www.cisolens.com

22 December 2025

Dr Jill Slay AM
Independent Reviewer

Dear Dr Slay AM

Submission to the Independent Review of the Security of Critical Infrastructure Act 2018

CISO Lens welcomes the opportunity to make a submission to the Independent Review into the operation of the SOCI Act. CISO Lens is a strategic information sharing and analysis community that fosters collaboration among cyber security executives and operational leaders from Australia's largest and most complex organisations. Our mission is to help our members deliver outstanding security outcomes for their organisations and the communities they serve. We hold a deep understanding of the cyber security risks, issues, and opportunities they face, and advocate for greater collaboration between government and the private sector to improve Australia's cyber security posture.

Collectively, our member organisations:

- Represent about 54 per cent of the market cap value of the ASX All Ordinaries index.
- Employ more than 1.5 million people, mostly based in Australia.
- Operated with a combined annual security budget of more than $2.7 billion in FY24.
- Are responsible for between 35-40 per cent of security spend in the Australia / New Zealand region.

More than half of our member organisations are regulated entities under the SOCI Act. To inform this submission, we consulted these members to gather their insights into how the Act operates. As requested, their feedback is set out below in response to the four questions you posed.

Please contact me directly via [redacted] if you would like to discuss any aspect of this submission.

Yours truly,

[redacted]

[redacted]

RESPONSE TO THE INDEPENDENT REVIEW QUESTIONS

Is the SOCI Act achieving its objectives ?

Our members consistently expressed the view that the SOCI Act is achieving its intended objectives of strengthening the security and resilience of Australia's critical infrastructure. There is broad support for the Act's purpose and direction, with one member capturing this sentiment succinctly: *"The SOCI Act is good for Australia."*

Is the SOCI Act functioning as intended ?

Our members view the SOCI Act as having a sound and valid intent, with control sets that remain correct and relevant.

The SOCI Act has provided a common framework for organisations to work toward, helping to drive greater focus, prioritisation and investment in cyber security across the business. For many, it has also supported a deeper and more structured understanding of their operating environment and associated risks.

Importantly, members value the flexibility built into the SOCI Act, particularly its recognition of different cyber security maturity models rather than prescribing a single approach that may not suit all risk profiles or operating contexts.

SOCI has also provided a clear regulatory imperative that helps elevate cyber security to the level of attention it requires at executive and board level, supporting more informed decision-making and sustained organisational focus.

Is the SOCI Act having any unintended consequences ?

Feedback from members at small to mid-sized regulated entities highlights the challenges of implementing SOCI Act requirements within constrained budgets. While the Act has elevated the profile and organisational priority of cyber security, particularly through increased board oversight of Critical Infrastructure Risk Management Plans (CIRMPs), this heightened focus has not always been accompanied by the additional funding required to deliver these programs effectively. As a result, some security leaders are struggling to meet their SOCI Act obligations while also progressing other critical, but non-regulated, elements of their security programs, such as the secure adoption and use of artificial intelligence.

Noting these budget pressures, some members indicated that any future reforms imposing additional obligations may require associated costs to be passed on to consumers

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

Our members are increasingly concerned about the growing risk of supply chain compromise and disruption. They note the rising frequency with which attackers, particularly hostile foreign state actors and their proxies, are targeting suppliers of essential goods and services, as well as upstream manufacturers of widely used IT hardware and software. In this context, members see opportunities to strengthen the SOCI Act to better support the management of supply chain security and resilience risk.

Members indicate the current rules are useful in helping organisations develop a stronger understanding of supply chain risk. Through their application, regulated entities have gained deeper visibility into their supplier networks, their dependencies, and their exposure to service disruption. However, while these insights are valuable, members report they have not translated into material improvements in supply chain security and resilience overall. In particular, members are concerned the current regulatory approach places the primary burden on regulated entities, without imposing sufficient responsibility on the organisations that supply them with critical goods and services. This leaves regulated entities with limited levers to drive meaningful uplift across their supplier networks.

Members characterise the current model as one of "security via contract management" and argue it would be more effective if greater—and more explicit—responsibility were placed on suppliers themselves. As one member responsible for security and resilience at a major critical infrastructure organisation observed:

> *"We ask all our suppliers to complete a questionnaire to help identify and assess security and resilience risks. The challenge with this is two-fold. First, it is extremely difficult to verify the accuracy of the responses we receive, noting that some large multinationals simply refuse to participate. Second, where we identify material risks, we have very few levers to force change. We can attempt to impose additional contractual controls, but these can be costly and difficult to enforce, and in extreme cases we may seek an alternative supplier—but this is impractical in very small or niche markets. I would like to see SOCI obligations explicitly cover both critical infrastructure organisations and their suppliers, creating a shared legal obligation for security and resilience. We need to address this problem from both ends; meaningful change will not occur until suppliers are also required to do better."*

In response, members propose that the SOCI Act place greater legal responsibility on the organisations that supply goods and services to regulated entities, requiring them to ensure the security and resilience of those goods and services and to support assurance over the effectiveness of relevant controls. Members acknowledge the complexity of such an approach and its potential regulatory impact on the wider market, but note its capacity to drive substantial and durable uplift in security and resilience across the broader economy.

[Submission ends]