



## NATIONAL SECURITY

Last updated: 12 April 2022.

- Foreign investment plays an important and beneficial role in the Australian economy. It helps drive economic growth, creates skilled jobs, improves access to overseas markets and enhances productivity. Without foreign investment, production, employment, and income would all be lower.
- Australia continues to welcome and remains an attractive destination for foreign investment. However, risks to Australia's national interest, particularly national security, have increased as a result of developments including rapid technological change and changes in the international security environment.
- Foreign investment carries risks related to the potential access and control investors may obtain over organisations and assets. When used as a vector for malign activities, foreign investment can harm national security. Foreign ownership of critical infrastructure and other sensitive assets may provide opportunities for foreign intelligence services to conduct espionage, or sabotage or other activities contrary to Australia's national security interests. Ongoing compromise of critical infrastructure assets can result in cascading consequences significantly impacting Australia's economy and national security.
  - This guidance is intended to provide information to investors on the operation of foreign investment framework with regards to national security, including information on the types of actions that may pose national security risks.

## Looking for more?

|  |    |
|--|----|
| A: National security .....   | 3  |
| B: Mandatory notification - ‘notifiable national security actions’ .....                           | 4  |
| National security business .....   | 4  |
| <i>Transitional arrangements for the expanded definition of a national security business</i> ..... | 8  |
| National security land .....   | 9  |
| Acquisitions of an interest in national security land .....  | 10 |
| Securities in a land entity that holds national security land.....                                 | 11 |
| C: Call in power – ‘reviewable national security actions’ .....                                    | 11 |
| Voluntary notification – ‘reviewable national security actions’ .....                              | 11 |
| D: National security exemption certificates.....   | 11 |
| E: Last resort power .....   | 12 |
| F: Sectoral guidance .....   | 13 |
| Financial services .....   | 13 |
| Communications .....   | 14 |
| Commercial construction contractors.....   | 16 |
| Commercial real estate .....   | 16 |
| Critical minerals .....  | 17 |
| Critical service providers and suppliers .....   | 18 |
| Critical Technologies.....   | 19 |
| Defence Providers .....  | 20 |
| Energy.....  | 24 |
| Electricity.....   | 24 |
| Gas .....  | 24 |
| Liquid fuels.....  | 25 |
| Energy Market Operators .....  | 26 |
| Food and Grocery.....  | 26 |
| Health .....   | 26 |
| Higher education facilities .....  | 27 |
| Information technology, data and the cloud.....  | 28 |
| Nuclear.....   | 30 |
| Space .....  | 31 |
| Transport.....   | 31 |
| Water and sewerage.....  | 34 |
| Further information .....  | 34 |

## A: NATIONAL SECURITY

The *Foreign Acquisitions and Takeovers Act 1975* (FATA):

- requires mandatory notification of proposed investments in national security land, proposed acquisitions of interests in exploration tenements over national security land, a proposed direct investment in a national security business or a proposal to start a new national security business;
- allows investments that are not required to be notified to be ‘called-in’ for review on national security grounds;
- allows investors who choose to voluntarily notify to receive certainty from being subject to ‘call-in’; and
- provides a last resort power, which, in exceptional circumstances, permits the Treasurer to impose conditions, vary existing conditions, or, as a last resort, require the divestment of any approved investment where national security risks emerge. This power is subject to a number of safeguards.

Investments subject to the national security test are assessed against factors that give rise to national security concerns.

The existing national interest test remains unchanged including the factors that typically underpin the assessment process, such as the character of the investor, competition, impact on the economy and community, national security and other Government policies (including tax).

To avoid overlap between the two tests, wherever the broader national interest test applies to a particular action, only that test is applied. This is because national security is already a relevant factor that the Treasurer considers when assessing the national interest.

### Example 1

Overseas Pension Fund (OPF) is a foreign government investor and wishes to acquire a direct interest in Anita’s Telecom Pty Ltd (AT). AT is a carrier under the *Telecommunications Act 1997* and has total assets of \$100 million. AT is considered a national security business.

OPF is required to notify the Treasurer as it is a foreign government investor proposing to take a direct interest (a significant and notifiable action). In the same application, OPF is also required to notify a proposed acquisition of a national security business (a notifiable national security action). As the proposed investment is both a significant and notifiable action and a notifiable national security action, it will be considered against the broader national interest test (not just in relation to potential national security concerns).

## B: MANDATORY NOTIFICATION - 'NOTIFIABLE NATIONAL SECURITY ACTIONS'

A foreign person proposing to take a notifiable national security action must seek foreign investment approval before taking the action. Penalties may apply for failure to notify. An action is a notifiable national security action if the action is taken, or proposed to be taken, by a foreign person and the action is any of the following:

- to start a national security business;
- to acquire a direct interest in a national security business;
- to acquire a direct interest in an entity that carries on a national security business;
- to acquire an interest in Australian land that, at the time of acquisition, is national security land; or
- to acquire a legal or equitable interest in an exploration tenement in respect of Australian land that, at the time of acquisition, is national security land.

Importantly, a business would not be a national security business unless it is publicly known, or could be known by making reasonable inquiries, that the business meets the criteria for being a national security business. Similarly, the definition of national security land is limited by the requirement that the existence of an interest in the land held by an agency in the National Intelligence Community (the NIC) is publicly known, or could be known by making reasonable inquiries.

- The purpose of the reasonable inquiry limitation is to ensure a foreign person taking an action is not contravening provisions or committing offences if a person, after reviewing publicly available information and making reasonable enquiries about the business or land the subject of the investment, is still not in a position to ascertain that the business or land meets the relevant criteria for being a national security business or national security land. What constitutes reasonable enquiries depends on the circumstances of the case.
- In this context, investors are expected to undertake a sufficient level of due diligence in order to make an informed assessment of whether the business is a national security business or the land is national security land. Investors should retain evidence of this process, and how they came to their conclusion about the status of the relevant business or land.

### Nationalsecurity business

National security businesses are endeavours that if disrupted or carried out in a particular way may create national security risks. A business is a national security business if it is carried on wholly or partly within Australia, whether or not in anticipation of profit or gain, and it:

- is a responsible entity (within the meaning of the *Security of Critical Infrastructure Act 2018*) for an asset; or
- is an entity that is a direct interest holder in relation to a critical infrastructure asset (within the meaning of those terms in the *Security of Critical Infrastructure Act 2018*); or

- is a carrier or nominated carriage service provider to which the *Telecommunications Act 1997* applies; or
- develops, manufactures or supplies critical goods or critical technology that are, or are intended to be, for a military use, or an intelligence use, by defence and intelligence personnel, the defence force of another country, or a foreign intelligence agency; or
- provides, or intends to provide, critical services to defence and intelligence personnel, the defence force of another country, or a foreign intelligence agency; or
- stores or has access to information that has a security classification; or
- stores or maintains personal information of defence and intelligence personnel collected by the Australian Defence Force (ADF), the Department of Defence (Defence) or an agency in the NIC which, if accessed, could compromise Australia's national security; or
- collects, as part of an arrangement with the ADF, Defence or an agency in the NIC, personal information on defence and intelligence personnel which, if disclosed, could compromise Australia's national security; or
- stores, maintains or has access to personal information on defence and intelligence personnel that has been collected as part of an arrangement with the ADF, Defence or an agency within the NIC, which, if disclosed, could compromise Australia's national security.

**Sensitive information****Information that has a security classification**

For foreign investment purposes, information that has a security classification means information that has been classified as Protected or higher within the Australian Government Protective Security Policy Framework (PSPF) and information with equivalent classifications from other countries.

**Personal information of defence and intelligence personnel**

Personal information of defence and intelligence personnel is information about individuals, collected by or on behalf of the ADF, Defence or an agency in the NIC, which if accessed or disclosed could compromise Australia's national security. Information may not necessarily be classified, but could pose a national security risk if, for example, it could be used to influence personnel or to derive an advantage from knowing aggregate statistics about the ADF or the NIC. Commercial datasets collected by private entities that contain personal information of defence and intelligence personnel that are unconnected to their roles relevant to national security would not be included. For example, the dataset associated with a supermarket rewards program that may be used by customers who are also defence personnel would not be captured by this definition.

