Australian Government

Critical Infrastructure Centre

Critical Infrastructure Centre Compliance Strategy

3-5 National Circuit
BARTON ACT 2600

+61 2 6141 3338

cicentre.gov.au

Contents

Purpose of this strategy

This strategy outlines the compliance approach of the Critical Infrastructure Centre (the Centre) as the body responsible for the administration and enforcement of aspects of the *Security of Critical Infrastructure Act 2018* (the SOCI Act) and the 2017 reforms to the *Telecommunications Act 1997* (the TSS reforms). This strategy also outlines the Centre's compliance approach in relation to aspects of the foreign investment review process under the *Foreign Acquisitions and Takeovers Act 1975* (FATA).

The purpose of this strategy is to outline how the Centre will facilitate full compliance by critical infrastructure owners and operators with their obligations under legislation and, where applicable, FATA conditions. The strategy outlines key obligations for critical infrastructure owners and operators and explains key elements of the Centre's compliance approach and activities.

The Centre will review this strategy periodically to account for new findings from intelligence, risk evaluation and regulatory engagement.

Role of the Critical Infrastructure Centre

The Centre develops policy and advice to address the complex national security risks to Australia's critical infrastructure.

What is Critical Infrastructure?

Critical infrastructure underpins the functioning of Australia's society and economy. While foreign investment and global supply chains are invaluable to Australia's critical infrastructure, foreign involvement also creates and exacerbates opportunities for activities prejudice Australia's national security.

The following definition guides the Australian Government's approach to critical infrastructure security:

'those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.'1

In this context, 'significantly' means an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia's international competitiveness in global markets, or impedes the continuity of government and its services.

The Australian Government identifies eight critical infrastructure sectors: telecommunications, energy (gas and electricity), water, government, transport, health, banking and finance, and food.

[1] Critical Infrastructure Resilience Strategy

The Centre

In January 2017, the Australian Government launched the Critical Infrastructure Centre (now within the Critical Infrastructure Security Division in the Department of Home Affairs) to enhance its ability to respond to the evolving threat environment, particularly from foreign interference in Australia's critical infrastructure.

The Centre's strategic purpose is to adopt a risk-based approach to ensure the resilience and security of critical infrastructure. The Centre undertakes two roles to achieve this purpose:

1. Support critical infrastructure owners and operators to build resilience and effectively manage risks to the integrity and continuity of their operations in the face of all hazards.
2. Intervene to ensure owners and operators protect critical infrastructure from a range of national security threats including espionage, sabotage and foreign interference.

Regulation is one of the Centre's tools to fulfil these roles, alongside risk assessments, activities to support compliance with FATA conditions and industry standards, risk scenario exercising, and information sharing.

Wherever possible, the Centre seeks to work in partnership with industry, and support them to understand and manage their own risk. Information sharing between government and industry, and across industry, has proven to be an effective mechanism to build organisational and sectoral resilience with minimal government intervention. The Centre's vision for Australia's critical infrastructure is one of voluntary compliance by owners and operators, with the Centre as an industry resource, whereby industry and government work cooperatively to jointly manage security risks.

The Centre manages and undertakes both policy and regulatory activities. This allows the Centre to use lessons learned to develop and increase the efficiency and effectiveness of policy and improve security outcomes.

Legislation and regulation

The Australian Government has introduced two sets of legislation, to address national security risks associated with Australia's critical infrastructure, SOCI and the TSS reforms, which operate alongside the FATA. The Department of Home Affairs' regulatory powers with respect to the SOCI Act and TSS reforms arise from provisions in the *Regulatory Powers (Standard Provisions) Act 2014*.

Security of Critical Infrastructure Act 2018

The SOCI Act is designed to manage national security risks arising from foreign involvement in Australia's critical infrastructure in the electricity, gas, water and ports sectors. It introduced three key measures to address and manage these risks:

- a reporting obligation and asset register: entities who own and control asset must provide the Government with that information
- an information gathering power: the Secretary of the Department of Home Affairs can obtain information and documents from reporting entities and operators, and
- directions powers: the Minister for Home Affairs can issue directions in cases where there is a national security risk and mitigations cannot be implemented in collaboration with asset owners and operators.

The SOCI Act applies to the highest risk assets in the electricity, gas, water, and ports sectors where existing regulatory regimes are insufficient to manage these risks, or no other regulatory options are available.

The SOCI Act came into force on 11 July 2018 and currently applies to approximately 168 assets in Australia. The Act provided for a grace period on initial reporting obligations. Two types of entities are required to report under the Act:

- A responsible entity: the entity that holds or is otherwise declared to hold operational responsibility for the asset, and
- A direct interest holder: any entity (together with any associates of the entity) that holds at least a 10 per cent interest in the asset or holds an interest that allows the entity to directly or indirectly influence or control the asset.

