• Assists universities in evaluating their implementation of communication, education and knowledge sharing; due diligence, risk assessments, and management; and governance and risk frameworks in accordance with the *Guidelines to Counter Foreign Interference in the Australian University Sector.*
Tertiary Education Quality and Standards Agency	Transnational education toolkit	• Provides guidance to the sector on offshore delivery of Australian higher education awards, including third party delivery involved in Australian transnational education.

Useful context

Organisation	Resource	Purpose/Key Insights
Attorney-General's Department	Foreign Influence Transparency Scheme Resources	• Assists individuals and entities to determine whether they are required to register under the Foreign Influence Transparency Scheme. • Provides information on how the scheme works, including key considerations such as what a registrable activity is, who a foreign principal may be, and the exemptions available.
Australian Institute of Criminology / Australian Security Intelligence Organisation	The Cost of Espionage	• Estimates the actual and prevented costs of espionage (including the mitigation, response, and direct costs).
Commonwealth Fraud Prevention Centre, Attorney-General's Department	Commonwealth Fraud and Corruption Control Framework 2024	• Supports government entities to effectively manage the risks of fraud and corruption. • The Framework guidance is transferrable to uplift fraud and corruption control in a non-government context.

Organisation	Resource	Purpose/Key Insights
Commonwealth Fraud Prevention Centre, Attorney-General's Department	Commonwealth Fraud Prevention Centre	• Publishes leading practice guidance and tools to strengthen counter-fraud and anti-corruption capability, including risk assessment, effective controls, designing fraud resistant policies, and preventing fraud in procurement administration.
Department of Home Affairs	Countering Foreign Interference in Australia	• Identifies the sectors most at risk and outlines the robust measures the Government has implemented to combat these threats. • Offers practical advice for individuals and organisations to protect themselves. • Provides a list of additional resources for government and industry.
Treasury	Guidance Note 8: National security	• Provides information for investors on the operation of the Foreign Investment Framework with regards to national security, including information on the types of actions that may pose national security risks. • The *Critical Technologies* section outlines mandatory and voluntary notification obligations for foreign persons seeking to invest in the listed critical technologies (including AI, quantum and genetic engineering).