Australian Government
Department of Home Affairs

Foreign Ownership, Control or Influence

Risk Assessment Guidance

Table of Contents

Overview **2**

Introduction 3
What is FOCI risk? 3
What makes Australia a target? 3
FOCI Risks for businesses 4
Understanding the threat 4
What is considered a secure and verifiable vendor? 6

Assessing the vendor **7**

Step 1 – Vendor review questionnaire 7
Flowchart 10
Step 2 – FOCI risk assessment 11
Identify and understand the threat 12
Jurisdictional hazard 12
Identify international precedent 13
Establish exposure 13
Rate the threat 14
Consider risks 15
Treatments 18

Evolving environment **19**

Periodic review 19

Glossary **20**

Foreign Ownership, Control or Influence

Overview

This document is a guide for medium-to-large Australian organisations that are procuring technology products or services. Foreign technology vendors offer significant value, capabilities and opportunities for Australian organisations and businesses. However, in some cases, the application, market prevalence or nature of certain technologies, coupled with foreign influence, could present risks to Australian organisations and the broader national interest. This document provides a template to support organisations to assess a vendor's exposure to foreign ownership, control or influence (FOCI) and correlating security risks. Managing FOCI risk extends beyond national security; it encompasses protecting your organisation's reputation, your organisation's systems and intellectual property, your business interests, and the privacy of your staff and customers. This template should form part of an organisation's broader procurement and due diligence processes.

The guidance within this document provides a repeatable methodology for organisations to identify, assess, recommend and implement mitigations commensurate to the risk posed by foreign technology vendors operating in their supply chains. While it asks specific questions, it does not provide an exhaustive list of security concerns associated with FOCI, nor is it a single source for supply chain risk mitigation information that will protect companies and organisations from all possible types of foreign interference, sabotage, and espionage.

Application of the processes within this guidance should always be supplemented with organisational risk management arrangements and the broader supply chain risk considerations, which are detailed at cyber.gov.au.

The assessment component of this guidance is comprised of two stages:

1. Vendor review questionnaire – to determine whether a FOCI risk assessment is required in relation to a foreign vendor.
2. FOCI risk assessment – using the research undertaken to answer the questionnaire, the full assessment will consider jurisdiction hazard against organisational exposure, FOCI activity risks, and possible treatment options.

A list of relevant resources is also provided to inform your risk assessments (see guidance section *Assessing the Vendor - Step 1 – Vendor review questionnaire* and **Appendix A**). A glossary at the end of the document provides descriptions on key terms mentioned across the guidance.

Importantly, the information gathered as part of conducting the risk assessment is point-in-time and should be reviewed throughout the procurement lifecycle. The review can be periodic and/or based upon trigger events or changing circumstances.

Introduction

There is an inherent risk every time an organisation interacts with a supplier, manufacturer, distributor, or retailer. Possible risks include vendor relationships that are impacted by FOCI. An organisation's supply chain relationships can affect the security of its systems, and its own products or services. If products or services access valuable systems, operate with privileged access, or have control over a large portion of a cyber-supply chain, they may expose a weakness that could be exploited by malicious actors. This could have wide-reaching and harmful consequences, including disruption to the confidentiality, integrity and availability of information systems and services.

If the vendor in question is subject to, or at risk of FOCI, organisations are encouraged to conduct a FOCI risk assessment.

What is FOCI risk?

FOCI risk refers to the ability for vendors to be directed by a foreign government, either through direct ownership channels, the domestic laws of a foreign jurisdiction or outside influence (such as political party membership) to conduct malicious activities on behalf of that government.

It can be present when a vendor is exposed to a foreign state through either ownership, control, or influence.

Foreign ownership: The degree to which foreign countries possess ownership stakes in a company, its subsidiaries, and its affiliates. It could mean that a portion of the company's shares is held under foreign investment by a foreign person, foreign resident, or that a foreign company has significant equity interest. Foreign investments can also come through venture capital.

Foreign control: The authority and influence exerted by foreign entities and governments over a company's decision-making processes. This can involve legislation allowing the use and access of data and communications generated and stored by industry in a foreign country, the appointment of key personnel, board members, or other measures that grant foreign interests a say in how the company operates.

Foreign (malign) influence: Can be applied on vendors through various coercive means, including economic leverage, strategic partnerships, or even subtle political manoeuvring. When foreign actors or governments seek to exert influence in a way that is actively hidden or not transparent, this can have serious implications for organisations and Australia.

Vendors subject to FOCI can be directed to act against their own business interests. They could be compelled by a foreign government to conduct malicious acts such as undermining the security of their products and services or providing privileged access to systems and client data. Such influence, if not properly managed, can lead to unauthorised access to sensitive information or negatively impact performance and contracts. Managing FOCI risk extends beyond national security; it encompasses protecting your organisation's reputation, your organisation's systems and intellectual property, your business interests, and the privacy of your staff and customers.

What makes Australia a target?

Australia is an attractive target for several reasons, including its position as a major commodity supplier, scientific and technological innovator, and its military modernisation program. Australia may also be targeted due to its strategic alliances. Strong economic and trade partnerships on their own may not deter a foreign government from compelling a vendor to act against Australia's interests.

Publicly available reports of bulk data collection activities, exploitation of cyber vulnerabilities and pre-positioning in critical infrastructure networks by foreign governments and state backed actors demonstrate there is a clear intent by certain countries to gather intelligence and prepare for future disruptive activities. The same governments also have a strong control over the private sector, and can compel companies and

individuals, through legal means or otherwise, to support their objectives. See **Appendix A – Resources** for further information.

It **should be** expected that some foreign technology vendors are being used to support espionage activities. It **should be** anticipated that a foreign technology vendor could be leveraged to exploit its commercial products and services to conduct sabotage activities, especially **during a time of heightened tension**.

FOCI Risks for businesses

Cyber security standards and controls may not provide full assurance against the risks posed by compromised foreign vendors. Decision-makers must look more closely at the political context of the source country of their suppliers. The distinction between business impact and the broader effect upon national security is narrowing. For example:

- unauthorised access to, or control of, surveillance technology, such as CCTV, can help threat actors identify targets for covert operations or compromise across government and industry;
- unauthorised bulk data exfiltration and aggregation can provide insights on customers, business structures, finances, strategies, and exposure to risk that could be exploited or used for influence or interference;
- theft of intellectual property harms Australian innovation, investment, and market confidence;
- sabotage can have significant impacts across all sectors of the economy and government security; and
- other activities may conflict, or interfere with, the contracted or procured service.

Modern businesses and organisations do not operate in isolation. The cumulative impact of compromised vendors across the economy has significant and cascading effects on national security, business confidence, and the economy. Preventative security measures – such as supply chain and market diversification, mitigating vendor specific risks, and information sharing with government – are the best way to secure Australian networks from FOCI risks.

Ignoring or not appropriately addressing FOCI risks can lead to legal and regulatory repercussions (including action relating to non-compliance), significant reputational damage, and even jeopardise national security interests. Recent initiatives by other countries have also added new dimensions to the FOCI landscape, since the suppliers or technologies you use may limit your ability to conduct business with foreign companies. For example, the recent action by the United States (US) Government on Kaspersky products and services is wide ranging, and applies to US registered businesses in Australia. Understanding these consequences is crucial for informed decision-making and effective risk management.

Understanding the threat

The risk of a vendor being exploited is dependent on the foreign jurisdiction under which it is owned, controlled, or influenced. For example, foreign vendors are typically subject to the laws of the country in which they or their parent company are based. These laws can include provisions to compel companies to provide information, systems access, or act on the foreign government's behalf.

Some key resources to assist organisations in considering jurisdiction risk when undertaking an assessment are available at **Appendix A**.

Five Eyes
Australia, Canada, New Zealand, the United Kingdom, and the United States have a long history of diplomatic cooperation, coordination, and information sharing on security and intelligence matters. This relationship is built on a mutual level of trust and respect. Across the five countries, we also share similar geopolitical challenges and threats, and face similar risks.

Foreign governments whose interests and values do not align with ours (or those of Five Eyes and other likeminded partners) are intent on collecting vast amounts of data, intellectual property, research and information about Australia's critical assets and people. These same foreign governments are more likely to exploit companies to achieve their strategic goals. This includes the malign and extrajudicial use of companies to support espionage and sabotage activities. It is likely that, during a period of heightened geopolitical tension, foreign governments could compel vendors to support espionage and sabotage operations in Australia via their products and services.

Foreign laws — legalising collection

Certain countries have laws in place that provide a legal basis for their government to exercise authority both inside and outside their borders. This enables these governments and their security services to leverage the resources and capabilities of any organisation or individual if the purpose is deemed relevant to the country's interest. Such measures can be, but are not limited to:

- the capacity to use and access data and communications generated and stored by industry in their country;

- the authority to collect, analyse and store all data that is transmitted or received on the country's networks; or

- inspection of computer systems, localisation of data, and control over online content.

For example, under China's National Intelligence Law, Chinese security and intelligence services can acquire the resources and capabilities of any organisation or individual if the purpose is deemed relevant to China's national security. The law applies to organisations and individuals based in China and Chinese citizens, and can be extended to organisations with Chinese ties incorporated in foreign jurisdictions, such as subsidiaries. The Multi-Layer Protection Scheme, brought into effect on 1 January 2020, further strengthened China's capacity to use and access data and communications generated and stored in China.

Russia's System for Operational Investigative Activities Law gives Russia's security service the authority to collect, analyse and store all data that is transmitted or received on Russian networks.

What is considered a secure and verifiable vendor?

In the context of FOCI risks, a secure and verifiable vendor is one that is a private or public company independent from foreign government and unsusceptible to government direction, coercion or pressure to engage in malign activities in Australia. A secure and verifiable vendor (and its parent company, if applicable) is more likely to be headquartered in a democratic country with a strong rule of law, effective judiciary, transparent government processes, and freedom of the press.

It should also be noted that many democratic countries, including Australia, have legal provisions to compel entities to assist government with certain matters (e.g. law enforcement activities). There are seven broad criteria, building on the OECD principles for government access to personal data held by private sector entities, for determining if a government direction to a vendor is lawful and non-malicious. The below principles reflect the shared values of OECD member countries and draw on commonalities in their existing laws and practices:

1. Legal basis – the direction is regulated by a legal framework, which is binding on the government. The legal framework should set out the purpose, conditions, limitations and safeguards, which apply to government directions.
2. Legitimate aims – the direction should conform to the rule of law. Access should be necessary, proportionate and reasonable to achieve explicit aims. These aims should not be in contravention with, or otherwise circumvent, reasonable laws within another jurisdiction.
3. Approvals processes – the direction should be subject to an independent approvals process. These approvals should be documented and apply rules, standards and processes which are appropriate to the degree of interference with privacy and/or human rights.
4. Information handling – the direction should be subject to physical, technical and administrative measures to ensure that any personal and sensitive information is protected and that only authorised personnel are able to access the information.
5. Transparency – the framework or justification governing the directive should be clear and accessible to the public.
6. Oversight – there should be mechanisms for effective and impartial oversight and contestability of any such direction. Oversight bodies must have the power to investigate and redress government entities for non-compliance and must have adequate resources to carry out their functions.
7. Redress – governments should ensure there are effective judicial and non-judicial avenues for identifying and remedying contraventions of the framework.

Assessing the vendor

Step 1 – Vendor review questionnaire

The following vendor review questionnaire is the first step in understanding exposure to FOCI risks in the procurement of new, or review of, existing technology products or services. At the end of the vendor review questionnaire, organisations will know whether it is necessary to also consider FOCI risks in their assessment processes. A corresponding flowchart is included on page 10.

Note: *This questionnaire should take approximately 60-90 minutes to complete utilising open source research.*

Appendix A *provides a non-exhaustive list of public resources to assist organisations in addressing the questions to understand the exposure to FOCI risks.*

Consideration should be given to the confidence level of each of your responses to the questionnaire and whether further due diligence would be required if the vendor is found to present a high, or very high, risk.

