NATIONAL SECURITY TEST

Last updated: 17 December 2020. This is a new guidance note introduced to help understand the new legislation that commences on 1 January 2021.

- Foreign investment is important for Australia's long term economic success, stability and prosperity. It creates jobs, improves productivity, enables the transfer of new technologies and connects Australian businesses to global supply chains.
- Foreign investment supports:
  - employment (one in ten jobs[1] are created by foreign businesses);
  - the national economy (businesses supported by foreign investment contribute more than a quarter of Industry Value Added); and
  - higher wages (foreign businesses pay wages that are on average $20,000 a year higher).
- Australia welcomes foreign investment – the overwhelming majority of investment is approved. A strong and secure economy creates a positive investment environment that ensures Australia 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.
- This guidance is intended to uphold our national interest, including through:
  - safeguarding national security and sovereignty;
  - upholding Australia's international reputation and relationships;
  - preventing economic damage; and
  - safeguarding critical infrastructure.
- The national security test provides the Treasurer with the ability to address new and emerging national security risks from foreign investment.
  - Actions that trigger mandatory national security notification requirements are, by their nature, likely to give rise to a national security concerns that, regardless of their size or value, require review by the Treasurer.

1 ABS cat. no.5494.0 — Economic Activity of Foreign Owned Businesses in Australia, 2014-15.

- However, there are some actions that, while not mandatory to notify, may still pose national security concerns. The Treasurer's 'call-in' power provides additional scrutiny over those investment proposals, without imposing a disproportionate regulatory burden on non-sensitive investments. Foreign investors can extinguish the Treasurer's ability to use the call-in power by voluntarily notifying of an action.
- The last resort power gives the Treasurer an opportunity to review actions notified after 1 January 2021 for which a no objections notification has been given, if exceptional circumstances arise.

Looking for more?

A: NATIONAL SECURITY TEST

The national security test:

- requires mandatory notification of proposed investments in national security land, interests in exploration tenements over national security land, a proposed direct investment in a national security business or starting a new national security business;
- allows investments that are not 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).

In order 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 nominated carriage service provider 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 (subject to a $0 threshold and the national interest test). In the same application, OPF is also required to notify a proposed acquisition of a national security business (subject to a $0 threshold and the national security test). As the proposed investment is caught by both the national interest test and national security test, it will be considered against the national interest (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 upon 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 is publicly known, or could be known upon the making of reasonable inquiries.

National security 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 a responsible entity (within the meaning of the *Security of Critical Infrastructure Act 2018* as enacted) 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* as enacted); 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;
- provides, or intends to provide, critical services to defence and intelligence personnel, the defence force of another country, or a foreign intelligence agency;
- stores or has access to information that has a security classification;
- stores or maintains personal information of defence and intelligence personnel collected by the Australian Defence Force, the Defence Department or an agency in the national intelligence community which, if accessed, could compromise Australia's national security;
- collects, as part of an arrangement with the Australian Defence Force, the Defence Department or an agency in the national intelligence community, 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 which, if disclosed, could compromise Australia's national security.

What is 'critical'?

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 national intelligence community.

'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, services and technology 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.

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 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 Australian Defence Force, the Department of Defence or an agency in the national intelligence community, 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 defence force or the intelligence community. 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 national intelligence community, 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 Protective Security Policy Framework, 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 Defence force and intelligence community. However, the fashion outlet would not be considered a national security business because while collecting information about members of the Defence and intelligence community, the information is not in connection to their work nor collected because of where they work.

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, 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 national intelligence community has an interest, if the existence of the interest is publicly known or could be known upon the making of reasonable inquiries.

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.

Starting a national security business

A foreign person must notify and seek foreign investment approval if the foreign person starts 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 circumstances in each case. If a business activity is sufficiently different from activities already carried out, it is likely to be considered to be starting a national security business.

Example 4

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 5

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.

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

The Treasurer can 'call-in' for review, 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.

