Amstelveen

Reflections on the first Board Approved Annual Report under the SOCI Act

Boards of critical infrastructure assets face heightened expectations to ensure a robust risk management framework is in place to understand and mitigate operational risks, ensuring compliance with transformative Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) reforms. As the due date for the first board-approved annual report required under the Act fast approaches; this article offers an overview of the obligation to embed a Critical Infrastructure Risk Management Program.

BY LOUIS WELLARD & BRANDON NGUYEN

Introduction

Reforms to the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) through the passing of two Bills in December 2021 and March 2022 have expanded the designation of infrastructure sectors that are regarded as critical within Australia, and increased obligations on owners and operators of critical infrastructure assets to protect Australia's social and economic interests.

These reforms reflect some of the most dramatic changes to the regulatory landscape across critical infrastructure in Australian legislative history, providing the government with unprecedented levels of authority to intervene in the response to a security incident, and access operational information relevant to critical infrastructure assets. In addition, these reforms provide yet another regulatory mandate for robust, systematic risk management practices to be in place and operating effectively. As we approach the 28 September 2024 due date for the first board approved annual report required under the Act, which attests to the existence and operation of a Critical Infrastructure Risk Management Program (CIRMP) for each critical infrastructure asset, the following provides an overview of the obligations needing to be met under the CIRMP.

Background

1 The first reforms to the SOCI Act occurred in December 2021 following the passing of the Security Legislation Amendment (Critical Infrastructure) Bill (SLACI).

The primary amendments resulting from this Bill included an expanded range of sectors to be classed as 'critical infrastructure', thresholds (which in some instances have been tightened) that define critical infrastructure assets relevant to each sector under the Act, and also implemented mandatory reporting requirements to the Australian Cyber Security Centre (ACSC) for cyber security incidents that have a direct or indirect impact on the operation of a critical infrastructure asset. In addition, 'government assistance measures' were also legislated, providing the government with a right to intervene in the management and response to a cyber security incident should they determine the response from the impacted entity is not sufficient.

The 2023 Critical Infrastructure Resilience Strategy defines critical infrastructure as:

"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'".

The reforms within the second Bill; the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP) that were passed in March 2022 provide a series of further obligations centred on risk management and cyber security for critical infrastructure owners and operators to comply with.

2

The key components of reforms associated with the SLACIP Bill include:

Part 2A – Critical Infrastructure Risk Management Program (CIRMP)

Requiring a critical infrastructure owner/operator to identify and either eliminate or mitigate as far as reasonably practicable all material risks that could impact on the availability, integrity, reliability or confidentiality of each critical infrastructure asset.

Part 2C – Enhanced Cyber Security Obligations

Which may be 'switched on' at the discretion of the Minister for Home Affairs for any asset categorised as a System of National Significance (SONS) under Part 6A (discussed below). These obligations include:

- Demonstrating the existence of Cyber Incident Response Plans relevant to each SONS asset;
- Undertaking cyber security exercises to build cyber preparedness (which can involve representatives from government and must occur within a defined notice period);
- Undertaking vulnerability assessments to identify vulnerabilities for remediation; and
- Providing system information to develop and maintain a near real-time threat picture, which could include periodic reporting, event-based reporting, or the maintenance of system software that will enable Government to undertake their own system reporting over key technology that enables the effective operation of a critical infrastructure asset.

Part 6A – Systems of National Significance

Provides the Minister for Home Affairs with discretion to consider a single critical infrastructure asset or series of assets to be classified as SONS, which enables further obligations (such as those within Part 2C above) to be enacted or 'switched on' for each designated asset.

Part 2A referenced above is activated through a set of Rules, known as the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) (Cth) (CIRMP Rules). The CIRMP Rules outline the specific obligations that critical infrastructure owners and operators must meet to comply with the SOCI Act. These Rules include the mandate for all in-scope critical infrastructure assets to manage and maintain a CIRMP, and on an annual basis to issue a board-approved report confirming the existence, operation and currency of the CIRMP for each critical infrastructure asset. Provisions within the SOCI Act enable the government to access and assess the CIRMP upon request. Some of the key aspects to the CIRMP are discussed further below.

All Hazards Critical Infrastructure Risk Management Program Obligation

Entities responsible for critical infrastructure assets are required to establish and adhere to a CIRMP that identifies, minimises, and mitigates material risks posed by all potential hazards to each critical infrastructure asset.

Material risks should be considered through the lens of whether a risk could have a 'relevant impact' on the availability, integrity, reliability or confidentiality of the effective operation of a critical infrastructure asset. For all material risks identified, responsible entities must eliminate, or reduce these risks as far as is reasonably practicable to do so.

Key Considerations for Management

The SOCI Act and CIRMP Rules are deliberate in the wording that define a CIRMP as a "written program that identifies and manages material risks of 'hazards' that could have a 'relevant impact' on a CI (critical infrastructure) asset."[1] Strict compliance with this wording requires a critical infrastructure operator to ensure they have a CIRMP that is 'asset-centric' and therefore directly considers risks specific to each critical infrastructure asset. In practical terms, this would mean material risks that could have a relevant impact on each critical infrastructure asset should be documented within a targeted risk profile. Therefore, unless there is common equipment, infrastructure, personnel, technology and physical and natural hazards between a collection of critical infrastructure assets, these each require their own risk profile and risk mitigation or minimisation response. Responsible entities with more than one critical infrastructure asset should be conscious of how their CIRMP adequately addresses the nuances and asset-specific risks that may exist.