A simple to follow and printable template of the vendor review questionnaire and an example are available at ***Appendix B****.*

Additionally, organisations are encouraged to develop a proactive approach to assess supply chain security. This includes embedding assessment and security controls throughout the relationship (from decision to outsource, supplier selection, contract award, supplier delivery to termination) and setting and communicating minimum-security requirements for suppliers, and the consequences for non-compliance. A range of other resources used by industry can support the implementation of such measures. Below is a non-exhaustive list of standards and guidance material available to the public, including:

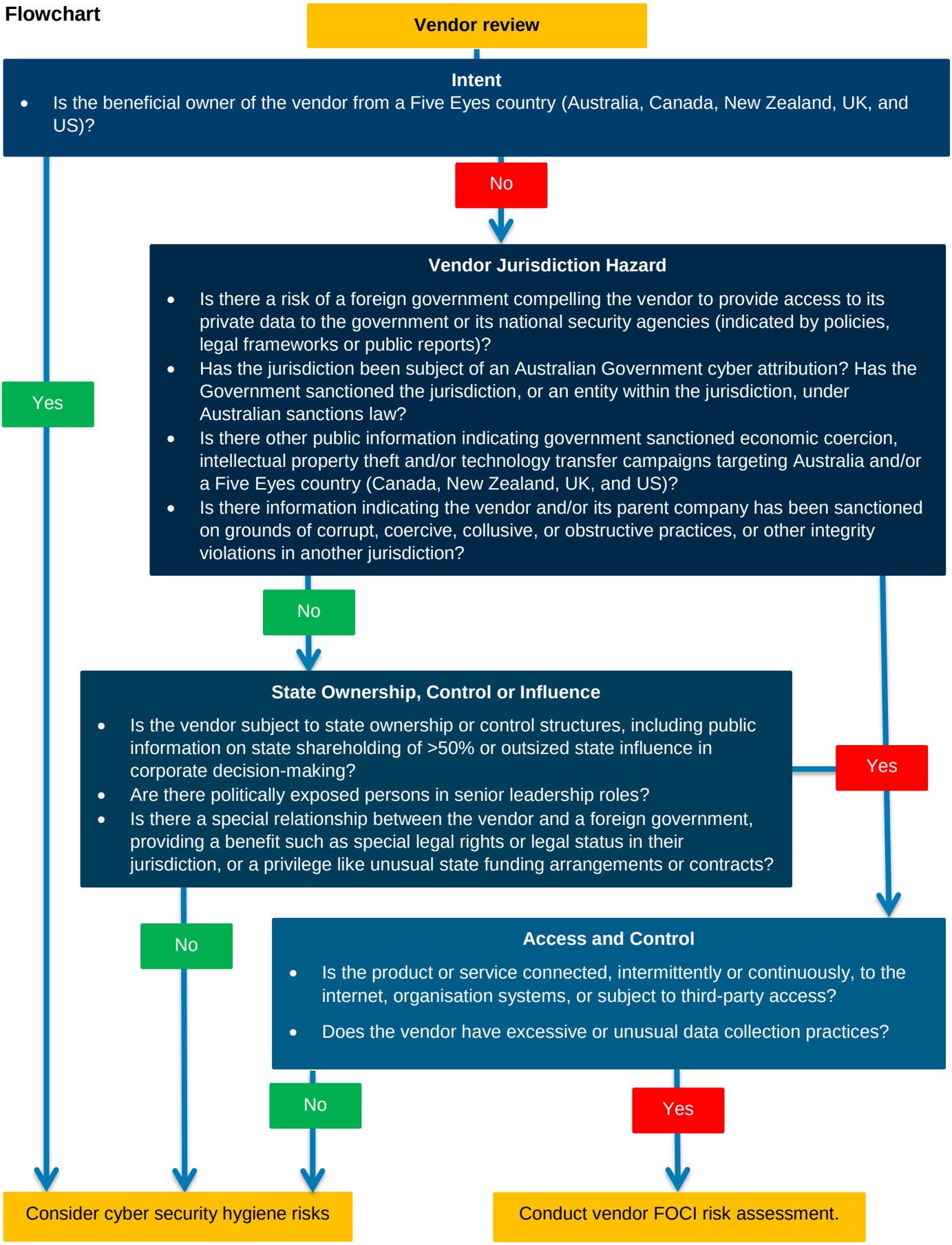
- Australian Signals Directorate's (ASD) *Identifying Cyber Supply Chain Risk guidance*;
- ASD's *Australian Cyber Security Centre's Information Security Manual*;
- ASD's *Essential Eight and Strategies to Mitigate Cyber Security Incidents;*
- ASD's *Information Security Manual (ISM)*. The ISM contains Guidelines for Procurement and Outsourcing applicable for Australian organisations;
- ASD's *Choosing Secure and Verifiable Technologies;*
- the Department of Home Affairs' *Critical Technology Supply Chain Principles*;
- ISO/IEC 27000 series of international standard to manage information security;
- ISO 28001 series of international standards to manage supply chains;
- ISO 31000 series of international standards to manage risk;
- NIST SP 800-53 standard helps to implement security and privacy controls; and
- NIST SP 1800 series is a set of publications that offer information on how to implement and apply standards-based cybersecurity technologies in real-world application.