**Example 2**

Foreign Data Centre Acquisitions Pty Ltd (FDCA) is a foreign person and wishes to acquire a direct interest in Damien's Data Centres (DDC). DDC provides data centre services to the NIC, and as part of this, stores classified information above the protected level. As DDC stores information that has been classified as Protected or higher within the Australian Government PSPF, DDC is considered a national security business. FDCA is required to notify the Treasurer as it is proposing to acquire a direct interest in a national security business.

**Example 3**

A large fashion outlet's rewards program collects information on customers, including identification and details about purchasing patterns. It is possible that some customers are part of the ADF and the NIC. However, the fashion outlet would not be considered a national security business because while collecting information about members of the ADF and the NIC, the information is not in connection to their work nor collected because of where they work.

***Carrying on a national security business***

Whether a business is considered to be carried on wholly or partly in Australia depends on the facts of each case, but the business would generally be expected to have a presence in Australia or some form of connection to Australia to be considered a national security business.

Some factors which may help to determine whether a business has a presence or connection to Australia include:

- A physical presence in Australia, such as locally engaged employees or a lease of office space;
- The need for regulatory approvals to operate in Australia, such as the requirement to have an Australian Business Number (ABN);
- The payment of tax in Australia;
- Whether the business receives payments into an Australian bank account for goods and services rendered;
- The terms of the contract, such as requirements to undertake certain steps in Australia;
- Using an agent in Australia to assist with some aspect of its business activities; or
- A website with a .au domain.

***Starting a national security business***

A foreign person must notify and seek foreign investment approval prior to the foreign person starting to carry on a national security business. If already carrying on a national security business, merely establishing a new entity (for example, creating a subsidiary) is not considered to be starting a national security business.

Whether undertaking a new business activity is considered to be starting a national security business depends on the facts in each case but the new activity would generally need to be sufficiently different from activities already carried out to be considered to be starting a national security business.

Some factors which may help to determine whether a business activity is sufficiently different from activities already carried out by the investor include:

- Whether the new activity is in a different division under the Australian and New Zealand Standard Industrial Classification (ANZSIC) Codes, noting changes in activity within ANZSIC codes may still constitute starting a national security business;
- Whether new licences or approvals are required;
- Whether new employees with different skillsets need to be engaged;
- Entering into business contracts or investment in a new product or service that is not incidental to the current business activity; or
- The new activity results in a materially different product, input or service than previously provided.

**Example 5**

Foreign-owned Heavy Machinery Pty Ltd (HM) manufactures bulldozers and other machinery for the mining industry. The Department of Defence issues a tender for new tanks and HM wins the contract. Manufacturing tanks is sufficiently different from manufacturing bulldozers. As the tanks are for a 'critical' military use, HM is starting a national security business and must notify the Treasurer and seek foreign investment approval.

**Example 6**

Foreign-owned Sensor Technologies Pty Ltd (ST) is working to develop a new heat-seeking technology for early detection of bushfires. The Department of Defence subsequently contracts ST to adapt the new technology for a 'critical' military purpose. Even though the technology now has a military use, ST has not substantially changed its business activities so it is not considered to be starting a national security business. However, ST is now a national security business as it now develops and supplies a 'critical' technology for military use, so foreign investors wanting to take a direct interest in ST in the future will need to notify the Treasurer and seek foreign investment approval.

**Example 7**

Foreign-owned Hydrocarbon Storage Pty Ltd (HS) operates a gas storage facility. HS has a current maximum daily withdrawal capacity of 50 terajoules per day, however due to growing demand, HS will be expanding its maximum daily withdrawal capacity to 100 terajoules per day. As expanding a gas storage facility does not sufficiently change the nature of the business, HS is not starting a national security business and will not need to notify the Treasurer and seek foreign investment approval. However, HS is now a national security business (as its maximum daily withdrawal capacity is above the 75 terajoule threshold) so foreign investors wanting to take a direct interest in HS in the future will need to notify the Treasurer and seek foreign investment approval.

**Example 8**

Foreign-owned Green Pty Ltd (Green), a manufacturer of air-to-ground missiles, has entered into joint venture with foreign-owned Rose Pty Ltd (Rose), a manufacturer of armoured vehicles, to manufacture new missile-based weaponry. The establishment of the joint venture entity between Green and Rose is considered to be starting a national security business. While Green is already a manufacturer of

missiles, Rose is undertaking a new business activity and as a result, the joint venture entity would need to notify the Treasurer to seek foreign investment approval.

#### ***Transitional arrangements for the expanded definition of a national security business***

The *Security Legislation Amendment (Critical Infrastructure) Act 2021* and the *Security of Critical Infrastructure (Definitions) Rules 2021*, which amended the *Security of Critical Infrastructure Act 2018* and repealed the *Security of Critical Infrastructure Rules 2018* with effect from 3 December 2021 and 14 December 2021 respectively, expanded the scope of a national security business defined in the *Foreign Acquisitions and Takeovers Regulation 2015*. This resulted in some actions, including those previously identified as reviewable national security actions, becoming notifiable national security actions.

The following paragraphs describe the approach taken to facilitate the efficient implementation of the change for the purposes of administering the FATA.

#### ***Pre-existing agreements***

The expanded notifiable national security action requirements are taken not to apply to an action taken under an agreement which was entered into by the parties before 14 December 2021, regardless of whether there are unmet conditions or not.

It is possible for an agreement to be reached prior to the formation of a contract, but this ultimately depends on the facts of each case. In determining whether an agreement has been reached before 14 December 2021, the agreement will need to be one where the negotiations have been completed and the parties have arrived at a mutual understanding of all the essential elements of their bargain. Therefore, the concept of an agreement does not cover any preliminary stage in negotiations or other circumstances short of a mutual understanding of all the essential elements of a bargain.

Entry into a 'head of agreement', 'letter of intent' or an 'agreement in principle' would normally not constitute an agreement for these purposes, but ultimately is a question of fact.

#### ***Pre-existing options***

If a foreign person is exercising pre-existing options under an agreement to acquire an interest in a security, asset, trust or Australian land prior to 14 December 2021, it is likely that this would not of itself give rise to a notifiable national security action. Section 15 of the FATA establishes the rule that, if a person has an option to acquire an interest in a security, asset, trust, or land, then they are taken to have acquired the interest at the time they acquire the option (whether or not they subsequently exercise that option).

#### ***Existing no objection notifications***

Where a foreign person, prior to 14 December 2021, has received a no objection notification, they do not have to apply for foreign investment approval again when taking the proposed action or executing the agreement with respect to that action, if the action is taken within the timeframe specified in the no-objection notification.

### *Existing exemption certificates*

Exemption certificates granted prior to 14 December 2021 in relation to national security actions continue to operate according to the terms of the certificate, provided the conditions (if any) specified in the certificate are met.

The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* further amended the scope of a national security business with effect from 2 April 2022. Investors need to be aware of the changes. Transitional arrangements do not apply.

### **National security land**

Land is national security land if it is:

- ‘Defence premises’ within the meaning of section 71A of the *Defence Act 1903*. This includes all land owned or occupied by Defence, including buildings and structures. It also includes Defence prohibited areas. The definition excludes subparagraph (a)(iii) of the definition which relates to vehicles, vessels or aircraft.
- Land in which an agency in the NIC has an interest, if the existence of the interest is publicly known or could be known by making reasonable inquiries.

### **Defence premises**

For the purposes of working out the scope of Defence premises under the foreign investment framework, Defence is taken to occupy land, if it has the legal right to use the land at the exclusion of others, at the time when the foreign investor is acquiring the interest in the land. The mere presence of Defence on the land will not amount to occupation.

Buildings that are owned by Defence Housing Authority are not considered to be defence premises under the foreign investment framework.

#### **Example 9**

Defence has a licence agreement with a building in Sydney CBD to undertake training exercises on the roof of the building. Under the licence agreement, Defence does not have the right to occupy the inside of the building and must only enter the building at the consent of the owner. As Defence has no right to the exclusive use of the licensed area, it is unlikely to constitute *defence premises*. If a foreign investor seeks to invest in the building in Sydney CBD, the license agreement with Defence will not render the land national security land.