In addition, the definition of a "material risk", "relevant impact", along with asset "availability", "integrity", "reliability" and "confidentiality" should be contextualised to be relevant to the critical infrastructure organisation they apply to. Whilst legislative definitions exist within the SOCI Act, practical application of these needs to be developed to embed appropriate considerations into risk management processes. For example, if a critical infrastructure operator designates all identified asset-level risks that are assessed as High or above as "material", the operator should ensure that the existing risk management framework being relied upon for this risk assessment is adequately considering the consequences of an asset's availability, integrity, reliability or confidentiality being compromised.

Annual Report and Attestation Over the Operation of the CIRMP

Entities responsible for critical infrastructure assets are required to establish and adhere to a CIRMP that identifies, minimises, and mitigates material risks posed by all potential hazards to each critical infrastructure asset. Section 30AG under the SOCI Act requires a responsible entity to complete an Annual Report, in a designated format, 90 days after the end of each Australian financial year.

This Annual Report includes:

- A declaration that the CIRMP was up to date at the end of the financial year;
- Whether a hazard occurred throughout the year that had a material impact on the operation of the asset;
- Whether any variations to the CIRMP were made during the year, particularly in response to a hazard occurring;
- Whether the CIRMP was effective in mitigating any relevant impacts from hazards that may have occurred throughout the year; and
- An attestation that the information contained within the annual report has been approved by the Board or a relevant governing body.

This Annual Report must be submitted to the relevant Commonwealth regulator, which is currently the Cyber and Infrastructure Security Centre (CISC) for all critical infrastructure centres except for payment systems (who instead should submit their Annual Report to the Reserve Bank of Australia).

Given the CIRMP Rules came into effect on 17 February 2023 with a six-month grace period to enable compliance, the first Annual Report to be provided under the SOCI Act is for the financial year ending 30 June 2024 and is due by 28 September 2024.

Key Considerations for Management

There is limited guidance or definition for what is meant when the Board attests to whether the CIRMP is “up to date”. As such, a responsible entity should ensure they clearly define what this means within their CIRMP, so it is transparent to the Board what their attestation is regarding. Strict interpretation of this wording would likely result in a responsible entity only being able to attest to a CIRMP being up to date if:

- All material risks that could have a relevant impact on the availability, integrity, reliability or confidentiality of each critical infrastructure asset have been identified and recorded;
- Responses required against each defined hazard vector (personnel, cyber security, supply chain and physical security/natural hazards) have been implemented; and
- All material risks identified above have been eliminated or reduced as far as is reasonably practicable.

It is likely that there will be a wide range of responses and interpretations in the first year that the Annual Report is provided. The government have means to amend the CIRMP Rules or the guidance supporting these Rules in future years once an understanding of the baseline across all impacted critical infrastructure sectors has been established, and it should be expected that these Rules will continue to evolve in the immediate term.

Conclusion – Considerations for the Board & the Australian Government

For the Boards of critical infrastructure assets, there is an increasing expectation to ensure a robust, asset-centric risk management framework is in place and embedded to ensure operational risks to assets are properly understood. This needs to stand up to external scrutiny, given the powers of the government as the regulator to request access to the CIRMP.

For the Government, the broadened definitions of critical infrastructure, increased obligations to ensure robust risk management of threats that can disrupt operations, and enhanced provisions to access operational data and intervene during certain operational disruptions creates a complex landscape to effectively monitor and regulate with sufficient levels of sector expertise.

In conclusion, the reforms to the SOCI Act represent a significant shift in the regulatory landscape for critical infrastructure in Australia. By expanding the scope of what is considered critical infrastructure and imposing stringent risk management and cyber security obligations, these reforms aim to safeguard Australia's social and economic interests against a wide array of threats.

The introduction of the CIRMP and the enhanced cyber security obligations for SONS underscore the importance of proactive and comprehensive risk management practices. As the deadline for the first board-approved annual report approaches, it is crucial for owners and operators of critical infrastructure to ensure they are fully compliant with these new requirements. This will not only help in mitigating risks but also in maintaining the resilience and security of Australia's critical infrastructure in the face of evolving challenges.

Our Authors

Louis Wellard
Director

Louis is a compliance management expert with over 16 years of experience in risk management. He has served as a consultant and led enterprise risk and privacy functions at a critical infrastructure operator. Specialising in compliance matters like the SOCI Act, he has transformed risk management frameworks and optimised controls across public, private, and government sectors. Louis played a key role in the SOCI Act reform consultation, provided insights from industry to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), and has assisted critical infrastructure owners in meeting their obligations under the SOCI Act.

Brandon Nguyen
Senior Consultant

Brandon is an admitted lawyer in the Supreme Court of New South Wales. He is a risk, compliance and legal specialist with strong experience in risk and control management, gained through secondment roles supporting Line 1 and Compliance functions at a major insurer. He was also involved in a major risk uplift initiative at a major Australian medical indemnity insurance provider. His broader experience includes work in major financial institutions with a heavy exposure to cyber risk, such as superannuation, private equity and venture capital.

Amstelveen

Amstelveen equips organisations to identify, assess and mitigate their most significant risks. Our risk, compliance and technology professionals support clients to improve the governance of their organisations. We provide specialist support to the largest public and private organisations in Australia and New Zealand.