Section 1 – Intent	
Question	**Example resources and information to assist** (more resources available at **Appendix A**)
Is the beneficial owner of the vendor from a Five Eyes country (Australia, Canada, New Zealand, UK, and United States)?	• Information can be available on securities websites (such as the Australian Securities Exchange), annual reports and business news reporting.
*If **YES**, consider cyber security hygiene risks posed by the vendor (see the ASD's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks").* *If **NO**, go to Section 2.* ***Note** – there are many non-Five Eyes countries whose interests, values and systems of government align with Australia's. Organisations may wish to expand the list of countries in this section for future assessments, informed by previous responses to Section 2.*	
Section 2 – Vendor jurisdiction hazard	
Question	**Example resources and information to assist** (more resources available at **Appendix A**)
The beneficial owner of the vendor could be reasonably inferred to reside in a jurisdiction where:	
There is a risk of a foreign government compelling the vendor to provide access to its private data to the government or its national security agencies (indicated by policies, legal frameworks, or public reports)?	• United Kingdom Government's Overseas Business Risk collection • World Justice Project Rule of Law Index
The jurisdiction has been the subject of an Australian Government cyber attribution? Has the Government sanctioned the jurisdiction, or an entity within the jurisdiction, under Australian sanction law?	• Australian sanctions and the Consolidated list • Online Search – ' (insert country) Australia cyber attribution'
There is information indicating government sanctioned economic coercion, intellectual property theft and/or technology transfer campaigns targeting Australia and/or a Five Eyes country (Australia, Canada, New Zealand, UK, and US)?	• United States Trade Representative annual review / watch list on global intellectual property protection • Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA • Council of Foreign Relations Cyber Operations Tracker
There is information indicating the vendor and/or its parent company has been sanctioned on grounds of corrupt, coercive, collusive or obstructive practices, or other integrity violations in another jurisdiction?	• OpenSanctions: Find sanctions targets and persons of interest • World Bank Listing of Ineligible Firms and Individuals • US Office of Foreign Assets Control - Sanctions List Search • Financial Action Task Force "Black and grey" lists
*If the answer is **YES** to any of the above, go to Section 4. If **NO**, go to Section 3.*	

Section 3 – State ownership, control or influence	
Question	**Example resources and information to assist** (more resources available at **Appendix A**)
State ownership, control or influence could be inferred where:	
The vendor is subject to state ownership or control structures, including public information on state shareholding of >50% or outsized state influence in corporate decision-making?	• Further information can be available on securities websites (such as the Australian Securities Exchange), annual reports and business news reporting.
There are politically exposed persons (PEPs) in senior leadership roles?	• OpenSanctions: Find sanctions targets and persons of interest • Attorney-General's Department' Foreign Influence Transparency Scheme Public Register • AUSTRAC Regulatory quick guide - Politically exposed persons • Sanctions | United Nations Security Council • For more information and guides on PEPs, see Appendix A.
There is a special relationship between the vendor and a foreign government, providing a benefit such as special legal rights or legal status in their jurisdiction, or a privilege like unusual state funding arrangements or contracts?	• Such information can be available on business news reporting, and geopolitical analysis and commentary.
*If the answer is **YES** to any of the above, go to Section 4.* *If **NO**, consider cyber security hygiene risks posed by the vendor (see the ASD's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks").*	

Section 4 – Access and Control	
Question	**Example resources and information to assist** (more resources available at **Appendix A**)
Is the product or service connected, intermittently or continuously, to the internet, organisation systems, or subject to third-party access?	Information can be available on their vendor's website, contract or directly sourced from the company.
Does the vendor have excessive or unusual data collection practices?	
*If the answer is **YES** to any of the above, **conduct a vendor FOCI risk assessment**.* *If **NO**, consider cyber security hygiene risks posed by the vendor (see the ASD's Australian Cyber Security Centre guidance on "Identifying Cyber Supply Chain Risks") and risks associated with disruption or suspension of service.*	

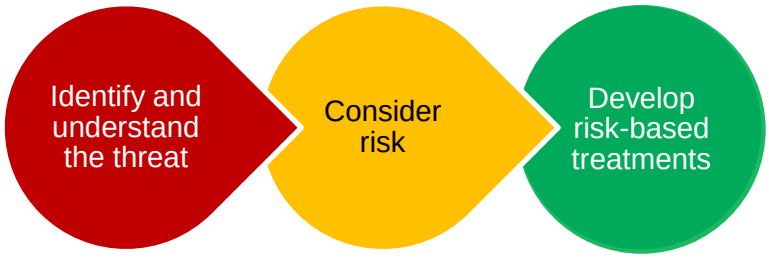
Flowchart


Vendor review
Intent
Is the beneficial owner of the vendor from a Five Eyes country (Australia, Canada, New Zealand, UK, and US)?
No
Yes
Vendor Jurisdiction Hazard
Is there a risk of a foreign government compelling the vendor to provide access to its private data to the government or its national security agencies (indicated by policies, legal frameworks or public reports)?
Has the jurisdiction been subject of an Australian Government cyber attribution? Has the Government sanctioned the jurisdiction, or an entity within the jurisdiction, under Australian sanctions law?
Is there other public information indicating government sanctioned economic coercion, intellectual property theft and/or technology transfer campaigns targeting Australia and/or a Five Eyes country (Canada, New Zealand, UK, and US)?
Is there information indicating the vendor and/or its parent company has been sanctioned on grounds of corrupt, coercive, collusive, or obstructive practices, or other integrity violations in another jurisdiction?
No
Yes
State Ownership, Control or Influence
Is the vendor subject to state ownership or control structures, including public information on state shareholding of >50% or outsized state influence in corporate decision-making?
Are there politically exposed persons in senior leadership roles?
Is there a special relationship between the vendor and a foreign government, providing a benefit such as special legal rights or legal status in their jurisdiction, or a privilege like unusual state funding arrangements or contracts?
Yes
No
Access and Control
Is the product or service connected, intermittently or continuously, to the internet, organisation systems, or subject to third-party access?
Does the vendor have excessive or unusual data collection practices?
No
Yes
Consider cyber security hygiene risks
Conduct vendor FOCI risk assessment.

