Critical Infrastructure Risk Management Program

Part 2A *Security of Critical Infrastructure* (SOCI) *Act 2018* Factsheet

This guidance material has been prepared to assist in the understanding of the Critical Infrastructure Risk Management Program Rules as part of the *Security of Critical Infrastructure Act 2018* (SOCI Act)

What is the CIRMP obligation?

The Critical Infrastructure Risk Management Program (CIRMP) is intended to uplift core security practices that relate to the management of certain critical infrastructure assets. It aims to ensure responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating risks.

Responsible entities of the asset classes in section 4 of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (the Rules) are required to establish, maintain, and comply with a written risk management program that manages the 'material risk' of a 'hazard' occurring, which could have a relevant impact on their critical infrastructure asset.

Responsible entities must identify, and as far as is reasonably practicable, take steps to minimise or eliminate these 'material risks' that could have a 'relevant impact' on their asset.

Principles-based outcomes

The SOCI Act and the Rules specify requirements to be contained in a CIRMP. These requirements are based on the following principles-based outcomes:

- Identify material risks – Entities will have a responsibility to take an all-hazards approach when identifying hazards that may affect the availability, integrity, reliability and confidentiality of their critical infrastructure asset.
- Minimise risks to prevent incidents – Entities will be required to consider risks to their critical infrastructure asset and establish appropriate strategies to minimise or eliminate the risk of hazards occurring, so far as is reasonably practicable. Entities should consider both proactive risk management as well as establishing and managing processes to detect and respond to threats as they are being realised to prevent the risk from eventuating.
- Mitigate the impact of realised incidents – Entities will be required to have robust procedures in place to mitigate, so far as is reasonably practicable, the impacts of a hazard, and recover from that impact as quickly as possible.
- Effective governance – Entities are required to provide an annual report that has been signed by their board, council or other governing body, to the relevant regulator, which in most instances is the Secretary of the Department of Home Affairs. The report must be in the approved form. The annual report does not need to contain the CIRMP but must advise the relevant regulator whether the program is up-to-date.

What assets are affected by the obligations?

The Rules apply to the following critical infrastructure assets:

- critical electricity assets
- critical energy market operator assets
- critical gas assets
- critical liquid fuels assets
- critical water assets
- critical financial market infrastructure assets used in connection with the operation of a payment system
- critical data storage or processing assets
- certain critical hospitals (listed in the Rules)
- critical domain name systems
- critical food and grocery assets
- critical freight infrastructure assets (the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* specify that the listed intermodal transfer facilities will be critical to the transportation of goods between states or territories).
- critical freight services assets
- critical broadcasting assets

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter and LinkedIn

February 2023

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

What is a material risk?

A ‘material risk’ to a critical infrastructure asset occurs when the risk has a ‘relevant impact’ on the asset. Section 6 (a-e) of the Rules provides the parameters of a material risk.

These include the risk of impairment, stoppage, loss of access to or interference with the asset.

What is a relevant impact?

A ‘relevant impact’ is an impact on the availability, integrity, and reliability of the asset, and the impact on the confidentiality of information about the asset, information stored in the asset if any, and, if the asset is computer data, the computer data.

The relevant impact may be direct or indirect. It must be more serious than a reduction in the quality of service being provided.

CIRMP Hazard Rules

The Rules contain obligations relating to protections within four key hazard vectors:

- Physical security and natural – physical security risks to parts of the asset critical to the functioning of the asset, including physical access to sensitive facilities (e.g., control rooms) or natural disasters.
- Cyber and information security – ‘cyber’ risks to digital systems, computers, datasets, and networks that underpin critical infrastructure systems. This includes improper access, misuse, or unauthorised control.
- Personnel – the ‘trusted insider’ risk posed by critical workers who have the access and ability to disrupt the functioning of the asset.
- Supply chain – risk of disruption to critical supply chains leading to a relevant impact on the critical infrastructure asset. The threat could be naturally occurring, malicious or purposefully intended to compromise the critical infrastructure asset.

What are the annual reporting requirements?

Entities are required to provide an annual report to the relevant Commonwealth regulator or the Secretary of the Department of Home Affairs, regarding the entity’s CIRMP. Entities must submit this report within 90 days after the end of the financial year and the report must be approved by the entity’s board, council, or other governing body.

The report must be in the approved form and state whether the risk management program was up to date, any variations to the program, and details of how the program was effective in mitigating any relevant impacts that hazards may have had on that asset during that year.

The report does not need to contain the full risk management program, but must advise the relevant Commonwealth regulator or the Secretary whether the program remains up-to-date.

What does ‘so far as it is reasonably practicable’ mean?

The requirement to minimise or eliminate material risks ‘so far as it is reasonably practicable’ advises the responsible entities to act at a particular time that is reasonably possible to address those risks.

In considering the material risks to their business, responsible entities must weigh up what can be done to mitigate those risks – i.e., what is possible in the circumstances and whether those actions are reasonable in the circumstance. There is no expectation that entities pursue risk mitigation measures that are disproportionate relative to the likelihood and consequences of a particular risk.

The requirement provides responsible entities flexibility to determine how they address material risk and relevant impact in relation to their business size, maturity, income and overall asset criticality. The intent is for responsible entities to seek to minimise or eliminate material risk where it is reasonably possible, in order to secure their critical infrastructure asset.

The Centre suggests better practice is for an entity’s board, council or other governing body (if the entity has one) to approve the CIRMP once developed. In doing so, it should appropriately balance the costs of risk mitigation measures with the impact of those measures in reducing material risk within their own operational context.

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.

Contact Us | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter and LinkedIn

February 2023

Australian Government
Department of Home Affairs
CYBER AND INFRASTRUCTURE SECURITY CENTRE