### **National intelligence community land**

Agencies in the NIC are defined within the meaning of section 4(1) of the *Office of National Intelligence Act 2018*, including:

- Office of National Intelligence (ONI);
- Australian Secret Intelligence Service (ASIS);
- Australian Security Intelligence Organisation (ASIO);
- Australian Signals Directorate (ASD);

- Australian Criminal Intelligence Commission (ACIC);
- Australian Geospatial Intelligence Organisation (AGO); and
- Defence Intelligence Organisation (DIO).

The Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian Federal Police (AFP), the Department of Home Affairs (Home Affairs) and Defence (other than AGO, DIO and the ADF) are also considered to be agencies in the NIC but only to the extent that they:

- collect, correlate, produce or disseminate intelligence that relates or may relate to national intelligence priorities, requirements or capabilities; or
- are maintaining or developing a capability that materially assists those intelligence activities.

Land where these agencies have an interest is only national security land if it is publicly known or could be known by making reasonable inquiries that these agencies have an interest in the land. What constitutes an ‘interest’ in the context of land in which an agency in the NIC has an interest depends on the facts of the case. ‘Interest’ is not limited by the definition of interest in Australian land in section 12 of the FATA. For example, the term interest would include legal or equitable interests in land and an interest as a lessee or licensee (regardless of the term of the lease or licence).

#### Acquisitions of an interest in national security land

Consistent with the treatment of other types of land under the foreign investment framework, acquisitions of interests in national security land are considered on a title-by-title basis. If an investor is acquiring two separate titles of national security land under a single contract, they are taking two actions.

However, with respect to acquisitions of land under a lease, the interest in land will be determined by what is being acquired on that title. Where an investor acquires a leasehold interest over part of the title (e.g. one floor in a commercial office building), their approval covers that leasehold interest only – not approval to acquire the entire building. Similarly, where an agency in the NIC has an interest in a portion of land under one title, it is only that portion of land that is national security land. If an investor acquires an interest in land that only represents a portion of the title, and that portion is not national security land, it will not require mandatory notification as a notifiable national security action.

If the acquisition relates to the whole of the land title, which contains the national security land, this will require mandatory notification.

#### Example 10

Foreign owned Bob’s Burgers is seeking to enter into a 5-year lease with Brisbane Airport, to operate their business within the Brisbane domestic terminal. The title on which the domestic terminal is found is likely to include land where the AFP and Home Affairs may, from time to time, undertake intelligence functions. However, as the area leased by Bob’s Burgers does not include the areas where AFP and Home Affairs may conduct their intelligence functions, the leased area is not national security land. As such, Bob’s Burgers would not be required to submit a mandatory notification for a notifiable national

security action. However, Bob's Burgers could decide to voluntarily notify the Treasurer if wanting certainty that the lease does not pose a national security risk.

#### **Example 11**

A foreign company is seeking to purchase a commercial office building in Perth CBD which is located on one title of land. The foreign investor is aware that the ACIC has a tenancy over three floors of this building. This acquisition will require mandatory notification due to the foreign investor acquiring an interest in Australian land that an agency in the NIC (the ACIC) has an interest. The acquisition of the building covers the lease held by the ACIC.

#### **Securities in a land entity that holds national security land**

An acquisition of securities in a land entity that holds national security land may constitute an action to acquire an interest in national security land.

For further information, see Guidance Note 7 *Business Investments*.

The Australian Government is undertaking further work to more clearly define when interests in land in proximity to Australian Government facilities may raise national security risks. The Guidance Note will be updated in due course.

### **C: CALL IN POWER – 'REVIEWABLE NATIONAL SECURITY ACTIONS'**

The Treasurer can 'call-in' for review reviewable national security actions which are not otherwise notified, if the Treasurer considers that the action may pose national security concerns. The review can occur when the action is still proposed or up to ten years after the action has been taken. For the types of actions that may constitute a reviewable national security action see Division 4B of the FATA. See also Section I of the *Key Concepts* Guidance Note.

Once called in, an investment will be reviewed to determine if it raises national security concerns. For investments 'called in', the Treasurer may issue a no objection notification, including with conditions, or prohibit the action, or require divestment.

#### **Voluntary notification – 'reviewable national security actions'**

The Treasurer cannot call-in an action that has been notified to the Treasurer or for which a no objection notification or exemption certificate exists. A foreign person can therefore choose to extinguish the Treasurer's ability to use the 'call-in' power by voluntarily notifying a reviewable national security action. Voluntary notification will not, however, extinguish the Treasurer's ability to use the 'last resort' power.

Guidance on investment areas that may raise national security concerns, and where investors are therefore encouraged to voluntarily notify, are outlined below in sectoral guidance. The fact that an investment is not subject to mandatory notification and is not encouraged to be voluntarily notified does not limit the use of the Treasurer's call-in or other powers.

### **D: NATIONAL SECURITY EXEMPTION CERTIFICATES**

A foreign person may apply for an exemption certificate in relation to actions that would otherwise be notifiable national security actions or reviewable national security actions.

Applications for exemption certificates will be considered on a case-by-case basis to ensure they are not contrary to national security. An action that is covered by the certificate would not be a

notifiable national security action and therefore would not be subject to the notification requirements that attach to notifiable national security actions. Similarly, an action that is covered by the certificate would not be a reviewable national security action and therefore not subject to the 'call-in' power.

An investor may apply for a national security exemption certificate at the same time as applying for exemption certificates for other types of interests in a single application. For example, an investor may wish to apply for both a notifiable national security actions certificate and a businesses/entities exemption certificate at the same time. While investors will need to specify each type of interest for which they are seeking exemption, only one fee will generally be payable for the entire financial limit sought under the certificates.

For further information, see Guidance Note 9 *Exemption Certificates* and Guidance Note 10 *Fees*.

## **E: LAST RESORT POWER**

The last resort power gives the Treasurer an opportunity to review actions notified after 1 January 2021 for which a no objection notification, an exemption certificate, deemed approval or a notice imposing conditions has been given, if exceptional circumstances arise.

If a national security risk arises in connection with an action, the Treasurer may give orders directing persons to act to reduce the national security risk. The factors and conditions that need to be met before the Treasurer may exercise the last resort power are:

- That after 1 January 2021, the Treasurer was notified of the action, an application for an exemption certificate was made, or the action was reviewed under the call-in power.
- Since that time, the business, structure or organisation of the person has materially changed, or the person's activities have materially changed, or the circumstances or the market have materially changed, or the Treasurer becomes aware of a relevant material, false or misleading statement or omission by the foreign person in notifying the action.
- The Treasurer conducts a review, receives and considers advice in relation to the action from an agency in the NIC, takes reasonable steps to negotiate in good faith with the foreign person, and is satisfied that exercising the last resort power is reasonably necessary for purposes relating to eliminating or reducing the national security risk, and that the use of other options under the existing regulatory systems of the Commonwealth, states and territories would not adequately reduce the national security risk.
- The Treasurer is reasonably satisfied that:
  - the false or misleading statement or omission directly relates to the national security risk;
  - the national security risk posed by the change of the business, structure or organisation of the foreign person or the change to the person's activities could not have been reasonably foreseen or could have been reasonably foreseen but was only a remote possibility at the time of the original approval; or
  - the relevant material change alters the nature of the national security risk posed at the time of the original approval.

If these factors and conditions are satisfied, the Treasurer may impose conditions, or vary or revoke any conditions that have been imposed, and may make orders prohibiting an action or requiring the undoing of a part or the whole of an action. This includes, as a last resort, requiring divestment.

## F: SECTORAL GUIDANCE

The information below has been provided to help investors understand the types of actions that may pose national security risks, the types of actions subject to mandatory notification and those actions where voluntary notification is encouraged. In addition, investors also need to be aware of other notification requirements in the FATA where the national interest test applies.