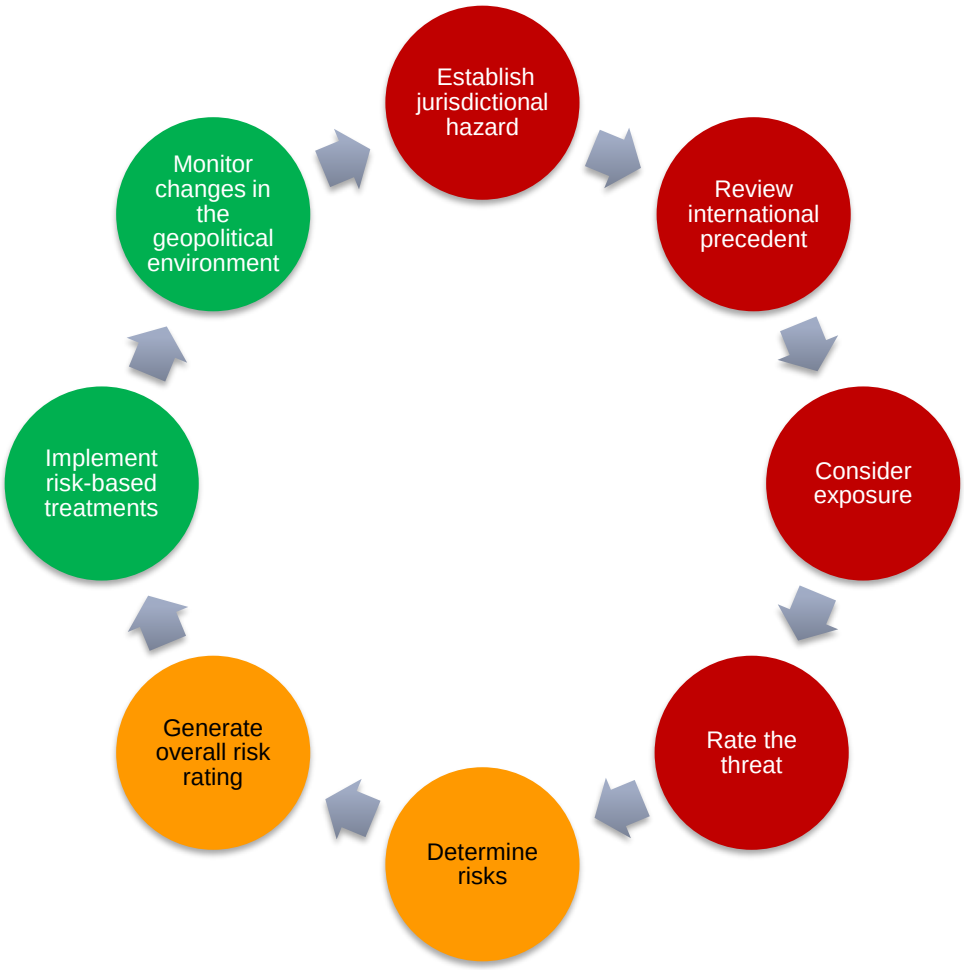
Step 2 – FOCI risk assessment

Where the vendor review questionnaire has identified a need to conduct a vendor FOCI risk assessment, organisations are encouraged to consider incorporating, in part or in whole, the below detailed methodology, comprised of a three-stage approach, into existing organisational risk assessment processes.

Three-stage approach



The full cycle of the FOCI risk assessment process could be conceived as:



Identify and understand the threat

Jurisdictional hazard

Legislative and policy settings in different jurisdictions enable certain foreign governments to compel entities to provide information or otherwise assist with foreign interference, espionage and sabotage activities.

Organisations should establish a jurisdictional hazard rating for foreign vendors, which will inform subsequent risk assessment steps. Organisations are encouraged to maintain awareness of developments in the geopolitical environment, which may alter jurisdictional hazard, particularly if there is a deterioration of bilateral relations with Australia. Regardless of whether an organisation is likely to be a target, organisations should remain cognisant of the risks posed by a rapidly changing geopolitical environment. **Appendix A** provides a non-exhaustive list of sources that can assist in security and geopolitical awareness building.

For example, sanctions regimes implemented in response to a situation of international concern might require use of products or services from that jurisdiction to cease at short notice (e.g. international sanctions on Russia following the invasion of Ukraine). Further, should Australian bilateral relations with a trade partner significantly deteriorate, its government could direct vendors or parent companies from their jurisdiction to withdraw from the Australian market.

While the process of identifying the threat is similar to the vendor risk review determination, organisations should develop more in-depth understandings of the specific jurisdictional context. Indicators of heightened jurisdictional hazard include:

- legal frameworks and/or policies which enable a foreign government to compel entities to take adverse action, without reasonable aims, in another jurisdiction;
- a lack of reasonable transparency measures (covering legal, regulatory, corporate and financial information) which enable foreign governments to conceal state ownership or control of a vendor;
- available information indicates competitive or adversarial strategic intent towards Australia and other Five Eyes partners or likeminded countries;
- documented history of offensive cyber, espionage and foreign interference campaigns;
- degree of direct government market intervention (e.g. control of commercial entities, expropriation, industry subsidies) or cooperation (e.g. commercial entities voluntary sharing sensitive information); and
- reported history of using economic coercion, arbitrary arrest or detention of foreign workers, intellectual property theft, and/or technology transfer campaigns targeting Australia and/or allies.

While certain jurisdictions have clear enabling legislation, which require vendors to assist in intelligence and foreign interference activities, other foreign governments are more opaque in their approach. Beyond the legislative and policy settings in certain jurisdictions, additional indicators of a foreign vendor's susceptibility to extrajudicial direction include:

- state ownership or control structures, including majority, or otherwise significant, shareholding;
- politically affiliated, or otherwise exposed, persons in senior leadership roles; and
- unusual or otherwise notable state funding streams, including in initial organisation establishment (e.g. seed funding), subsidies and significant government contracts and agreements.

Some jurisdictions have taken or are taking steps to make corporate and accounting information less transparent or accessible to conceal government ownership, control, or influence. Foreign vendors and their parent company headquartered in democratic countries with strong rule of law, effective judiciary, transparent government processes, and freedom of the press are at lower risk of being compelled or exploited to conduct or facilitate foreign interference, espionage and sabotage activities in Australia.

Identify international precedent

Organisations should research and use public information to identify if any government has placed regulations, restrictions or sanctions on the vendor and/or any associated or parent organisations, in relation to national security or cyber security risk. If such regulations are identified, they should be considered when establishing jurisdictional hazard (noting some jurisdictions implement arbitrary trade restrictions to reflect the state of bilateral relations). The existence of regulation and restrictive measures in another jurisdiction may indicate risks requiring treatment.

