Australian Government
Department of Home Affairs

TechFIT
TECHNOLOGY FOREIGN INTERFERENCE TASKFORCE

Factsheet for Critical Technology Sectors

Foreign interference and espionage risks

Foreign actors are seeking to exploit Australia's open systems and dual-use innovations for military, political, and economic gain. This introduces complex and evolving risks which may undermine Australia's sovereignty, prosperity, and national security. Recognising the potential impacts of these risks to our critical technology sectors is pivotal to ensuring appropriate action is taken to strengthen resilience against state and state-sponsored threats.

This factsheet provides an overview of foreign interference and espionage risks for Australia's critical technology sector and includes considerations for risk mitigation.

Overview

Foreign interference and espionage are being used to gather valuable information and expertise on technology for strategic advantage. These activities are typically focused upon military or military-adjacent technologies. However, the current threat applies to both military and dual use technologies. The risk is also heightened for critical technologies, which may act as a force multiplier for further technological development and associated commercial or strategic benefits.

Protecting the research and technology sectors against these risks is critical to the security of Australia's current and future critical technologies, including artificial intelligence, biotechnology, and quantum.

Artificial Intelligence

Biotechnology

Quantum

Vectors

Malicious actors may use the following vectors to introduce foreign interference and espionage risks:

1. **Physical:** Leveraging or gaining access and using it to steal information.
2. **People and networks**: Using personal relationships and interactions to transfer sensitive information or intellectual property.
3. **Investment and supply chain:** Investing in a company or its supply chain – thereby exposing it to foreign ownership, control, or influence risks – to gain partial or full control and exploiting this access to steal information.
4. **Collaboration:** Establishing research partnerships, academic relationships, and engagement programs and exploiting them to transfer critical information and technology.
5. **Cyber:** Gaining access to sensitive systems and networks to steal data, sensitive information and IP.

CONTACT US | TechFIT@homeaffairs.gov.au

Impacts

These risks can have a range of potential impacts:

- **Loss of key information:** Provides adversaries with insights into domestic commercial, military, and scientific operations. This information is used to inform additional malicious activity to weaken our strategic position.
- **Loss of competitive market position:** Theft of sensitive data and intellectual property is used to enhance the research and development activities of competitors.
- **Diminished autonomy:** Malicious actors may obtain partial or complete administrative ownership or control over, or build influence within a critical technology company, or its related components or patents.
- **Weakened public perception:** Loss of public perception of and trust in institutions, resulting in reputational damage for organisations.
- **Damaged international standing:** Erodes Australian companies' standing as prospective partners, both for research and commercial opportunities.

Mitigations

To manage these risks, organisations should consider their security posture and implement comprehensive risk management processes.

As threats and risks change, so should your security practices – it is important to regularly assess, review, and update security controls to account for any changes. Some general risk mitigations to consider are outlined below.

Raise awareness across your organisation and its people so threats can be identified and risks managed.

Implement strong **physical security controls**, including limiting access to visitors, delegations and investors.

Establish **due diligence processes** for employees, business partners, investors, and research collaborators that includes continuous risk management.

Establish a **third-party risk management** program, including for software vendors, to address vulnerabilities and foreign ownership, control and influence (FOCI) risks.

Implement **robust cyber security controls**, considering government and industry frameworks such as the Information Security Manual and National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Takeaways

1. Foreign interference and espionage targeting Australia's critical technology sectors has escalated and will persist for the foreseeable future.
2. There are a range of malicious actors using different vectors to target our world leading IP and expertise. This exposes us to additional risks to manage.
3. The impacts of these risks can be deep and long-lasting – ultimately, they can harm Australia's national security and economic development, and the viability of our enterprises.
4. There are a range of mitigations that critical technology companies should use to manage foreign interference and espionage risks. This includes using continuous due diligence processes to inform risk management actions.

CONTACT US | TechFIT@homeaffairs.gov.au

Australian Government
Department of Home Affairs

TechFIT
TECHNOLOGY FOREIGN INTERFERENCE TASKFORCE

Where can I find out more?

The Technology Foreign Interference Taskforce (TechFIT) was established within the Department of Home Affairs to work with Australia's technology industry to build awareness of and resilience against foreign interference and espionage threats. TechFIT works with a subset of industry stakeholders towards safeguarding the Australian technology industry, and our intellectual property and innovations. More information can be found on the Department's TechFIT page.

The Australian Security Intelligence Organisation (ASIO) publishes guidance on protective security, including on insider threats, research collaborations and partnerships.

Additional resources

1. FOCI Risk Assessment Guidance
   - A repeatable methodology to identify, assess, recommend and implement mitigations commensurate to the risk posed by vendors operating in their supply chains.
2. ASIO Due Diligence Integrity Tool (available 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.
3. ASIO Secure Your Success
   - Guidance to prevent foreign powers gaining advantage from Australian innovation by stealing intellectual property, harvesting expertise and co-opting academic research.

Additionally, the Australian Government Due Diligence Resource Summary provides a broad summary of existing government due diligence guidance on foreign interference and espionage-related matters. This includes guidance from other sectors that may have insights for Australia's technology sector.

OFFICIAL
CONTACT US | TechFIT@homeaffairs.gov.au