BCA
Business Council of Australia

19 December 2025

Dr Jill Slay
Independent Review of the Security of Critical Infrastructure Act 2018
Department of Home Affairs

Dear Dr Slay

The Business Council of Australia (BCA) welcomes the opportunity to provide a submission to the Independent Review of the Security of Critical Infrastructure Act 2018. We believe that a robust critical infrastructure protection framework is crucial for Australia's economic growth, productivity, and international competitiveness. The SOCI Act has been world-leading in many respects and could be made more efficient and effective.

Question 1: Is the SOCI Act achieving its intended objectives?

The SOCI Act has been effective in elevating awareness of security risks, both cyber and physical, at Board and Executive levels. In many organisations, it has driven stronger governance and accountability.

However, the Act would better achieve its objectives if regulated entities could spend less time interpreting complex and, at times, ambiguous obligations and definitions. Currently, a significant proportion of effort is directed towards understanding regulatory scope rather than addressing material security risks.

One example is the requirement to report on hazards that have had a "significant relevant impact." While "significant impact" is defined under 30BEA for cyber security incidents, it is not defined for reporting hazards, while "relevant impact" (not "significant") for hazards is defined under 8G.

The definition of "relevant impact" under 8G includes any impact to the availability, integrity, reliability or confidentiality of information about an asset. This sets an extremely low threshold, particularly for third-party supplier incidents, and low-level confidentiality events that do not disrupt service.

The result is over-notification and diversion of effort away from genuine risk management.

This could be solved by amending the SOCI Act to streamline and standardise the terminology used for "significant" and "relevant impact". If legislative amendment is not pursued, government could issue rules or clarifying guidance.

Question 2: Is the SOCI Act functioning as intended?

The breadth of definitions within the Act has encouraged a "compliance-first" approach rather than a "risk-first" culture. Entities subject to SOCI obligations now often prioritise legal interpretation and bespoke critical infrastructure risk management program (CIRMP) documentation over practical uplift in security resilience.

As a result, resources are frequently diverted from risk mitigation activities (such as improving incident response capability or strengthening supply chain assurance) towards compliance activities.

This could be addressed through amendments to section 30AH of the SOCI Act to state that a CIRMP should include evidence of implemented and tested controls (proportionate to the criticality of the asset), potentially including incident response, system recovery and continuity arrangements.

Question 3: Is the SOCI Act having any unintended consequences?

Several unintended consequences warrant attention.

The designation of telecommunications assets under the SOCI Act is misaligned with the Telecommunications Act, resulting in entities such as Mobile Virtual Network Operators (MVNOs) being captured despite not being regulated as telecommunications facilities. The SOCI Act should be amended to clarify that it covers only those telecommunications entities that operate facilities or exercise material control over network infrastructure.

There is a lack of clarity regarding obligations under section 12F(3) to notify other data storage or processing services. In practice, regulated entities face challenges in getting global service providers to accept, recognise or act on SOCI notifications. This could be addressed through more detailed guidance from the Department of Home Affairs on how this obligation is intended to operate.

The definition of "business critical data" is overly broad, particularly for modern data storage environments, capturing data that is peripheral to the operation of critical infrastructure assets. To refocus on the data that matter, the definition in section 5 of the Act could be narrowed to data whose loss or compromise would materially affect service delivery, pose safety or national security risks or prevent recovery of the asset. As a consequence, this would then narrow the scope of "data storage systems", meaning entities no longer have to look at an excessively large set of in-scope systems.

There is overlap between SOCI obligations and other regulatory frameworks, including APRA CPS 230 and CPS 234, the Privacy Act, and reporting obligations to APRA, ASIC and the OAIC. This is particularly acute in the banking and finance sector, where entities are effectively double-regulated and subject to duplicative and, at times, inconsistent incident notification and risk management requirements. A more harmonised approach, including a single government point of contact and aligned notification thresholds, would reduce regulatory burden while improving information quality. The BCA supports the Australian Government's stated intent in the 2023–2030 Australian Cyber Security Strategy to simplify regulatory reporting through a single cyber incident reporting portal. This approach would improve compliance efficiency and enable entities to focus on managing incidents.

Finally, the Commonwealth's "step-in" powers remain unclear, including the specific scenarios or triggers for their use and how such interventions would be operationalised in practice. Greater transparency on these powers (including more guidance on scenarios in which step-in powers may be considered) would improve industry confidence and support more effective contingency planning.

Question 4: Are there new or emergent threats the SOCI Act is unable to manage in its current form?

The Act primarily treats assets in isolation. Greater consideration should be given to systemic and concentration risks across shared supply chains and service providers. Addressing these collective dependencies would strengthen national resilience and better reflect the contemporary threat environment.

Thank you for the opportunity to contribute to this important review.

Yours sincerely,

[redacted]

[redacted]

[redacted]

Business Council of Australia