The guidance may change over time as Australia's security environment changes and to account for changes in other legislation. The sectoral guidance should not be understood as an exhaustive indication of those investments that may be the subject of the Treasurer's powers. The Treasurer retains the ability to exercise powers in other investment areas not listed in the sectoral guidance, where a national security risk exists. The assets listed in the sectoral guidance have been listed because foreign investment in those assets may raise national security risks. The Treasurer's powers will be exercised by reference to the particular circumstances of each case and the existence of national security concerns.

Investors are encouraged to carefully consider the type of action that is being proposed. Where the action is not a significant and notifiable action or a notifiable national security action, it is up to the investor to decide whether or not they wish to voluntarily notify based on their individual circumstances.

### Financial services

The financial services sector ensures the delivery of essential banking and finance services and underpins economic activity. A significant disruption to the financial sector would have a detrimental impact on Australia's national interest including public trust, financial stability, market integrity, the economy and national security. The information contained within the sector is a target for espionage, sabotage and foreign interference.

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business, or acquiring a direct interest in the following banking and finance businesses or entities:

- Banks, credit unions, building societies and other authorised deposit-taking institutions: Entities that own or operate an authorised deposit-taking institution with total assets above \$50 billion total, or a related body corporate of such an entity.
- Superannuation: A Registerable Superannuation Entity (RSE) licensee with assets under management of \$20 billion or more. An RSE is defined to have the same meaning as in section 10 of the *Superannuation Industry (Supervision) Act 1993*.
- Insurance: Entities that own or operate, a general insurance entity with assets greater than \$2 billion, a life insurance business with assets greater than \$5 billion, or a health insurance business with assets greater than \$0.5 billion, or a related body corporate of such an entity.

- Financial markets: Entities that own or operate the holder of a Tier 1 market license under subsection 795B(1) of the Corporations Act 2001, and has, for at least two consecutive quarters, a turnover on its market that meets one of the following:
  - 35 per cent market share or \$4 billion average daily value of traded Cash Market Products; or
  - \$15 billion average daily notional value of Futures Market Contract transactions; or,
  - \$30 billion average daily notional value of non-Cash Market Products or Futures Market Contracts.
  - 'Cash Market Product' has the meaning given by the section 3 of the *ASIC Market Integrity Rules (Securities Markets) 2017*. 'Futures Market Contract' has the meaning given by *Section 3 of the ASIC Market Integrity Rules (Futures Markets) 2017*.
- Clearing and settlement facilities: Entities that own or operate the holder of an Australian clearing and settlement facility licence that is incorporated in Australia or a related body corporate of that licence holder that is required to comply with the financial stability standards under section 827D of the *Corporations Act 2001*.
- Payment systems: Responsible entities that own or operate a payment system that is critical to the security and reliability of the financial services and markets sector (as outlined in the table below). 'Payment Systems' is as defined in the *Payment Systems (Regulation) Act 1998*, a critical payment system is critical to ensuring the security and reliability of the financial system.

| Payment system                          | Responsible entity   |
|---|--|
| Mastercard debit and credit card system | Mastercard Asia/Pacific Australia Pty Ltd (ABN 95 108 603 345) |
| Visa debit and credit card system       | Visa AP (Australia) Pty Ltd (ABN 20 134 885 564)               |
| EFTPOS card system                      | eftpos Payments Australia Limited (ABN 37 136 180 366)         |
| New Payments Platform                   | NPP Australia Limited (ABN 68 601 428 737)                     |

- Derivative trade repositories: Entities that own or operate businesses that hold an Australian derivative trade repository licence where:
  - the holder is incorporated in Australia or a related body corporate of that holder; and
  - the repository has at least \$20 trillion average daily notional value of outstanding transactions for all asset classes for at least two consecutive quarters.
- Benchmark administrators: Entities that own or operate the holder of a benchmark administrator licence or a related body corporate of that licence holder and administer a benchmark that is declared under section 908AC(2) of the *Corporations Act 2001*.

## Communications

Australia's national security is increasingly dependent on communications networks and infrastructure.

### **Telecommunications**

Telecommunications networks, systems and facilities are vital to the delivery and support of other critical infrastructure and services such as power, water and health. The access and control afforded by foreign investment in telecommunications may create opportunities for foreign actors to harm national security. A serious compromise of the telecommunications sector would have a cascading effect on other critical infrastructure sectors and significantly impact Australia's national security. The information contained within the networks and the connection to other critical infrastructure sectors also makes telecommunications networks and facilities a key target for espionage, sabotage and foreign interference activity.

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business or acquiring a direct interest in a business that is a carrier or a nominated carriage service provider to which the *Telecommunications Act 1997* applies.

A foreign person must also seek foreign investment approval prior to acquiring a direct interest in a telecommunications network or facility that is owned or operated by a carrier or carriage service provider and used to supply a carriage service.

Carriers operate telecommunications networks and infrastructure. Carriage service providers use carrier networks and infrastructure to provide services such as fixed and mobile telephone services and access to the internet. Further information is available from the [Australian Communications and Media Authority](#).

For the purposes of administering the foreign investment framework, a carriage service provider is taken to include a carriage service provider that is registered with the Telecommunications Industry Ombudsman scheme under Part 6 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999*.

### **Broadcasting**

Broadcast media play an important role in emergencies, including in disseminating and collecting information about an incident. The ability for broadcasters to deliver emergency messages is dependent on the resilience and security of transmission and distribution infrastructure. The disruption of critical transmission and distribution infrastructure which national and commercial broadcasters rely on could pose a national security risk.

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business, or acquiring a direct interest in an entity that owns or operates broadcasting transmission assets that operate at least 50 different sites. A foreign person must also seek foreign investment approval to acquire a direct interest in TX Australia Pty Ltd (ABN 98 086 979 339).

A broadcasting transmission asset is a radio communications transmitter, a broadcasting transmission tower or an associated transmission facility that is used, or capable of being used,

in connection with the transmission of a national broadcasting service, commercial radio broadcasting service, or a commercial television broadcasting service.

### **Domain namesystems**

The .au namespace plays an important role in supporting the digital economy. With the online environment becoming increasingly enmeshed with everyday life, a disruption to a critical Domain Name System could have significant implications for Australian businesses, government and the community. Malicious exploitation can compromise users' ability to conduct business, navigate the internet or compromise sensitive data.

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to acquiring a direct interest in .au Domain Administration Ltd (ABN 38 079 009 340).

### **Commercial construction contractors**

Construction firms often hold contracts with government agencies and critical infrastructure service providers. Commercial construction firms which develop assets for sensitive clients typically have the ability to select sub-contractors and other suppliers and may have access to sensitive information, through building blueprints or building information management systems. Such information may be of value to foreign intelligence services. Foreign intelligence services may also pre-position for future intelligence activities – such as by building surveillance equipment into the premises during construction to gather information on intended sensitive tenants.

#### *Mandatory notification obligations (notifiable national security actions)*

There are generally no notifiable national security actions. However, some investments in this sector may be notifiable actions under the broader national interest test. See the *Overview Guidance Note* for more information.

#### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity which holds contracts to construct buildings which will house the following types of tenants are encouraged to notify:

- Commonwealth, state or territory governments (except where the contract includes information with a security classification, in which case it may be subject to [mandatory notification](#)); or
- local governments in metropolitan areas; or
- critical infrastructure assets as defined by the *Security of Critical Infrastructure Act 2018*.

### **Commercial real estate**

Commercial buildings may house government or critical infrastructure tenants from across multiple sectors, which hold sensitive data that may be of interest to foreign intelligence services. Foreign ownership of such commercial buildings may provide vectors through which foreign intelligence services may gain access to tenants' offices and work areas, giving rise to potential espionage risks.

### *Mandatory notification obligations (notifiable national security actions)*

There are generally no notifiable national security actions (except if Defence or an agency in the NIC has an interest in the target of the acquisition). However, some investments in this sector may be notifiable actions under the broader national interest test. See the *Overview* Guidance Note for more information.

### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in commercial real estate with Commonwealth, state or territory government, or local government (metropolitan areas only) tenants, or critical infrastructure asset (as defined by the *Security of Critical Infrastructure Act 2018*) tenants, where the foreign person will be involved in the day-to-day management of the building, are encouraged to voluntarily notify.