Once called in, an investment will be reviewed under the national security test 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. For the types of actions that may constitute a reviewable national security action see Division 4B of the *Foreign Acquisitions and Takeovers Act 1975*. 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 power.

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.

For further information, see the *Exemption Certificate* Guidance Note.

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 objections 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 the Treasurer was notified of the action after 1 January 2021, 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 national intelligence community, takes reasonable steps to negotiate in good faith with the foreign person, and is satisfied that exercising those powers 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 whole of an action. This includes, as a last resort, requiring divestment.

F: SECTORAL GUIDANCE

Investors are encouraged to carefully consider whether the type of action that is being proposed would be a notifiable national security action or a reviewable national security action. 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 *Foreign Acquisitions and Takeovers Act 1975* 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 such as the *Security of Critical Infrastructure Act 2018*. The Security Legislation Amendment (Critical Infrastructure) Bill 2020 that is currently before Parliament will, if passed, result in additional investments becoming subject to mandatory notification.

The sectoral guidance should not be understood as an exhaustive indication of those investments that may be the subject of the call-in powers. The Treasurer retains the ability to exercise the call-in power 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 call-in power will be exercised by reference to the particular circumstances of each case and the existence of national security concerns.

Banking and Finance

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

Mandatory notification obligations

Nil 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 invest in the following banking and finance businesses or entities are encouraged to seek foreign investment approval:

- Banks, credit unions, building societies and other authorised deposit-taking institutions: Businesses that own or operate an authorised deposit-taking institution with total entities above $50 billion total and critical to the carrying on of banking business by the authorised deposit-taking institution.
- Superannuation: Businesses that own or operate and are critical to the operation of, a registrable superannuation entity with entities under management of $20 billion or more.
- Insurance: Businesses that own or operate, and critical to the operation of, a general insurance business with entities greater than $2 billion, a life insurance business with entities greater than $5 billion, or a health insurance business with entities greater than $0.5 billion.

- Financial markets: Businesses that own or operate the holder of an Australian market licence that is incorporated in Australia or a related body corporate of that licence holder, and is critical to the operation of a domestic financial market.

- Clearing and settlement facilities: Businesses 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 and is critical to the operation of a clearing and settlement facility.

- Payment systems as defined in the *Payment Systems (Regulation) Act 1998*. Businesses that operate an entity that is critical to the operation of a critical payment system. A critical payment system is critical to ensuring the security and reliability of the financial system.

- Derivative trade repositories: Business that own or operate entities that hold an Australian derivative trade repository licence where the holder is incorporated in Australia or a related body corporate of that holder; and is critical to the operation of the derivative trade repository operated by the holder of the licence.

- Benchmark administrators: Businesses that are owned or operated by the holder of a benchmark administrator licence that is incorporated in Australia or a related body corporate of that licence holder and is critical to the administration of a financial benchmark.

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. 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

A foreign person must seek foreign investment approval prior to 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 starting a business that is a carrier to which the *Telecommunications Act 1997* applies.

Voluntary notification

Foreign persons proposing to start a carriage service provider to which the *Telecommunications Act 1997* applies and they expect that they may be subsequently nominated under subsection 197(4) of the *Telecommunications (Interception and Access) Act 1979* are encouraged to seek foreign investment approval.

Carriers operate telecommunications networks and infrastructure. Carriage service providers use carrier networks to provide services such as phones and internet. Further information is available from the Australian Communications and Media Authority at https://www.acma.gov.au/carriers-and-carriage-service-providers.

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

Nil 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 invest in a business or entity that owns or operates broadcasting transmission assets and operates from, or intends to operate from, at least 50 different sites are encouraged to seek foreign investment approval.

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 name systems

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 of the Domain Name System can compromise users' ability to conduct business, navigate the internet or compromise sensitive data.

Mandatory notification obligations

Nil 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 invest in a business or entity that is critical to the administration of an Australian domain name system are encouraged to seek foreign investment approval.