Establish exposure

After determining the jurisdictional hazard of each vendor, organisations should establish their exposure to the threat. Establishing exposure is a three-fold process:

1. **Review your organisation context** – why might your organisation be subject to foreign interference, espionage, or sabotage?

   Organisations should conduct a review to understand why they may be targeted, what may be targeted and what the consequences of that activity are to organisational processes and Australian national security more broadly.

   For example, if your organisation:

   - owns or operates an asset designated as critical infrastructure (CI);
   - is in the supply chain of a CI declared asset;
   - is generally important to national interests and security, yet falls outside of the classes of CI; or
   - is in the possession of information or systems that may be of interest to adversaries.

   Organisations should also consider these broad environmental risks when considering their exposure, resilience and mitigation plans:

   - Do you provide an essential product/service?
   - Do you have access to significant data (volume, nature, sensitivity)?
   - Do you have intellectual property that may provide a competitor an advantage?
   - Are there dependencies on your product/service?
   - Are you connected, or adjacent to, government or critical infrastructure processes or information?
   - Do you provide services to government, military or sensitive sites and facilities?
   - What would the broader community consequences be if there is disruption to your products/services?
   - Do you have any critical assets or over-reliance upon single suppliers?
   - What components of your organisation need to be protected from interference?

2. **Understand the product/service offering**
   - What level of access and/or control does the product/service provide the vendor?
   - Does the product originate with your vendor, or are they reselling a ‘white label’ product that originates with a vendor of concern?

3. **Access, control and connectivity** are the greatest determinants in establishing threat exposure. Organisations should seek to create a hierarchy of exposure based on the degree of access, control and connectivity the product or service provides (for example, vendors providing products or services such as security, software, communications, information processing and storage,

operational technologies and adjacent processes have inherently greater exposure than less invasive or non-connected products or services).

- What is the nature of the product/service provided by the vendor?
- What level of access or control does the provision of that product or service provide over your business operations or information?
- Is the product or service connected to the internet or subject to (remote) third party access?
- Would you consider the role of the product/service or its processes to be sensitive or a critical asset?
- What are the dependencies on the product/service provided by the foreign vendor?
- What are the consequences to your business should the product/service be disrupted?

4. **Consider the foreign vendor** – what is the relevant legislation influencing the vendor's susceptibility to extrajudicial and extraterritorial direction?

   Some foreign governments impose obligations on entities even when operating outside of their jurisdiction or legal framework. Consider whether the vendor is obligated to comply with foreign government demands, as well as the strength of the foreign government's privacy legislation and regulations.

   Organisations must be proactive in establishing the jurisdiction hazard posed by vendors. Organisations must also assess the level of access and control the vendor may have by virtue of their product/service and associated risks in the vendor's supply chains.

   - What is the nature of the vendor's access to your organisations' information and/or assets? I.e. is it ongoing, and how is access provided.
   - Who may have access to your information and/or assets?
   - Does your vendor use any subcontractors? Are you aware of the threat they may pose?

Rate the threat

Following the above steps, organisations should rate the threat. Threat is defined here as a combination of intent and capability of malicious actor to undertake a course of action, and can be visualised as:

Threat = intent *(Vendor jurisdiction hazard + international precedent)* ***x capability*** *(exposure)*

Using this formula, organisations should develop a threat rating. Determining the threat is critical to ensure accurate mapping of risks and the development of risk-based treatment options. An example of a threat matrix is included below and the following page:

Intent

Capability	**Unlikely**	**Possible**	**Probable**	**Expected**	**Certain**
Extreme	Moderate	High	Very high	Very high	Very high
Significant	Low	Moderate	High	Very high	Very high
Moderate	Very low	Low	Moderate	High	Very high
Limited	Very low	Low	Low	Moderate	High
Nil	Very low	Very low	Very low	Low	Moderate

Threat level descriptors

Very high	Sure to happen and/or have major consequences
High	Almost sure to happen and/or to have major consequences
Moderate	Likely to happen and/or to have moderate consequences
Low	Possible to happen and/or to have moderate consequences
Very low	Unlikely to happen and/or have minor negligible consequences

Consider risks

Organisations are encouraged to consider specific impacts should the threat materialise. Organisations must develop their own understanding of risks unique to their activities. This risk assessment process considers three risks posed by foreign vendors of concern, which are detrimental to business interest and national security. These risks include:

- Sabotage (including arbitrary suspension of service)
    - Any activity that damages, impairs or introduces a vulnerability to public infrastructure, including electronic systems, prejudicing Australia's national security, or to advantage a foreign power.
        - For example, a malicious cyber operator gains access to industrial control systems for part of Australia's electricity grid and manipulates those systems to disrupt power supply to several Australian states.
- Espionage (theft of intellectual property, sensitive information, or bulk data):
    - Theft of information or capabilities by someone either acting on behalf of, or intending to provide information to a foreign power or foreign political organisation, that will prejudice Australia's national security or advantage the national security of a foreign country. Espionage can target defence, political, industrial, foreign relations, commercial, or other information or things that are usually unavailable to the foreign power.
        - For example, an Australian Government employee removes privileged or sensitive information from a computer network via USB drive and provides that USB drive to a foreign power or proxy.
- Acts of foreign interference:
    - Activities carried out by, or on behalf of, are directed or subsidised by, or are undertaken in active collaboration with, a foreign power and either involves a threat to a person, or is clandestine or deceptive, and is detrimental to the Australia's interests.
        - For example, a foreign power covertly directs a community member to donate to an Australian politician's political campaign. The Australian politician is subsequently positively disposed towards the community member, and agrees to the individual's subsequent request that the Australian politician take a particular position on an issue of benefit to the foreign power. The community member does not tell the Australian politician that a foreign power directed them to engage in this behaviour. In this example, both the foreign power and the community member have engaged in an act of foreign interference, but not the politician, who is unwitting to the covert involvement of the foreign power.