### **Critical minerals**

Technological change has been driving global demand for critical minerals which due to their unique catalytic, metallurgical, nuclear, electrical, magnetic, and luminescent properties, are increasingly used in the manufacture of mobile phones and computers, wind turbines, electric cars, solar panels, batteries, defence industry products and technologies, and many other high-tech applications. The scarcity and geographical concentration of some critical minerals leaves them potentially vulnerable to supply chain manipulation and disruptions for strategic gain that could cause long-term harm to national security.

### *Mandatory notification obligations (notifiable national security actions)*

There are generally no notifiable national security actions. However, there would be relatively few circumstances in which the national interest test would not apply. See the *Overview* Guidance Note for more information.

### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity involved in the extraction, processing or sale of the following minerals are encouraged to seek foreign investment approval:

- Rare Earth Elements
- Lithium
- Graphite
- Cobalt
- Vanadium
- Copper
- Nickel
- Silicon
- High-Purity Alumina

### Critical service providers and suppliers

Service providers can be key components in the supply chain for essential goods and services that Australians rely on. The access and control afforded by foreign investment may create opportunities for foreign actors to harm national security. Critical service providers and suppliers may have significant access to, or operational control over, sensitive government or critical infrastructure assets—including key components that relate to their function as a critical asset. This introduces national security risk through the potential disruption or denial of service, or access to information that may be of value to foreign intelligence services or be used to support foreign interference activity.

#### *Mandatory notification obligations (notifiable national security actions)*

There are generally no notifiable national security actions. However, some investments in this sector may be notifiable actions under the broader national interest test. See the *Overview Guidance Note* for more information.

#### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity with the following criteria are encouraged to seek foreign investment approval:

- The business provides services to:
  - Commonwealth, state or territory governments; or
  - local governments in metropolitan areas; or
  - critical infrastructure assets as defined by the *Security of Critical Infrastructure Act 2018*; or
  - more than five businesses in a critical infrastructure sector as defined by the *Security of Critical Infrastructure Act 2018*;

AND

- Their contractual arrangements involve at least one of the following criteria:
  - Provision of security or incident planning services of any kind;
  - Unescorted physical access to restricted areas;
  - Privileged access into digital networks;
  - Access to sensitive data owned or managed by the client entity. Sensitive data comprises sensitive network and operational data or [sensitive personal information](#) or any non-public data collected by or on behalf of the Commonwealth in relation to more than 100,000 residents;
  - Operational control of any aspect of a government client's business;
  - Operational control of a critical infrastructure client's business that is directly related to its function as part of a critical infrastructure sector (as defined in the *Security of Critical Infrastructure Act 2018*);

- Supply of services, components or inputs to a critical infrastructure asset that is essential to their ability to operate their asset (as defined in the *Security of Critical Infrastructure Act 2018*); or
- Telecommunications suppliers and service providers, for example, systems integrators, managed service providers and entities that provide support functionality, build or maintain telecommunications networks.

### Critical Technologies

Critical technologies are current and emerging technologies that have the capacity to significantly enhance or pose risk to our national interest. They are fundamental to Australia's economic prosperity, social cohesion, and national security, and are increasingly the focus of international geopolitical competition. Critical technologies can be digital or non-digital.

Critical technologies confer a strategic edge, and because of this they may be the target of malicious activity, including foreign interference, espionage, and sabotage.

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting, or acquiring a direct interest in, a business that develops, manufactures or supplies critical technology that is, or is intended to be, for a military use, or an intelligence use, by defence and intelligence personnel, the defence force of another country, or a foreign intelligence agency (see table on pages 22-24).

#### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity that is otherwise not captured by the mandatory notification requirements are encouraged to seek foreign investment approval if the business or entity develops, manufactures, or supplies any of the following critical technologies:

- Advanced data analytics
- Advanced optical communications
- Advanced radiofrequency communications (including 5G and 6G)
- Advanced robotics
- Artificial intelligence (AI) algorithms and hardware accelerators
- Autonomous systems operation technology
- Drones, swarming and collaborative robots
- Genetic engineering
- High performance computing
- Machine learning (including neural networks and deep learning)
- Natural language processing (including speech and text recognition and analysis)

- Novel metamaterials
- Photonic sensors
- Protective cyber security technologies
- Quantum communications (including quantum key distribution)
- Quantum computing
- Quantum sensors
- Satellite positioning and navigation

These technologies are drawn from the *List of Critical Technologies in the National Interest*, which features descriptions of each of the technologies and is available [here](#).

**Example 12**

David is a foreign person looking to start a medical technology company in Australia. David's company would develop artificial intelligence and machine learning systems, specifically targeted at image classification algorithms for medical image analysis. David does not intend for these products to be for a military or intelligence use. While artificial intelligence (including machine learning) is considered to be critical by Defence, as David is not intending for it to have a military or intelligence use, his proposed business would not meet the thresholds defined in legislation for a national security business. However, given the status of machine learning as a critical technology, David is encouraged to voluntarily notify the proposed transaction.

**Defence Providers**

Defence providers play a critical role in ensuring Defence is appropriately equipped to protect Australia's national security. Given this criticality, some of these providers may be a target for malicious activity for foreign interference, espionage and sabotage. The Australian Government seeks to oversee foreign investment in critical goods, technology, and services that has the capacity to significantly enhance or pose a risk to national security, and to which the Australian Government needs to:

- ensure ongoing access due to the highly essential nature to Defence's capability advantage; and/or
- limit others' access due to the highly sensitive nature which could adversely impact upon Defence interests.

***Mandatory notification obligations (notifiable national security actions)***

Foreign persons must seek foreign investment approval prior to starting, or acquiring a direct interest in, a business that develops, manufactures, or supplies critical goods or technology, for or intended for, a military end-use by Defence or the defence force of another country. Foreign persons must also seek foreign investment approval prior to starting, or acquiring a direct interest in a business that provides, or intends to provide, critical services to Defence or the defence force of another country.

For the avoidance of doubt, a critical defence industry asset as defined by the *Security of Critical Infrastructure Act 2018* is intended to be a sub-set of the definitions in the preceding paragraph.

#### **What is a ‘critical’ good, technology or service for Defence or intelligence purposes?**

For foreign investment purposes, goods, technology, and services that are ‘critical’ must be vital to advancing or enhancing Australia’s national security and could be detrimental to Australia’s national security if not available or if misused. This includes goods, technologies, and services to which ongoing access is essential to the capability advantage of Defence and agencies in the NIC.

‘Critical’ does not include businesses that provide goods, technologies and services that are generic or widely available for a range of inputs.

- For example, generic goods, technology, and services such as cleaning, furniture, stationery and catering would not be considered critical.
- Widely available goods, technologies, or services – such as certain minerals or commodities, and other off-the-shelf non-military specific goods would not be considered critical, notwithstanding that it may be used as an input to another good, technology or service that is critical.

#### **What is covered?**

‘Develops’, ‘manufactures’, or ‘supplies’ is intended to cover the entire lifecycle of a good or technology from initial idea generation and design, through testing and development, to production and supply to the final user. Follow-up repairs and services would also be included, particularly where those services are carried out regularly and the persons carrying out those services have developed a familiarity with the goods and their experience and knowledge have national security value themselves.

