Submission to the Independent Reviewer

Consultation on the Independent Review of the Security of Critical Infrastructure Act 2018

[redacted]

22 December 2025

I welcome this opportunity to provide this submission to Professor Jill Slay, Independent Reviewer of the *Security of Critical Infrastructure Act 2018* (Cth)(SOCI). I make this submission in my personal capacity. I provide a brief overview and comment on 2 of the 4 questions:

- Is SOCI achieving its intended objectives?
- Are there new or emergent threats the SOCI Act is unable to manage in its current form?

The Independent Review of SOCI provides an opportunity for critical infrastructure sectors, regulators, government and academia to take stock of the operation of SOCI since its enactment in 2018 and the effect of its major reform over the last 5 years. SOCI has seen a lot of change in recent years, as successive Australian Governments strive to better protect Australia's critical infrastructure sectors and assets from threats to Australia's social and economic stability, defence and national security. This is a crucial mission that requires a strong and abiding commitment to the rule of law and democratic governance.

Overview

SOCI is one of the most important pieces of legislation in the suite of national security legislation that seeks to protect Australia's economic stability, social cohesion and national security. Its operation is complemented by the 2023 Critical Infrastructure Resilience Strategy and Plan and enhanced by the 2023-2030 Cyber Security Strategy. SOCI interacts with other legislation in the broader national security legislative framework, including but not limited to the *Foreign Acquisitions and Takeovers Act 1975* (Cth) and the *Cyber Security Act 2024* (Cth). It incorporates national and international standards and frameworks into its risk management program regime, providing flexibility and guidance for responsible entities regulated by SOCI.

SOCI is also part of a broader governance structure around national security, significantly cyber security but incorporating all hazards. As a hybrid security framework, it combines mandatory requirements, such as asset registration, positive security obligations for systems of national significance, response to serious cyber incidents and ministerial powers of direction, with more flexible arrangements, such as the ability of responsible entities to formulate a risk management program that reflects the needs of their businesses and sector while meeting statutory requirements. Together, these interactions create a robust, hybrid regulatory framework.

Is SOCI achieving its intended objectives?

The stated object of SOCI in section 3 is to 'provide a framework for managing risks relating to critical infrastructure.' Section 3 lists 6 core actions for achieving SOCI's object (listed below). Overall, SOCI is achieving its intended objectives. I make the following comments about each action to achieve the object:

- improving the transparency of the ownership and operational control of critical infrastructure in Australia to better understand those risks

The register of information in relation to critical infrastructure assets assists in understanding a range of risks, including changes in ownership of responsible entities and assets. I note that the register is not public. This impacts what can be known and understood about the ownership and control of critical infrastructure in Australia.

While there is a public interest in continuing to protect this information, for improving transparency, consider what can reasonably be made public. Additionally, how is this information being used and updated. Are there technological improvements to the register that can be made to make it more effective and useful?

The Trusted Information Sharing Network (TISN) operates as an important regulatory intermediary, seemingly creating space for critical infrastructure sectors to share information about the risks to CI. The TISN may provide an even more valuable opportunity to improve the transparency of ownership and operational control, while still protecting sensitive information through confidential and secure arrangements.

- facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks

TISN appears to have an important role in facilitating cooperation between government, regulators, owners and operators of critical infrastructure to share, identify and manage risks. Consideration could be given to whether the TISN is operating as effectively as it could and whether there are innovations within its current structure that would improve cooperation and collaboration across all levels of critical infrastructure security. Defining the different types of collaboration and cooperation that are available may be a good start in looking at improvements. For example, understanding how collaboration is practised within TISN, how it operates as a governance mechanism and whether it has more innovative applications.

- requiring responsible entities for critical infrastructure assets to identify and manage risks relating to those assets

This is a matter for responsible entities. There is not a lot of information on the public record about how responsible entities identify and manage risks relating to their assets, except as outlined in relevant rules, standards, frameworks and annual reporting. There may be issues for entities in identifying assets based on the definitions in the Act. There also needs to be some consideration of whether all assets are adequately identified.

- imposing enhanced cyber security obligations on relevant entities for systems of national significance to improve their preparedness for, and ability to respond to, cyber security incidents

The operative provisions of SOCI impose these obligations on systems of national significance. However, there is not a great deal of information on the public record about systems of national significance, except the number of entities declared as SONS by the Minister.

- imposing enhanced security obligations on responsible entities for critical telecommunications assets

Telecommunications assets are now covered by the SOCI regime. This was an important reform for bringing telecommunications with SOCI framework.

- providing a regime for the Commonwealth to respond to serious incidents relating to critical infrastructure assets

The SOCI Act provides a regime for the Commonwealth to respond to serious incidents relating to critical infrastructure assets. The main issue with this object is whether the interactions with other legislative frameworks, such as the *Cyber Security Act 2024*, and other governance arrangements, such as state based (eg, NSW) and sectoral (eg, AESCSF) arrangements, are working as they should be in regard to the serious incident response regime.

Are there new or emergent threats the SOCI Act is unable to manage in its current form?

SOCI may be unable to manage new or emergent threats in its current form. The impact of new and emerging technologies, such as developments in computing, communications and cryptography enabled by quantum information science, may challenge some of its legislative constructs, concepts and obligations. While SOCI also has in-built flexibility mechanisms within its risk management program rules that enable it to adapt to new or emergent threats, these mechanisms should be regularly reviewed and 'stress-tested' through forecasting new and emerging technologies and threats, and looking at how critical infrastructure sectors are responding, whether national and international standards bodies are responding, and whether SOCI should be updated to incorporate changing governance and standardisation.

With my colleague, Associate Professor Kayleen Manwaring (UNSW), we examined the capacity of SOCI to absorb technological change and manage or emergent threats. With Associate Professor Manwaring and Dr Tyrone Berger, we examined the complexity of the regulatory environment for the cloud services sector, which included obligations arising under the SOCI Act.

- In our co-authored article (with Associate Professor [redacted]), [redacted], published in the ANU Journal of Law and Technology in 2024, outlines the potential impact of quantum information technologies on the ability of critical infrastructure sectors to comply with their obligations under national security laws, including whether SOCI contains sufficient flexibility to absorb technological change and manage new or emergent material risks.
- In our article (with Associate Professor [redacted] and Dr [redacted]), [redacted], published by Bond Law Review in 2025, we identify and critically examine key elements of existing statutory, regulatory and guidance instruments imposing cyber security and CI obligations on cloud services providers, as well as agencies and institutions holding key regulatory roles. These elements are examined in the context of cloud services providers subject to direct legal obligations, such as being responsible entities for CI assets and/or systems of national significance under the SOCI Act and other cloud services entities that form part of the supply chain for other providers with such obligations.

There is scope to improve and enhance the operation and functions of the Trusted Information Sharing Network through research into its role as a regulatory intermediary between government and industry, and as a mechanism for early detection of new and emergent threats.

Critical infrastructure sectors are undergoing immense technological change, which in turn is reorganising how information technology and operational technologies interact. There is a need to examine how 'system-of systems', such as positioning, navigation and timing (PNT), are

responding to technological change, including how they are defined and managed within the SOCI regime, and whether 'system or systems' assets are appropriately defined and managed.

Questions also arise about how risks are understood and mitigated, and whether it is prudent to define 'system of systems', such as PNT, or other emerging sectors, as stand-alone critical infrastructure sectors. Research about sector definition methods and the economic and regulatory implications of defining new critical infrastructure sectors should be undertaken to ensure SOCI maintains its relevance and is able to anticipate changes within the economy and regulated sectors.