These risks could be considered either manifest (e.g. apparent once they have occurred) or latent (e.g. may be occurring but not obvious), however both are capable of damaging business operations, industry efficacy, market confidence, and the Australian national interest more broadly. These security risks are not mutually exclusive – they can overlap and, in some instances, facilitate each other. For example, espionage can enable foreign interference.

The above illegal activities should be plotted on a risk matrix (likelihood x consequence), with likelihood derived from an understanding of the threat. Threat likelihood alone does not determine mitigation effectiveness. When determining consequence, organisations are encouraged to consider the implications on business operations and national security more broadly.

Determining the consequences is critical to ensure accurate mapping of risks and the development of commensurate treatment options. An example of a risk matrix and definitions are included below:

Risk Matrix	**Consequence**				
Likelihood	**Low**	**Moderate**	**Significant**	**High**	**Extreme**
Almost certain	Medium	High	Extreme	Extreme	Extreme
Likely	Medium	Significant	High	Extreme	Extreme
Possible	Low	Medium	Significant	High	Extreme
Unlikely	Low	Medium	Medium	Significant	High
Improbable	Low	Low	Low	Medium	Medium

Establishing the identified risk and overall risk posed by a vendor will assist the assessing entity in determining appropriate treatments.

Likelihood description

Improbable	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
0-5%	6-20%	21-50%	51-80%	81-99%
The event may occur in exceptional circumstances.	The event may, but is not likely to, occur in normal circumstances.	The event may occur at some time.	The event is expected to occur at some time, or will probably occur in most circumstances.	The event is expected to occur in most circumstances.
Likelihood statements – explaining estimative language This descriptor uses a range of estimative terms, from 'improbable' to 'almost certain', to convey analytical judgements about the likelihood of a development or event occurring. Your judgments are not factual statements; they reflect your best understanding of a scenario or situation at a point in time, based on the available information. This table shows the relationships between the estimative terms and how they correspond to approximate ranges of likelihood.				

The following consequence definitions may assist organisations in determining risk:

Consequence Level	Description
Extreme	Adverse activity would plausibly result in: • extreme economic, financial and reputational costs to the organisation with nil recovery options; • disruption, degradation or destruction of a critical business asset, with catastrophic impacts across the organisation with lasting impacts; • exfiltration of information, data or technology causing exceptionally grave damage to the organisation; • extremely detrimental impacts to the organisation's reputation and public confidence; and/or • extremely severe and enduring foreign interference activity, enabling malicious foreign actors to coerce the organisation through control of or influence over its assets.
High	Adverse activity would plausibly result in: • severe economic, financial and reputational costs to the organisation with limited recovery options; • disruption, degradation or destruction of the organisation's assets with severe impacts across the organisation; • exfiltration of information, data or technology causing severe damage to the organisation; • severe impacts to the organisation's reputation and public confidence; and/or • severe and enduring foreign interference activity, enabling malicious actors to coerce the organisation through control of or influence over its assets.
Significant	Adverse activity would plausibly result in: • significant economic, financial and reputational costs to the organisation with potential recovery option; • disruption, degradation or destruction of organisation's assets with some significant downstream impacts; • exfiltration of information, data or technology causing significant damage to the organisation; • significant impacts to the organisation's reputation and public confidence; and/or • significant but relatively isolated foreign interference activity.
Moderate	Adverse activity would plausibly result in: • limited economic, financial and reputational costs to the organisation with viable recovery options; • localised disruption, degradation or destruction of the organisation's assets with minor downstream impacts; • exfiltration of information, data or technology causing minor damage to the organisation; • limited impacts to organisation's reputation and public confidence; and/or • limited foreign interference activity.
Low	Adverse activity would plausibly result in: • negligible economic, financial and reputational costs to the organisation with solidified recovery options; • localised disruption, degradation, or destruction of the organisation's assets with negligible downstream impacts; • exfiltration of information, data or technology causing negligible damage to the organisation; • negligible impacts to the organisation's reputation and public confidence; and/or • no foreign interference activity.

Overall risk ratings may adhere to the following definitions:

Risk level	Description
Low	The vendor and product or service offering presents **minimal risk** to business operations and/or Australian national security.
Medium	The vendor and product or service offering presents **some risk** to business operations and/or Australian national security.
Significant	The vendor and product or service offering presents **significant risk** to business operations and/or Australian national security.
High	The vendor and product or service offering presents an **unacceptable risk** to business operations and/or Australian national security.
Extreme	The vendor and product or service offering presents **extreme and unacceptable risk** to business operations and/or Australian national security.

Treatments

To mitigate the threat posed by vendors, Australian companies and organisations may have to compromise on up-front cost. This may mean spending more on products and services delivered by secure and verifiable technologies and vendors. An up-front investment in a more secure product can reduce disruption and result in significant savings in the longer term. This is especially relevant as domestic and international regulatory environments and technology sanctions regimes may develop in response to situations of international concern.

Risk treatments should be commensurate to the identified risk. While organisations will have their own treatment mechanisms, this process proposes five broad treatment outcomes:

1. Nil action – there is insufficient risk to justify an intervention in relation to the vendor and product or service offering.
2. Technical controls – scalable solutions to treat the specific access and control risks. There are three categories of technical controls: technical restrictions (e.g. operation system controls, etc.); technical transparency (e.g. code audits, penetration testing, open sourcing, etc.); and data localisation requirements (e.g. isolated data silos, domestic payments, transmission constraints, etc.).
3. Structural requirements – the imposition of contractual obligations on a vendor (e.g. reporting on security performance, adherence to stipulated risk management policies and processes, supply chain mapping, requirements on sub-contractors etc.).
4. Diversify vendors – the risk is managed through diversification beyond a sole source to ensure there is not a single point of failure or over-reliance upon a source jurisdiction.
5. Restriction – if the risk cannot be effectively treated by other means, the assessing entity is recommended to restrict access to the vendor in procurement processes, or replace the product or service if procurement has already occurred. Restriction may occur proactively, when existing contracts expire or products due for refresh, or in response to some geopolitical event.

In certain circumstances, the Australian Government through ASD's Cyber Security Partnership Program and/or ASIO Outreach can assist with the provision of treatment advice. Organisations must establish regular compliance review mechanisms to ensure the selected treatment is and remains effective.

