



Australian Government

Attorney-General's Department

**Australian Security
Intelligence Organisation**

15 January 2016

**Foreign investment review framework
Attorney-General's Department and Australian Security
Intelligence Organisation submission to the Senate
Economics References Committee**

Role of the Attorney-General's portfolio

The Attorney-General's Department (the Department) and Australian Security Intelligence Organisation (ASIO) are the two key agencies in the Attorney-General's portfolio which provide input to the foreign investment review process. The Department consults other portfolio agencies on particular applications as necessary.

The role of the Attorney-General's Department: Critical Infrastructure resilience policy

The Attorney-General's Department is the lead Commonwealth agency for critical infrastructure resilience policy as part of its broad responsibility for national security laws and policies and our role working with portfolio agencies and across government to prevent and respond to national security threats.

Critical infrastructure delivers essential services such as food, water, healthcare, electricity, communications, transportation and banking. The Commonwealth and state and territory agreed definition of critical infrastructure is:

Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.

The ongoing efficient operation of these services underpins Australia's social cohesion, economic prosperity and public safety. The resilience of our critical infrastructure is therefore integral to a strong economy, a vibrant business sector and government's ability to deliver routine and emergency response services. It is also vital to the resilience of our communities to disasters.

Foreign investment in Australia plays an essential element in the resilience of our critical infrastructure. In addition to assisting our companies access overseas markets, securing vital funding for expansion and diversification, and tapping into expertise and innovation, it also provides a vital source of funds to restore and enhance ageing critical infrastructure networks and assets in order to increase their resilience and better ensure the continuity of the essential service they provide.

While foreign investment benefits both Australia and individual critical infrastructure organisations, there are potential risks to Australia's national security associated with this involvement that require consideration and management as necessary. This may include, for example, licence conditions or deeds of agreement to protect the integrity of critical infrastructure against potential national security threats of espionage, sabotage and foreign interference.

Foreign investment is just one of the vectors considered by the Department. Espionage, sabotage and foreign interference can also be enabled through other forms of foreign involvement in critical infrastructure, such as offshoring and outsourcing (particularly of key business systems or processes) and involvement in the supply chain. The Telecommunications Sector Security Reform (led by the Department in collaboration with ASIO and the Department of Communications and the Arts) is an example of an initiative to better manage national security threats associated with foreign involvement in the telecommunications sector (high risk

critical infrastructure) through telecommunications supply chains and outsourcing and offshoring arrangements.

Consideration of national security risks to critical infrastructure from espionage, sabotage and foreign interference forms one component of the Department's broader 'all hazards' approach to critical infrastructure resilience. The potential range of threats considered under this 'all hazards' approach ranges from natural disasters through to cyber-attacks and terrorism.

The Attorney-General, Senator the Hon George Brandis QC, launched the new Critical Infrastructure Resilience Strategy (the Strategy) on 21 May 2015. The Strategy consists of a Policy Statement that outlines the Government's high-level policy approach to critical infrastructure (**Attachment A**) and a Plan that provides details on the activities to be undertaken to implement the policy (**Attachment B**). The aim of the Strategy is the continued operation of critical infrastructure in the face of all hazards. More resilient critical infrastructure will also help support the continued provision of essential services (provided by critical infrastructure) to businesses, governments and the community, as well as to other critical infrastructure sectors.

The Strategy builds on the success of previous strategies through a range of resilience building initiatives designed to deliver greater value and flexibility to critical infrastructure stakeholders, including owners and operators and state and territory governments (state and territory governments have primary responsibility for responding to incidents that occur within their jurisdictions and each state and territory government has its own critical infrastructure program).

The Trusted Information Sharing Network (TISN) continues to be the most visible component of the business-government partnership approach underpinning the Strategy. It provides an environment where business and government can share information on the resilience of our critical infrastructure. In particular, the TISN provides a secure environment for critical infrastructure owners and operators across seven sector groups to regularly share information and cooperate within and across sectors to address security and business continuity challenges. This provides a key mechanism for raising awareness of national security threats associated with foreign involvement in supply chains.

The Australian Security Intelligence Organisation

ASIO's role is to provide advice on threats to security, as outlined in the *Australian Security Intelligence Organisation Act 1979*. These threats include sabotage, espionage and foreign interference.

As part of its responsibilities, ASIO provides advice to the Government on potential security threats associated with foreign investment, where an application has been referred to ASIO from the Treasury (as part of the foreign investment review process) or the Organisation is aware of potential threats through ASIO's investigative activities and/or other means.

ASIO also has a role – through the National Threat Assessment Centre (NTAC) – in providing threat advice regarding critical infrastructure to assist stakeholders, including government and industry, to understand their environment so they can plan and implement risk management strategies.

Portfolio input to foreign investment proposals

The *Foreign Acquisitions and Takeovers Act 1975* (the Act) empowers the Treasurer to prohibit or impose conditions on an investment if satisfied it would be contrary to the national interest. The Act confers upon the Treasurer the power to decide in each case whether a particular investment would be contrary to the national interest. The factors typically considered include national security, as well as broader national interest considerations of competition, impact on the economy and community, and the character of the investor.

There are well established Government processes in place to support consideration and mitigation of national security implications of foreign investment in critical infrastructure for applications subject to the Foreign Investment Review Board (FIRB). This process provides national security agencies with the ability to scrutinise prospective foreign investments in critical infrastructure and where needed implement measures to mitigate identified risks. The Attorney-General's portfolio agencies contribute to this process to ensure that national security and broader critical infrastructure resilience issues are taken into account in determining whether a foreign investment is in the national interest.

As part of the Government's consideration of foreign investment applications, Treasury, on behalf of the FIRB, consults with a wide range of Australian Government agencies, including the Department, ASIO and other portfolio agencies as required, on whether the proposals are in the national interest.