'Australian domain name system' means a country code Top Level Domain or a generic Top Level Domain where the administrator of that domain name system is resident in Australia.

Commercial construction contractors

Construction firms often hold contracts with government agencies and critical infrastructure service providers. Commercial construction firms which develop assets for these clients may have significant access to sensitive information, such as building blueprints and supply chains. 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, in order to gather information on intended sensitive tenants.

Mandatory notification obligations

Nil 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 invest in a business or entity which holds contracts to construct buildings which will house the following types of tenants are encouraged to notify:

- The 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*.

Commercial real estate

Commercial buildings may house government or critical infrastructure tenants from across multiple sectors, which hold sensitive data which may be of interest to foreign intelligence services. 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

Nil notifiable national security actions (except if Defence or an agency in the national intelligence community has an interest). 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 invest 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 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.

However, the scarcity and geographical concentration of some critical minerals leaves them potentially vulnerable to supply chain manipulation and disruptions.

Mandatory notification obligations

Nil 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 invest 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

Critical service providers and suppliers

Service providers can be key components in the supply chain for essential goods and services that Australian's rely on. 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

Nil 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 invest in a business or entity with the following criteria are encouraged to seek foreign investment approval:

- The business provides services to:
  - The 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 Legislation Amendment (Critical Infrastructure) Bill 2020 that is currently before Parliament;

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 Legislation Amendment (Critical Infrastructure) Bill 2020 that is currently before Parliament).
  - 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*).
  - 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 have the capacity to significantly enhance or pose risk to our national interests, including in particular national security. Given their criticality, these goods, technologies, and services may be a target for malicious activity for foreign interference, espionage and sabotage.

Mandatory notification obligations

Nil 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 invest in a business or entity that develops, manufactures or supplies critical technologies with a civilian or dual use focus which is otherwise not captured by the mandatory notification requirements in the following areas are encouraged to seek foreign investment approval:

- Material sciences and advanced manufacturing
- Quantum technologies
- Artificial intelligence and robotics
- Biotechnologies
- Communications and sensing
- Space capabilities

Example 6

David is a foreign person looking to start an additive manufacturing company in Australia. David's company would manufacture prosthetics using proprietary 3D printing technology. David does not intend for these products to be for a military use, or an intelligence use. While additive manufacturing is on the defence critical technology list, as David is not intending for it to have a military use, his proposed business would not meet the thresholds defined in legislation for a national security business. However, given the status of advanced manufacturing 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.

Mandatory notification obligations

The Australian Government seeks to oversee foreign investment in critical goods, technology, and services that have 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 their highly essential nature to Defence's capability advantage; and/or

- The Australian Government needs to limit others' access due to their highly sensitive nature which could adversely impact upon Defence interests.

Accordingly, foreign persons must seek foreign investment approval prior to starting, or acquiring a direct in, a business that develops, manufactures, or supplies critical goods or technology, for or intended for, a military end-use by defence and intelligence personnel or the defence force of another country.

- '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 publically 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.

Indicative Sectors	**Non-exhaustive examples**
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 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.

Indicative Sectors	Non-exhaustive examples
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.
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, related equipment, components and materials, and related equipment, components and materials.

Indicative Sectors	Non-exhaustive examples
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 national security 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 invest in businesses or entities with a contractual relationship with the Department of 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. 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

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 is critical to ensuring the security and reliability of electricity networks or electricity systems (this includes synchronous generators above relevant jurisdictional capacity thresholds and generators contracted to provide system restart services).
    - The relevant capacity thresholds are New South Wales (1,400 megawatts (MW)), Victoria (1,200MW), Queensland (1,300MW), Western Australia (600MW); South Australia (600MW), Tasmania (700MW) and the Northern Territory (300MW).

Voluntary notification

Investments in other types of electricity assets may also pose national security risks. As renewable energy plays a greater role in Australia's energy mix, access to and control of new forms of generation and storage may create risks from espionage, sabotage and foreign interference.