Evolving environment

The strategic and regulatory environment continues to evolve. As technology becomes more interconnected and assumes an even greater role in business and government operations, bad faith state actors will increasingly use private entities and cyber operations to conduct malicious activities.

The Australian Government is striving to establish a more considered digital regulatory environment. This includes government consideration of all options to manage whole-of-economy supply chain risks. Organisations that are active in their vendor and supply chain risk management approaches will be better placed to navigate current and emerging threats and associated regulatory processes.

Effective FOCI risk management within supply chains necessitates a cooperative approach between Government and industry. Industry is encouraged to share information relating to supply chain risks with Government who can advise on appropriate treatment options (see **Appendix A** for relevant Government agencies). Further, the greater the Government understands the scale and scope of threat across the Australian economy, the more accurate and effective the advice that can be provided to industry.

Periodic review

It is recommended to undertake a periodic review to assess the effectiveness of existing FOCI risk management. Periodic reviews will ensure exposure risk is minimised as the strategic and operating environment continues to evolve (for example, the decoupling from the Russian market as a result of international sanctions due to the Russo-Ukrainian War) or when new information on FOCI risks become available. This should include the periodic review of implemented control measures to ensure their ongoing appropriateness and effectiveness based on the latest information.

The frequency of the periodic review process should be commensurate with the rate at which an organisation and its operating environment is changing.

Glossary

Note: The terms defined within this document are specific to this guidance document only.

Beneficial owner	An individual or persons who ultimately own or control an interest in a legal entity or arrangement, such as a company, a trust, or a foundation. Ownership and control may be direct (such as through shares) or indirect (such as shares held by a third party on the individual's behalf). 'Control' means having the ability to determine decisions about the entity's financial and operating policies
Bulk data exfiltration	The unauthorised or non-transparent transfer or exploitation of personally identifiable information, aggregate population, and company datasets and other data with value by companies, governments, or individuals.
Data localisation	The practice of storing and processing data within a specific geographic location.
Economic coercion	A broad term that can include a range of trade or investment related actions and measures, designed to achieve an underlying objective. Trade-related economic coercion uses, or uses the threat of, measures affecting trade and investment in an abusive, arbitrary, or pretextual manner to pressure, induce or influence a foreign government into taking, or not taking, a decision or action in order to achieve a strategic political or policy objective, or prevent or interfere with the foreign government's exercise of its legitimate sovereign rights or choices. Trade-related economic coercion is frequently disguised as a legitimate government regulatory or public policy measure unrelated to the strategic objective that it is intended to advance. It may also occur indirectly through government entrustment or direction given to state-owned, state-controlled, or private enterprises.
Espionage	Theft of information or capabilities by someone either acting on behalf of, or intending to provide information to, a foreign power or foreign political organisation, that will prejudice Australia's national security or advantage the national security of a foreign country. Espionage can target defence, political, industrial, foreign relations, commercial, or other information or things that are usually unavailable to the foreign power.
Extrajudicial direction	A direction issued by an actor outside of, or without the permission of, the official legal system or legislation within the relevant jurisdiction.
Extraterritorial direction	A direction issued in the situation when a country extends its legal power beyond its territorial boundaries.
Five Eyes partners or countries	An alliance of five democratic countries who engage in mutual data and intelligence sharing and cooperate in areas of national security. This alliance includes Australia, Canada, New Zealand, the United Kingdom, and the United States.

Foreign interference	Activities carried out by, or on behalf of, are directed or subsidised by, or are undertaken in active collaboration with, a foreign power and either involves a threat to a person, or is clandestine or deceptive and is detrimental to the Australia's interests.
Foreign Ownership, Control or Influence (FOCI)	An entity is considered to be operating under FOCI when a foreign interest has the power, direct or indirect whether or not exercised, and whether or not exercisable, through the ownership of the company under the purview of its National Security Authority/Designated Security Authority, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that entity in a manner which may result in unauthorised access to classified information or adversely affect the performance of classified contracts or may otherwise be contrary to the interests of national security.
Intellectual property theft	The theft or unauthorised removal or movement of intellectual property such as patents, copyrights, trademarks, trade secrets, or specific work products, from the rightful property holder. The theft may be intentional through malicious insiders or specific threat actors, or unintentional through human error.
Politically exposed person (PEP)	A person who has been entrusted with a prominent public function. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence they may hold. The terms "politically exposed person" and senior foreign political figure are often used interchangeably, particularly in international forums. The following are examples of politically exposed persons: • current or former government officials; • high-ranking military officers; • senior officials of major foreign political parties; • judges and top-level judiciary positions; • senior executives or board members of foreign government-owned commercial enterprises; or • immediate family members or publicly known personal or professional associates of a PEP.
Product	Any kind of goods or services, which could facilitate the operations of a business. Technology products could include anti-virus software and cloud platforms, internet of things (IoT) devices such as smartphones, surveillance cameras, and drones, as well as social media, payment systems, enabling technologies, and communications equipment and products with immediate adjacency to the technology sector, such as biotechnology and genomics or automated mechanical systems.
Sabotage	Any activity that damages, impairs or introduces a vulnerability to public infrastructure, including electronic systems, prejudicing Australia's national security or to advantage a foreign power.
Sanctions	Restrictive measures imposed on a particular individual, entity, country, group or vessel in response to a situation of international concern. Sanctions take many forms including targeted financial sanctions, travel bans, trade sanctions, and commercial activity sanctions. They may be designed to bring a situation of international concern to an end by influencing those responsible; to limit adverse impacts of a situation; or to penalise those responsible.

Service	Any professional service, which facilitates the use of technology, by providing, specialised solutions through a combination of technological offerings and expertise. This could include services like software development, cyber security, IT support, consulting, research, hosting, and asset management.
Technology vendor	An entity that provides a technology-related product or service offering.
Vector	A threat or attack vector is a path, method, or means by which an attacker can break into a system, facility, or organisation.
Vendor	An organisation in a supply chain, which makes goods and services available to businesses, such as a supplier.