Telecommunications Act 1997

The TSS reforms created a regulatory framework to better manage national security risks to Australia's telecommunications networks and facilities. Key elements of the reforms include:

- a security obligation – all carriers, carriage service providers and carriage service intermediaries are required to do their best to protect networks and facilities from unauthorised access or interference
- a notification obligation – carriers and nominated carriage service providers are required to notify the Australian Government of planned changes to their networks and services that could compromise their ability to comply with the security obligation
- an information gathering power – the Secretary of the Department of Home Affairs can obtain information and documents from carriers and carriage service providers for the purpose of assessing their compliance with the security obligation, and
- directions powers – the Minister for Home Affairs can direct a carrier, carriage service provider or carriage service intermediary:
  - to not use or supply carriage services if the Minister considers the use or supply prejudicial to national security, and
  - to do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks.

The TSS reforms came into force on 18 September 2018.

Foreign Acquisitions and Takeovers Act 1975

Under Australia's foreign investment framework, the Australian Government requires certain proposed foreign investments to be notified and a no objections notification be issued before the investment can be made. Under the FATA, the Treasurer makes a national interest decision on foreign investment proposals that fall under the regime. The Centre supports the FATA by providing national security advice to support the Treasurer's national interest decision. The Centre's advice focuses on the national security risks of espionage, sabotage and foreign interference from foreign involvement in Australia's critical infrastructure.

Where national interest concerns arise, the Treasurer may impose certain conditions on the investment to mitigate those concerns. Treasury has primary responsibility for compliance with those conditions. The Centre and other security agencies work with the Treasury to manage compliance with those conditions that address national security risks.

The Centre also supports other regulatory regimes that involve critical infrastructure, such as the Northern Australian Infrastructure Facility (NAIF) and the Australian Energy Market Operator (AEMO).

Our approach to compliance

The Centre seeks to ensure consistent and effective security and risk management measures are implemented and maintained across critical infrastructure sectors.

Compliance Model

The Centre's utilises a tiered approach based on risk differentiation and responsive compliance models. Under this approach, responses to non-compliance are determined by the specific nature of the risk created by non-compliance or the behaviour of the entity regarding its non-compliance, illustrated in *Figure 1* below.

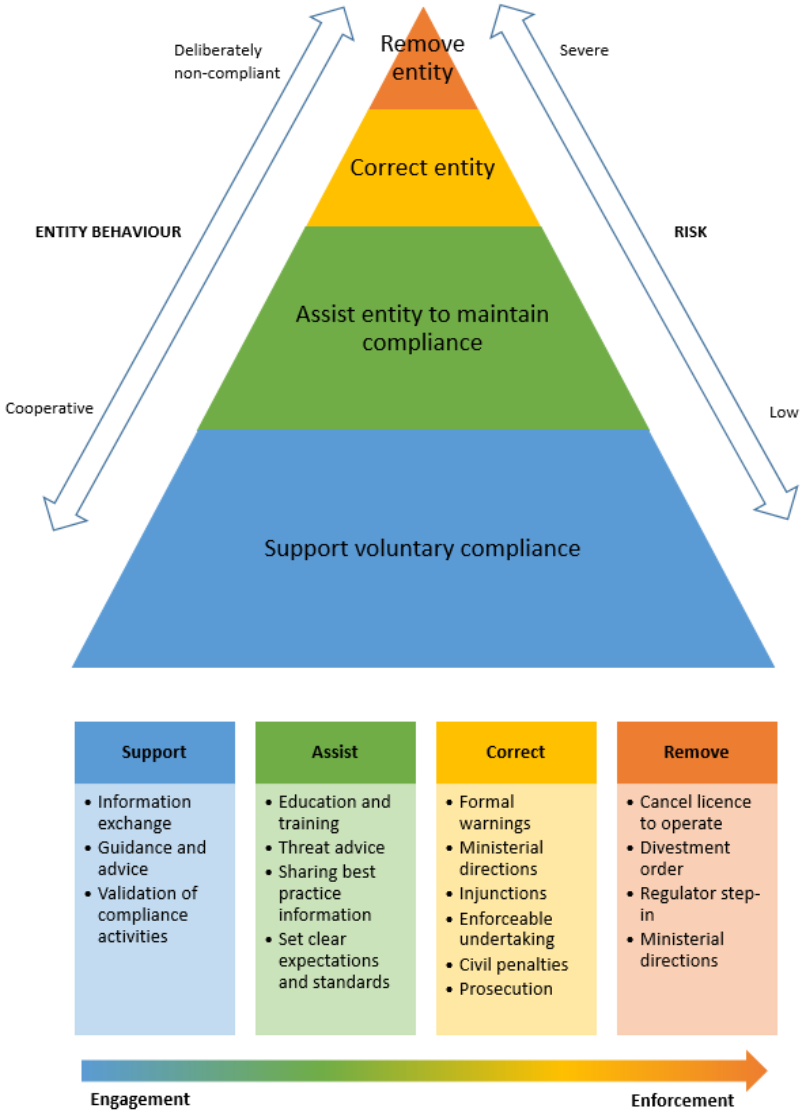

Figure 1: Critical Infrastructure Centre Compliance Model

Principles

The Centre's compliance model is founded on the following principles:

Managing risk – The Centre defines success through the mitigation of risk, rather than by applying enforcement measures. The Centre therefore supports dialogue and information exchange with non-compliant entities, including developing alternative measures based on industry advice if they are determined to be more effective at reducing risk. The Centre holds enforcement powers under legislation if necessary to manage and reduce risk.

Confidentiality – The Centre maintains strict confidentiality practices to safeguard confidential or sensitive information (such as commercial-in-confidence price or market sensitive information), ensure fairness to entities, and maintain the privacy of personal information. These practices accord with information protection provisions in the SOCI Act (s45-46), the TSS reforms (s315H), FATA (Part 7, Division 3), and the Privacy Act 1988, whilst also meeting obligations under the Freedom of Information Act 1982.

Constructive relationships – The Centre assists and supports entities that are willing to comply and genuinely seeking to mitigate security risks in their enterprises. The Centre will wherever possible undertake good faith engagement when working with non-compliant entities, and considers its enforcement powers a measure of last resort.

Education and awareness – The Centre considers an informed industry essential to achieving compliance. As such, the Centre emphasises industry engagement, education, awareness raising, and support in its compliance activities. The Centre supports open dialogue with entities on security threats, its activities, and its goals in order to assist entities with their decision-making.

Voluntary compliance – Over the long term, the Centre builds towards a culture of voluntary compliance by industry, with the Centre acting as a validating body. The Centre envisions compliance with critical infrastructure security requirements as a natural part of business process and industry best practice.

Compliance Activities

The Centre will conduct monitoring activities to assess entity compliance with their obligations under the SOCI Act, the TSS reforms and to support Treasury's compliance activities under the FATA. Monitoring activities may include, but are not limited to:

Monitoring Activity	SOCI	TSS	FATA
Entity reporting requirements	✓	✓	✓
Information gathering	✓	✓	✓
Inspection and retention of documents	✓	✓	✓
Audits, by the Centre or authorised representatives	✓	✓	✓
Assessing compliance	✓	✓	✓

Managing non-compliance

Approach

The Centre will seek to address non-compliance in accordance with the approach set out above in Figure 1. Assessments of non-compliance will be based on evidence, with an overall goal of consistency and fairness.

When assessing non-compliance and determining an appropriate response, the Centre considers three factors:

1. **Risk** – what impact does non-compliance have on Australia's national security? What is the nature of the risk? What solutions are available? How effective are they? Does the risk demand urgent action?
2. **Proportionality** – how serious is the risk created by the identified breach? Are there any aggravating circumstances?
3. **Engagement of the entity** – what is the entity's attitude towards compliance? How cooperative is the entity, based on engagement with the Centre and their compliance history?

The Centre's response options to non-compliance can be categorised broadly as:

Support – The Centre will provide information and guidance to entities to support their compliance efforts.

Assist – Where an entity is non-compliant but engaged, the Centre will seek to establish an agreed course of action with the entity to return to compliance. The Centre expects the majority of its compliance activities to focus on supporting and assisting entities.

Correct – Where engagement, negotiation, or mediation are unsuccessful, or where the Centre believes the entity is not acting in good faith, the Centre will escalate to enforcement measures to achieve compliance and mitigate the identified risk. The Centre expects this scenario to be rare.

Remove – Finally, in extreme cases where non-compliance presents an intolerable risk to national security, or the entity is unwilling or unable to become compliant, then the Centre may recommend that action be taken to remove the risk entirely, including through using the s32 directions power in the SOCI Act. The Centre expects this scenario to be extremely rare.

In circumstances where a serious risk unexpectedly presents itself and must be addressed urgently, the Centre may escalate immediately to direct measures to protect critical infrastructure, but will seek to maintain communication and cooperation with the entity as much as circumstances allow.

Review

The Centre will continually review its activities based on the results and impact on industry. The Centre may also develop new activities or amend existing ones as the risk environment evolves over time.

Integrity

The Centre takes integrity and fairness seriously when undertaking its compliance activities. Compliance activities are conducted by Centre officers with distinct compliance responsibilities separate from those of officers that handle the Centre's SOCI, TSS and FATA responsibilities, to ensure impartiality and avoid prejudice.