The list below is a non-exhaustive and indicative list based upon existing publicly available Defence documents, such as the areas identified by the [Next Generation Technologies Fund](#), the [Defence Innovation Hub](#) priorities, and the [Defence Industrial Capability Plan](#).

| <b>Indicative Sectors</b>                        | <b>Non-exhaustive examples</b>  |
|--|---|
| Protection systems for vehicles for military use | Technology underpinned by automation, autonomy and autonomous systems, disruption technologies, infrared, thermal imaging, and image intensifier equipment.   |
| Protection systems for individual soldiers       | Combat clothing survivability signature management and disruption technologies, military personal protective equipment, armour plate, body armour, helmets and components, infrared, thermal imaging and image intensifier equipment. |
| Land vehicles for military use                   | Maintenance, technology upgrades, disruption technologies, armour plate, infrared, thermal imaging and imaging intensifier equipment, and weapons.  |
| Aircraft for military use                        | Hypersonic weapons and aircraft, fighter aircraft, strike and air combat capabilities, bombers, manned and autonomous   |

| Indicative Sectors   | Non-exhaustive examples  |
|--|--|
|  | or remotely piloted aircraft, stealth technologies, and advanced air and sea lift technologies.  |
| Watercraft for military use  | Next-generation position, navigation, timing technologies, submarine and other submersible vessels and related articles, shipbuilding, maintenance, and technology upgrades, and maritime and anti-submarine warfare.  |
| Signal processing, electronic warfare, cyber and information security for military use | Intelligence collection, analysis, communications, navigation, targeting and surveillance, reconnaissance, electronic warfare technologies, and command and control systems.   |
| Communications and sensing for military use  | Active and passive military radar systems, (such as phased array radar, high frequency skywave radar, active electronically scanned array radar), underwater acoustics, signature reduction, non-acoustic signature reduction, electronic warfare, electronic countermeasures and surveillance, ultra wide band tactical mesh, laser communications, photonics, adaptive optics, and cognitive networking. |
| Material sciences and advanced manufacturing for military use                          | Additive manufacturing, armour and explosives, nanomaterials/nanotechnology, adaptive camouflage, functional textiles, biomaterials, bio-composites, and thermal barrier coatings, and high-specification machining processes.   |
| Artificial intelligence and robotics for military use                                  | Autonomous cyber operations, machine learning, trusted autonomous systems, artificial intelligence cloud technologies, micro-drone and micro-robotics, swarming technology, molecular robotics, self-assembly robots, and smart dust.  |
| Biotechnologies for military use   | Medical countermeasure products, enhancements to the physical and cognitive capability and capacity of personnel, brain-computer interfaces.   |
| Directed energy capabilities for military use  | Directed energy weapons, energy management and resilience, laser and particle beam systems and countermeasures for military use.   |
| Space capabilities for military use  | Satellite systems, space launch vehicles, rocket technology, and next-generation position, navigation, and timing technologies.  |

| Indicative Sectors   | Non-exhaustive examples   |
|--|---|
| Quantum technologies for military use  | Quantum computing, quantum sensing, quantum encryption, and quantum communications and technologies.  |
| Toxic chemicals, biological agents, and radioactive materials for military use | Chemical or biological toxic agents, radioactive materials, and related equipment, components and materials.  |
| Weapons and weapon systems for military use                                    | High velocity kinetic energy weapon systems and related equipment and ammunition, and smooth bore weapon components and accessories.  |
| Munitions for military use   | Bombs, torpedoes, rockets, missiles, other military explosive devices and charges, components and accessories, equipment for launching, deploying, decoying, disruption, detection, and jamming.  |
| Other  | Any business that receives innovation, research, or development funding from Defence or NIC agencies in Australia or from equivalent agencies overseas, and any business that produces goods, technology, or services for military use that are subject to export controls. |

### *Voluntary notification*

Foreign investors proposing to undertake a reviewable national security action by investing in businesses or entities with a contractual relationship with Defence which are otherwise not captured by the mandatory notification requirements in the following sectors are encouraged to seek foreign investment approval:

- Telecommunications, information, communications or technology (ICT), and data;
- Electricity (including renewable energy), gas and water;
- Ports and airports;
- Health;
- Building maintenance;
- Construction;
- Transport and logistics;
- Education and training;
- Space industry, or science and technology businesses; and
- Defence industry (including subcontractors in the Defence contractor's supply chain).

## Energy

The Australian energy sector provides an essential service that Australians rely on for their well-being, and the ongoing availability of energy is essential to maintain Australia's national security. The access and control afforded by foreign investment in the energy sector may create opportunities for foreign actors to harm national security. If the energy sector was impacted by a significant disruption, through sabotage or foreign interference activity, it would lead to cascading consequences for a range of other sectors, significantly impacting Australia's economy, society and security.

## Electricity

Electricity is fundamental to modern society. A prolonged disruption to the production, distribution or supply of electricity would have a significant impact on individuals, communities, businesses and national security capabilities. Some electricity providers also hold large data sets about customers and their electricity usage, which need to be appropriately protected from espionage and foreign interference.

### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business, or acquiring a direct interest in an entity that owns or operates a:

- network, system or interconnector for the transmission or distribution of electricity to ultimately service at least 100,000 customers; or
- an electricity generation station that provides a system restart ancillary service in a state or territory; or has a nameplate generation capacity that is greater than or equal to 30 megawatts (MW); and is connected to a wholesale electricity market.

For foreign investment purposes, the point at which a project in the National Electricity Market (NEM) is considered to be connected to a wholesale electricity market is once the electricity generation station is considered to be an 'existing plant' by the Australian Energy Market Operator (AEMO) and has a commitment status of 'In Service'.

### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in an energy retailer (gas or electricity) where the foreign person would subsequently hold interests in energy retailers with more than 100,000 customers are encouraged to seek foreign investment approval.

## Gas

Gas is an important energy source for Australian households and businesses. A prolonged disruption to Australia's gas networks would have a significant impact on individuals, communities, businesses, and national security capabilities.

### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business, or acquiring a direct interest in an entity that owns or operates:

- a processing facility with a capacity of at least 300 terajoules per day;

- a storage facility with a maximum daily withdrawal capacity of at least 75 terajoules per day;
- a distribution network or system ultimately servicing 100,000 customers;
- any of the following gas transmission pipelines at the prescribed nameplate rating (including a control room, or any other asset that is required to operate any of them):

| Pipeline                                   | Nameplate rating       |
|--|------------------------|
| Eastern gas market transmission pipelines  | 200 terajoules per day |
| Northern gas market transmission pipelines | 80 terajoules per day  |
| Western gas market transmission pipeline   | 150 terajoules per day |
| Tasmanian gas pipeline                     | N/A                    |
| Carpentaria gas transmission pipeline      | N/A                    |

### *Voluntary notification*

Some gas providers also hold large data sets about customers and their gas usage which need to be appropriately protected. As suggested above, foreign persons proposing to undertake a reviewable national security action by investing in an energy retailer (gas or electricity) where the foreign person would subsequently hold interests in energy retailers with more than 100,000 customers are also encouraged to seek foreign investment approval. Foreign persons proposing to undertake a reviewable national security action by investing in suppliers of smart meters are also encouraged to seek foreign investment approval.

### **Liquid fuels**

Liquid fuels (including crude oil and condensate, petrol, diesel and jet fuels) are essential to Australia's energy security. A compromise or prolonged disruption to Australia's liquid fuel sector would have a significant impact on individuals, communities, businesses and national security capabilities.

### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business or acquiring a direct interest in an entity that owns or operates:

- a liquid fuel storage facility that has a storage capacity of more than 50 megalitres; or
- the liquid fuel refinery at Corio, Victoria, or the liquid fuel refinery at Lytton, Queensland; or
- the Sydney Metropolitan Pipeline, Gore Bay Pipeline, Westernport Altona Geelong Pipeline, or Longford (Dutson) to Hastings Pipeline; or
- Melbourne Airport Jet Fuel Pipelines, Jet Fuel Pipeline (Kurnell to Sydney Airport), Brisbane Airport Jet Fuel Pipeline or Perth Airport Jet Fuel Pipeline.

## Energy Market Operators

Energy market operators play a critical role in maintaining the security of supply and the efficient operation of gas and electricity systems. A disruption to Australia's key market operators would have a significant and widespread impact on individuals, communities, businesses and national security capabilities.

### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to acquiring a direct interest in the following energy market or system operators that is essential to ensuring the security and reliability of an energy market:

- the Australian Energy Market Operator Limited (AEMO); Power and Water Corporation; Regional Power Corporation (Horizon Power - ABN 57 955 011 697); and Electricity Networks Corporation (Western Power- ABN 18540492861).

