Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy

April 2022

Contents

Compliance and Enforcement Strategy

The purpose of this strategy is to outline how the Cyber and Infrastructure Security Centre (the Centre) will accomplish compliance and enforcement of the entities it regulates by ensuring they satisfy their regulatory obligations under relevant legislation. In delivering a best-practice, industry-focused, active and engaged regulatory partnership that works with industry to improve Australia's security and prosperity, the Centre drives an all-hazards approach across each of the 11 critical infrastructure sectors it regulates, underpinned by a strong focus on cyber security.

The Compliance and Enforcement Strategy explains the key principles that underpin the Centre's regulatory, compliance and enforcement approach and should be read in conjunction with the Centre's Protecting Australia Together publication and the Critical Infrastructure Resilience Strategy .

The Centre promotes best-practice security and risk management by ensuring regulated businesses are aware of and understand their regulatory obligations and risks, and to undertake controls that appropriately and proportionately mitigate risk. The Centre will make legislative decisions that uphold effective regulatory settings, strengthened by compliance activities to assure government that security outcomes are being met.

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

Who do we regulate?

The Centre plays a vital role in enhancing security and resilience in the following critical infrastructure sectors:

- communications
- financial services and markets
- data storage or processing
- defence industry
- higher education and research
- energy
- food and grocery
- health care and medical
- space technology
- transport (including aviation, maritime and land transport)
- water and sewerage.

Our critical infrastructure sectors are more interdependent than ever before, where failure or disruption in one area can impact others. The Centre works in partnership with all levels of government and industry to help owners and operators across each critical infrastructure sector understand potential threats, including natural disasters, terrorism and foreign interference that could impact their asset, and help them to plan and prepare for them.

Our legislation

The Centre administers the following legislation:

- *Security of Critical Infrastructure Act 2018* (SOCI)
- Telecommunications Sector Security Reforms (TSSR) to Part 14 of the *Telecommunications Act 1997*
- *Aviation Transport Security Act 2004* (ATSA)
- *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA)
- *AusCheck Act 2007.*

The Centre also provides risk advice to other agencies, including under the *Foreign Acquisitions and Takeovers Act 1975* (FATA), administered by the Treasury.

Functions and powers

SOCI and TSSR confer functions and powers on the Department that broadly include and are not limited to:

- reporting obligations and asset register collection information
- notification obligations for telecommunications carriers and nominated carriage service providers
- information gathering powers – the Secretary of the Department of Home Affairs can obtain information and documents from reporting entities and operators
- 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 ATSA and MTOFSA and associated regulations (collectively referred to as the transport security legislation) confer functions and powers on the Centre that broadly include and are not limited to:

- establishing mechanisms to safeguard against unlawful interference with aviation or maritime sectors
- establishing a regulatory framework centred around the development of security programs for aviation assets and maritime entities to meet security outcomes
- the requirement to provide security compliance information to the Secretary
- security incident reporting obligations
- Secretary-issued security control directions
- ensuring Australia's aviation obligations are met under the *Convention on International Civil Aviation*, Security – including its annex Safeguarding International Civil Aviation against Acts of Unlawful Interference – also known as the Chicago Convention
- ensuring Australia's maritime obligations under Chapter XI-2 of the *International Convention for the Safety of Life at Sea 1974* (SOLAS) and the *International Ship and Port Facility Security Code 2003* (ISPS Code) are met.

The *AusCheck Act 2007* confers functions and powers on the Department that broadly include and are not limited to:

- background checking services for the Aviation Security Identification Card (ASIC), Maritime Security Identification Card (MSIC), National Health Security (NHS) check schemes, and Major National Events (MNEs)
- confirming the holder of such cards has a valid background check and is not a threat to aviation or maritime security
- assessment of an applicant's criminal history against criteria for aviation-security-relevant offences (ASROs) and maritime-security-relevant offences (MSROs).

Our regulatory principles

The following principles guide us in carrying out our regulatory activities to ensure security outcomes are achieved, exercising our regulatory powers and rules, and engaging with industry stakeholders, participants and regulated entities. Through our decisions and actions we will embrace the following five principles:

Focus on risk	Taking a risk-based approach, focusing our attention and resources on areas of higher risk to ensure the resilience and security of the sectors we regulate
Promote voluntary compliance	Where appropriate, adopting a consultative approach, soliciting feedback to inform continuous improvement and providing education and guidance to assist industry partners to understand legislative obligations
Be accountable, fair and transparent	Avoiding unnecessarily impeding the efficient and effective operations of regulated entities, while making timely decisions based on legislative requirements
Act consistently	Delivering equitable decision-making by treating like situations in a like manner, while taking account of specific case circumstances
Act proportionately	When exercising enforcement powers we will take into account the: • security implications of the non-compliance • seriousness of the non-compliance • compliance history and regulatory posture of the entity • need for deterrence • facts of the matter at hand • impact on Australia's reputation or Australian interests overseas.

Our regulatory approach

Wherever possible, the Centre seeks to work in partnership with industry, to ensure regulated entities 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 regulated entities is one of voluntary compliance by owners and operators, with the Centre as an industry resource, whereby industry and government work cooperatively together to ensure security risks are effectively managed.

The Centre recognises that both educative and enforcement mechanisms are necessary to provide an effective and flexible regulatory system that does not unnecessarily impede the efficient and effective operations of regulated entities. A range of regulatory options are available to address non-compliance including, but not limited to:

- education and engagement
- non-compliance and observation notices
- corrective action plans
- infringement notices
- directions
- enforceable undertakings
- enforcement orders
- suspension or revocation of authorisations
- prosecution.

Accordingly, we will assess any reported or detected breach of legislation and adopt the approach most likely to promote the legislation's objectives, including encouraging voluntary compliance or taking enforcement action where appropriate. In doing so, the Centre may consider a combination of options above to achieve the desired outcome, and this may result in an escalation to enforcement as appropriate to the relevant breach.

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. Various compliance functions are carried out by officers across the Centre; these have separate responsibilities, so as to avoid cross-over, ensure impartiality and avoid prejudice.

Regulator Performance

Through the renewed Deregulation Agenda, the Australian Government is committed to ensuring that this regulation is as effective and efficient as possible, through:

- Improving the accountability and transparency of regulator performance.
- Sharing best practice.
- Building regulator capability.
- Driving a culture of regulator excellence.

On 1 July 2021, the Regulator Performance Guide (the Guide) came into effect, replacing the 2014 Regulator Performance Framework. The Guide sets out the Government's expectations for regulator performance and reporting via the principles of regulator best practice:

- Continuous improvement and building trust.
- Risk based and data driven.
- Collaboration and engagement.

In line with the stewardship approach, entities with regulatory functions are empowered to apply the principles of regulator best practice in a way that is appropriate to their organisation and consistent with Australian Government and stakeholder expectations.

Compliments, complaints or suggestions

Your feedback is valuable to us. It informs business improvement opportunities and further enhances the quality of our services. We welcome your feedback through our feedback form.

Further information

In you need further information related to the Centre or have an enquiry please contact the Centre via the General Enquiry Form or 1300 272 524 (Monday to Friday, 9 am to 5 pm AEST).

Aviation and maritime industry participants who operate under the transport security legislation and subsidiary regulations can contact the Transport Security Guidance Centre for regulatory information and advice via the Guidance Centre Enquiry Form or 1300 791 581 (option 1) (in Australia).

Australian Government

Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE