Australian Government

Critical Infrastructure Centre

The *Security of Critical Infrastructure Act 2018*

The *Security of Critical Infrastructure Act 2018* (the Act) contains a range of powers, functions and obligations that only apply in relation to specific critical infrastructure assets in the electricity, gas, water and ports sectors.

Why is the Act needed?

Foreign involvement in Australia's critical infrastructure has increased in recent years. Rapid technological changes have resulted in critical infrastructure assets with increased cyber connectivity, and greater participation in, and reliance on, global supply chains with many services being outsourced and offshored. The Australian Government welcomes these arrangements, which are vital to Australia's economy and infrastructure.

However, while recognising the many benefits, foreign involvement exposes Australia's critical infrastructure assets to national security risks, particularly sabotage, espionage and coercion. Foreign involvement, through ownership, offshoring, outsourcing and supply chain arrangements, can greatly increase a malicious actor's ability to disrupt critical infrastructure assets which could have a range of serious implications for business, government and the community.

The responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community is shared between owners and operators of critical infrastructure, state and territory governments, and the Australian Government.

The Act strengthens the Australian Government's capacity to manage the national security risks resulting from foreign involvement in Australia's critical infrastructure.

The Act also supports the work of the Critical Infrastructure Centre (the Centre). The Centre works across all levels of government and with critical infrastructure owners and operators to identify and manage the national security risks of espionage, sabotage and coercion. For more information on the Centre, please refer to the 'What is the Critical Infrastructure Centre' Factsheet?

When will the Act come into force?

The Act received Royal Assent on 11 April 2018 and came into force on 11 July 2018. Owners and operators of critical infrastructure assets captured by the Act will have six months from this date to report information on the Register of Critical Infrastructure Assets.

What assets are captured by the Act?

The Act only applies to specific assets in the electricity, gas, water and ports sectors which are characterised by a lack of:

- diversity and disaggregation of operators, and/or
- existing regulatory regimes designed to manage national security risks.

For more information on critical infrastructure assets captured by the Act, please refer to the 'Coverage of the *Security of Critical Infrastructure Act 2018*' Factsheet.

The *Security of Critical Infrastructure Act 2018*

What is in the Act?

The Act contains three key measures to manage national security risks related to critical infrastructure:

- the Register of Critical Infrastructure Assets (the Register)
- information gathering power, and
- Ministerial directions power.

Register of Critical Infrastructure Assets

The Register provides the Australian Government with greater visibility and understanding of who owns, controls and has access to critical infrastructure assets. The Act imposes reporting requirements on two sets of entities: direct interest holders and responsible entities.

Direct interest holders are entities holding greater than 10 per cent direct interest in the asset, or any entity who through direct ownership is in a position to directly or indirectly influence or control the asset. Direct interest holders will be required to provide interest and control information.

Responsible entities are the body licensed to operate the asset. Responsible entities will be required to provide operational information.

Direct interest holders and responsible entities initially have six months (from 11 July 2018) to report information on the Register. Following initial reporting, entities are obligated to notify the Australian Government of any changes to the required information within 30 days of the notifiable event. The Centre will maintain a secure web portal for entities to easily report this information.

The Register imposes a minimal compliance burden on impacted entities. Any information provided remains protected and confidential and will not be publicly disclosed.

Information gathering power

The Act provides the Secretary of the Department of Home Affairs with the power to request certain information from direct interest holders, responsible entities and operators of critical infrastructure assets. This enables the Secretary to request information from owners and operators to:

- inform risk assessments conducted by the Centre
- rectify any information gaps on the Register
- assist with determining whether a Ministerial direction should be issued to mitigate a national security risk.

Any information that is obtained using this power is protected and confidential and will not be publicly disclosed.

Ministerial directions power

The Ministerial directions power allows the Minister to issue a direction to an owner or operator of a critical infrastructure asset to mitigate national security risks, where the risks cannot be managed through collaboration with owners and operators or via existing regulatory frameworks. The directions power is only able to be used where:

- there is a risk identified which is prejudicial to security
- through collaboration, the owner or operator does not or cannot implement mitigations to address the risk, and
- there are no existing regulatory frameworks that can be used to enforce mitigations.

Before issuing a direction, the Minister must be satisfied of certain matters, consult, and give consideration to a number of factors, including:

- giving primary consideration to a mandatory ASIO adverse security assessment
- being satisfied that 'good faith' negotiations have occurred
- consulting directly and giving consideration to any representation made by the relevant First Minister, state or territory minister and the affected entity to which the direction applies
- considering the costs and consequences to services in implementing the mitigation, and
- ensuring the direction is a proportionate response to the risk.

These safeguards reinforce the Australian Government's intention to promote a collaborative approach to managing national security risks from foreign involvement. It also ensures the Ministerial directions power is exercised within the remit of specific national security risks that cannot be addressed through other means.

Ministerial Directions Power in practice

Identify Risk

The Centre completes an asset-level risk assessment.

The Centre identifies a national security risk related to foreign involvement in an asset.

Consult with owners, states and regulators

The Centre engages with relevant stakeholders to develop a strategy to mitigate the risk.

Stakeholders include the Australian Government, state or territory governments, regulators and asset owners and operators.

Attempt to implement mitigations

Risk mitigations will be developed collaboratively.

There are two possible scenarios:

1. risk mitigations are implemented voluntarily by the asset owner or operator, or by leveraging existing legislative or regulatory mechanisms.

   If risk mitigations implemented, no further action required.

2. risk mitigations are not fully implemented.

Meet legislative requirements to use power

If existing mechanisms are inadequate, the Centre will consider recommending the Minister issue a specific direction to mitigate the risk.

The directions power will only be used when conditions outlined on the previous page are met.

Minister issues Direction

The Minister will issue a direction only if the legislative requirements have been satisfied.

The Minister's decision to issue a direction is subject to judicial review.