The focus is on assets that are essential to a market operator undertaking its statutory functions, for example managing market trading and ensuring the security and reliability of the physical infrastructure. Although Western Power's primary function is as a transmission and distribution network operator, it has been included as it undertakes market operator functions within this meaning.

## Food and Grocery

The COVID-19 pandemic has placed food and grocery distribution and supply under significant pressure, revealing both the criticality and vulnerability of these networks. The key retailers and wholesalers listed below collectively account for over 80 per cent market share, and if disrupted, could have a severe and widespread impact on the availability of food and grocery.

### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to acquiring a direct interest in the following entities or their subsidiaries:

- Aldi Pty Ltd (ABN 68 086 493 950);
- Coles Group Limited (ABN 11 004 089 936);
- Woolworths Group Limited (ABN 88 000 014 675); or
- MetCash Trading Limited (ABN 61 000 031 569).

## Health

The health sector provides essential goods and services that all Australians rely on – this has been brought into sharp focus during the COVID-19 pandemic. The health sector also undertakes critical medical research, clinical trials and health technology development and holds significant amounts of sensitive Australian patient data. National security risks could arise through a widespread failure or disruption, which may have a significant impact on individuals, communities and the economy, or large-scale collection of health-related patient or research data for malicious purposes or strategic gain.

### **Health sector facilities and services**

Health sector facilities and services provide essential health services to Australians. National security risks may arise due to sabotage or espionage risks. The health sector is a major aggregator of sensitive personal information which may have value to foreign intelligence services.

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business, or acquiring a direct interest in an entity that owns or operates a hospital that has a general intensive care unit.

#### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a hospital without a general intensive care unit, general and specialist practice, diagnostic and treatment facility (for example, radiology and oncology) or pathology provider that would result in the applicant holding sensitive personal information relating to greater than 100,000 individuals are encouraged to seek foreign investment approval.

### **Medicines and medical devices**

Medicines and medical devices are critical inputs to the operation of the health system and for health-care for all Australians. National security risks may arise through malicious actors denying the supply of medicines or medical devices. In addition, manufacturers of such products may have access to large quantities of sensitive biomedical information which may be valuable to foreign intelligence services.

#### *Mandatory notification obligations (notifiable national security actions)*

There are generally no notifiable national security actions. However, some investments in this sector may be notifiable actions under the broader national interest test. See the *Overview Guidance Note* for more information.

#### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity that manufactures essential medicines or medical devices are encouraged to seek foreign investment approval.

- Essential medicines include those that are listed in the Pharmaceutical Benefits Scheme.
- Essential medical devices include the manufacture of personal protective equipment and diagnostic equipment, pacemakers and prosthetics.

### **Higher education facilities**

Universities are responsible for a significant portion of critical research and innovation activities in Australia so maintaining the security and stability of Australian universities is important. The higher education sector is a major source of information of critical research and innovation in all fields which may have value to foreign intelligence services. Australian universities may also be targets for espionage, sabotage and foreign interference.

*Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business or acquiring a direct interest in an entity that is:

- registered in the Australian university category on the National Register of Higher Education Providers, including the Australian National University; and
- Is used in connection with undertaking a program of research that is critical to a critical infrastructure asset (other than the higher education and the research sector), the defence of Australia or national security.

**Information technology, data and the cloud**

Information technology (IT), data and cloud services underpin a broad range of economic and social activity and are fundamental inputs to other sectors, including the provision of essential services and critical infrastructure. Australia's economic prosperity and national security is increasingly dependent on safe and secure IT, data and cloud services.

The access and control afforded by foreign investment in the IT, data and cloud sector may create opportunities for foreign actors to harm national security. Foreign intelligence services seek to exploit Australia's businesses for intelligence purposes, including industries that hold a large amount of personal data that that could provide an economic or strategic edge.

**Data centres and cloud providers**

Data centres and cloud providers are critical to maintaining the supply and availability of data and cloud services in Australia. These services offer large economic and social benefits and are critical for business continuity, but the widespread use of these services also introduces data security risks. Sensitive data and personal information is a target for espionage, sabotage and foreign interference activity.

*Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business or acquiring a direct interest in a data centre or cloud provider that stores or has access to information that has a security classification, or stores or processes business critical data for the Commonwealth, a state or territory government, or an entity responsible for a critical infrastructure asset (as defined by the *Security of Critical Infrastructure Act 2018*).

For the purposes of administering the foreign investment framework, storing or processing data means acquiring or managing the computing infrastructure required for providing storage and processing services, running the storage or processing software that provides the services, and makes arrangements to deliver the storage or processing services to consumers through network access. A data service means a service that enables end-users to store or back-up data and is provided on a commercial basis. Data processing means the use of one or more computers and is provided on a commercial basis.

*Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by acquiring an interest in land to establish a data centre, where it is otherwise not captured by the mandatory notification requirements, are encouraged to seek foreign investment approval.

### ***Sensitive personal information***

Data is a national asset in need of appropriate and proportionate protections. The volume, sensitivity and value of data held by the Australian Government and industry, including critical infrastructure entities, has increased exponentially over recent years and is likely to grow. Bulk sensitive data and personal information can be stolen, manipulated or fabricated to achieve a purpose which is in the interest of a foreign actor.

Bulk data sets often contain detailed information about a large volume of individuals that could be used by foreign intelligence services (or other malicious parties) to assist in identifying people that could be coerced or bribed to perform certain actions that may be contrary to Australia's national security, or assist in monitoring people of interest. This information could identify particular vulnerabilities in a person's life, such as financial debts, medical conditions or compromising circumstances. Larger data sets or those aggregated across multiple sources are more likely to contain information about individuals who could be targeted and provide greater visibility of a given individual's behaviour.

### ***Mandatory notification obligations (notifiable national security actions)***

A foreign person must seek foreign investment approval prior to starting a business or acquiring a direct interest in an entity that stores, maintains, or has access to personal information, collected by the ADF, Defence or an agency in the NIC, which if disclosed, could compromise Australia's national security. This includes information that is not necessarily classified information, but that could pose a national security risk, if, for example, it could be used to influence the personnel or derive an advantage from knowing aggregate statistics about the defence force or intelligence community.

### ***Voluntary notification***

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity that has access to bulk sensitive personal information of over 100,000 Australian residents are encouraged to seek foreign investment approval. Sensitive personal information includes but is not limited to:

- Medical/psychological information;
- Psychometric and profiling information;
- Individuals' financial information, including debts; and
- Genetic information.

### ***Access to sensitive network or operational information***

Sensitive network or operational information is valuable for foreign intelligence services – particularly as it relates to government information or that of critical infrastructure operators. Access to this information could facilitate acts of espionage, sabotage and foreign interference that could have significant impacts on Australia's national security – for example through denial of service, including across multiple critical infrastructure operators (where information is aggregated).

### *Mandatory notification obligations (notifiable national security actions)*

There are generally no notifiable national security actions. However, some investments in this sector may be notifiable actions under the broader national interest test. See the *Overview Guidance Note* for more information.

### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity that has access to sensitive network or operational information in relation to a Commonwealth or state or territory government entity, a critical infrastructure asset (as defined by the *Security of Critical Infrastructure Act 2018*) or more than five businesses in the water, energy, telecommunications, banking and finance, space and hospital sectors are encouraged to seek foreign investment approval.

Sensitive network or operational information includes:

- Security arrangements, physical security, IT security and incident management. This includes passwords and access credentials.
- Network architecture, layout of physical facilities or configuration of equipment specific to the critical infrastructure entity.

### **Nuclear**

Australia has around one third of the world's uranium resources and is the world's third largest producer of uranium ore concentrate (UOC). All Australian uranium is exported for conversion, enrichment, fuel fabrication and civilian use within our network of nuclear cooperation agreements. Uranium is used both for civilian nuclear reactor fuel as well as other purposes including as source material for nuclear medicine production. The access and control afforded by foreign investment in the nuclear sector may create opportunities for foreign actors to harm national security. Without proper controls (for example, nuclear safeguards) enriched uranium used in the civilian sector could also be further enriched for use in nuclear weapons or used to generate plutonium (in a reactor) for such weapons. Sabotage of a nuclear-related facility or process could both cause immediate harm, undermine the public's confidence in Australia's nuclear industry and damage nuclear-related cooperation with international defence partners key for protecting national security.