Foreign persons proposing to invest in a business or entity that owns or operates an electricity generation station (including storage) with a generation capacity of at least 50MW (and which is not covered by the mandatory notification requirements) are encouraged to seek foreign investment approval.

Foreign persons proposing to invest 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.

Example 7

Green Energy Fund (GEF) is a foreign person and wishes to acquire a direct interest in Deb's Solar Farm Pty Ltd, which owns and operates a 200MW solar farm in Queensland. As the solar farm is not a synchronous generator of 1,300MW or above, and is not contracted to provide system restart services, it is not considered a national security business. The proposed transaction is not subject to mandatory notification. However, as the solar farm has a capacity greater than 50MW, GEF is encouraged to voluntarily notifying the proposed transaction.

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

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;
- storage facility with a maximum daily quantity of at least 75 terajoules per day;
- distribution network or system ultimately servicing 100,000 customers; or
- a gas transmission pipeline that is critical to ensuring the security and reliability of a gas market.

The thresholds for whether a gas transmission pipeline is critical are different in different markets. In the Eastern gas market, a transmission pipeline with a capacity of 200 terajoules per day is critical. In the Northern gas market, the threshold is 80 terajoules per day, and in the Western market the threshold is 150 terajoules per day.

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 invest 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.

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

Nil 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 invest in a business or entity that owns or operates a liquid fuel refinery or owns or operates a storage facility capable of storing more than 100 megalitres are encouraged to seek foreign investment approval.

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

Nil 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 invest in an energy market operator, or an asset used by an energy market operator that is essential to ensuring the security and reliability of an energy market, are encouraged to seek foreign investment approval.

For these purposes, energy market operators include 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.

Health

The health sector provides essential services that all Australians rely on – this has been brought into sharp focus during the COVID-19 crisis. National security risks could arise through a widespread failure or disruption, or large-scale collection of health-related data for malicious purposes.

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

Nil 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 invest in a hospital, 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

Nil 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 invest 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 part of the National Medical Stockpile and 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. Australian universities may also be targets of foreign interference.

Mandatory notification obligations

Nil 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 invest in a business or entity that is registered in the Australian university category of the National Register of Higher Education Providers are encouraged to seek foreign investment approval.

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.

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

A foreign person must notify the Treasurer and seek approval prior to acquiring a direct interest in a business that stores or has access to security classified information. Security classified information means information that is classified as Protected or higher within the Australian Government Protective Security Policy Framework, and information with equivalent classifications from other countries.

A foreign person must also notify the Treasurer and seek approval prior to acquiring a direct interest in a business that stores, maintains or has access to personal information, collected by the Australian Defence Force, the Defence Department or an agency in the national intelligence community, which if accessed or 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 invest in a business or entity that owns or operates a data centre or cloud provider that stores or processes 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*) 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

Nil 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 invest 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

Nil 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 invest 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. However, 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.

Mandatory notification obligations

Nil 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 invest 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 or 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

Nil 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 invest in a business or entity that operates a satellite ground station, or 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.

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

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 ensure the security of maritime ports and shipping within Australian waters.

Foreign persons proposing to invest 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

Nil 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 invest in a business or entity that owns or operates a security controlled airport under the *Aviation Transport Security Act 2004* are encouraged to seek foreign investment approval.

Foreign persons proposing to invest in a business or entity that owns or operates a regulated air cargo agent under the Aviation Transport Security Regulations 2005 are encouraged to seek foreign investment approval.

Foreign persons proposing to invest in a business or entity that is an aircraft operator (within the meaning of the *Aviation Transport Security Act 2004*) that provides 'a regular public transport operation' (within the meaning of 1.06(1)(a) of the Aviation Transport Security Regulations 2005) are encouraged to seek foreign investment approval.

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

Nil 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 invest in a business or 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 are encouraged to seek foreign investment approval.

Water and sewerage

A clean and reliable supply of water is essential to all Australians, and many of our critical infrastructure sectors and businesses. 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

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 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.