### *Mandatory notification obligations (notifiable national security actions)*

There are generally no notifiable national security actions. However, there would be relatively few circumstances in which the national interest test would not apply. See the *Overview Guidance Note* for more information.

### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity involved in, the extraction, processing or sale of uranium or plutonium are encouraged to seek foreign investment approval. Similarly, foreign persons proposing to invest in a business or entity that owns or operates a nuclear facility are encouraged to seek foreign investment approval.

## Space

Space technologies and services provide vital inputs to virtually every sector of the Australian economy, everyday life, critical infrastructure and essential services. A significant disruption of these services could have profound impacts on national security. Access to sensitive technology and information would be valuable to foreign intelligence services.

### *Mandatory notification obligations (notifiable national security actions)*

There are generally no notifiable national security actions. However, some investments in this sector may be notifiable actions under the broader national interest test. See the *Overview Guidance Note* for more information.

### *Voluntary notification*

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity that operates a satellite ground station, launch facility, or land to build these assets, or invest in a business or entity involved in the development of space technology and missions are encouraged to seek foreign investment approval.

## Transport

Australia's geographic spread means the reliable and efficient transport of goods and passengers across regions is essential. The access and control afforded by foreign investment in the transport sector may create opportunities for foreign actors to harm national security.

## Ports

Ports support the supply of liquid fuels, the supply chains for other critical infrastructure, and Defence purposes. Compromise, control over or disruption to Australia's critical ports could have wide-reaching national security impacts.

### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to acquiring a direct interest in an entity that owns or operates one or more of the 20 maritime ports listed under section 11 of the *Security of Critical Infrastructure Act 2018*.

### *Voluntary notification*

In addition to the 20 ports listed in the *Security of Critical Infrastructure Act 2018*, the Government regulates another 57 ports under the *Maritime Transport and Offshore Facilities Security Act 2003*. This Act establishes a regulatory regime to ensure the security of maritime ports and shipping within Australian waters.

Foreign persons proposing to undertake a reviewable national security action by investing in a business or entity that owns or operates one or more of the 57 additional prescribed ports (that is, those not listed in the *Security of Critical Infrastructure Act 2018*) under the *Maritime Transport and Offshore Facilities Security Act 2003* are encouraged to seek foreign investment approval.

## Aviation

An efficient, safe, and secure aviation system is integral to Australia's social and economic well-being—the disruption of which would be of significant consequence to national security.

Those parts of the aviation industry and the air cargo supply chain that require protection against national security threats are identified through the regulatory framework set out in the *Aviation Transport Security Act 2004*.

*Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business or acquiring a direct interest in an entity that is:

- an airport or airport operator as defined by the *Aviation Transport Security Act 2004*;
- an aircraft operator used in connection with the provision of an air service as defined by the *Aviation Transport Security Act 2004*; or
- a regulated air cargo agent used in connection with the provision of an air service as defined by the *Aviation Transport Security Act 2004*.

For the purposes of administering the foreign investment framework, an airport refers to a designated airport in regulation 1.03 of the *Aviation Transport Security Regulations 2005*. An air service refers to screened air services that depart from a designated airport. A regulated air cargo agent refers to a regulated air cargo agent that is also a cargo terminal operator at a designated airport.

**Freight Services**

*Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business or acquiring a direct interest in an entity that has an annual revenue of at least \$150 million and provides a road freight transport service, a freight forwarding service, a rail freight transport service or a water freight service and the freight service provided by the business involves the transport or storage of any of the following:

- food and groceries, where transported to or from Aldi, Coles, Metcash or Woolworths;
- therapeutic goods registered on the Australian Register of Therapeutic Goods moved to or from premises storing such goods;
- the supply of medicines listed under Schedules 2, 3, 4 or 8 of Part 4 of the current Poisons Standard, where transported to or from a premises at which the manufacture of the medicine is permitted under a law of a State or Territory;
- liquid fuel, where transported to or from a critical liquid fuel asset as defined in the *Security of Critical Infrastructure Act 2018*;
- essential goods and supplies required for water treatment facilities; or
- any other good that is critical for the operation, maintenance or management of a critical infrastructure asset as defined in the *Security of Critical Infrastructure Act 2018*.

### Freight Infrastructure

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to acquiring a direct interest in an entity that owns or operates one or more of the 14 intermodal terminals listed in the table in Schedule 1 to the *Security of Critical Infrastructure (Definitions) Rules 2021* (below) and is critical to the transportation of goods between 2 States, a State and Territory, 2 Territories or 2 regional centres.

| Intermodal Terminal       | Location | Jurisdiction | Locality Terminal Operator                         |
|---------------------------|----------|--------------|--|
| <b>Chullora</b>           | NSW      | Metropolitan | PacificNational                                    |
| <b>Parkes</b>             | NSW      | Regional     | PacificNational and SCT Logistics                  |
| <b>Townsville</b>         | QLD      | Metropolitan | Linfox   |
| <b>Acacia Ridge</b>       | QLD      | Metropolitan | PacificNational                                    |
| <b>Bromelton</b>          | QLD      | Metropolitan | SCT Logistics                                      |
| <b>Islington</b>          | SA       | Metropolitan | PacificNational                                    |
| <b>Penfield</b>           | SA       | Metropolitan | SCT Logistics                                      |
| <b>Brighton Transport</b> | TAS      | Metropolitan | TasRail and IPEC Pty Ltd                           |
| <b>Dynon-North</b>        | VIC      | Metropolitan | QUBE Logistics and Victorian Rail Track (VicTrack) |
| <b>Dynon-South</b>        | VIC      | Metropolitan | PacificNational                                    |
| <b>Altona</b>             | VIC      | Metropolitan | SCT Logistics                                      |
| <b>Barnawartha</b>        | VIC      | Regional     | SCT Logistics                                      |
| <b>Forrestfield</b>       | WA       | Regional     | SCT Logistics                                      |
| <b>Kewdale-Welshpool</b>  | WA       | Metropolitan | PacificNational                                    |

### Public transport

Large and connected public transport networks (including passenger rail, light rail, buses and ferries) are critical to the functioning of Australia's economy, and any malicious disruption of these networks would have a consequential impact on national security. Some public transport providers also hold large data sets relating to their customers; including billing information and their public transport usage, which also need to be appropriately protected from espionage and foreign interference.

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business or acquiring a direct interest in an entity that owns or operates a public transport network or system that is

managed by a single entity and is capable of handling at least 5 million passenger journeys per month.

### **Water and sewerage**

A clean and reliable supply of water is essential to all Australians, and many of our critical infrastructure sectors and businesses. The access and control afforded by foreign investment in the water and sewerage sector may create opportunities for foreign actors to harm national security. A compromise or disruption to Australia's water supply or water treatment facilities, through foreign interference or sabotage, would have major health consequences and significantly impact businesses that rely on water. Critical infrastructure interdependencies which for water includes but is not limited to data centres, electricity generation stations, hospitals, military facilities and telecommunications infrastructure.

#### *Mandatory notification obligations (notifiable national security actions)*

A foreign person must seek foreign investment approval prior to starting a business, or acquiring a direct interest in an entity that owns or operates a water or sewerage system or network that ultimately delivers services to at least 100,000 water connections or 100,000 sewerage connections.

### **FURTHER INFORMATION**

Further information is available on the [FIRB website](#) or by contacting 1800 050 377 from Australia or +61 2 6216 1111 from overseas.

**Important notice:** This Guidance Note provides a summary of the relevant law. As this Guidance Note tries to avoid legal language wherever possible it may include some generalisations about the law. Some provisions of the law referred to have exceptions or important qualifications, not all of which may be described here. The Commonwealth does not guarantee the accuracy, currency or completeness of any information contained in this document and will not accept responsibility for any loss caused by reliance on it. Your particular circumstances must be taken into account when determining how the law applies to you. This Guidance Note is therefore not a substitute for obtaining your own legal advice.