Australian Institute of Company Directors

[redacted]

23 December 2025

Dr Jill Slay AM
Independent Reviewer

Dear Dr Slay

Independent Review of the Security of Critical Infrastructure Act 2018

Thank you for the opportunity to contribute to the independent review of the *Security of Critical Infrastructure Act 2018* (**SOCI Act**)(**the Review**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of more than 53,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits (**NFPs**), large and small and medium enterprises and the government sector.

The AICD has in recent years engaged extensively on Government consultations and proposed reforms in the cyber security and data management policy areas, including submissions on the *Cyber Security Act 2024* (**CS Act**), the development of the 2023-2030 Australian Cyber Security Strategy, amendments to the SOCI Act and reform of the *Privacy Act 1988* (**Privacy Act**).

We have also supported directors to improve their knowledge of cyber security and data governance better practice through extensive publicly available guidance materials, including the *Cyber Security Governance Principles* (**Principles**), *Governing Through a Cyber Crisis* and the *Data Governance Foundations for Boards* publications. We acknowledge the valuable engagement and support of Home Affairs and Australian Signals Directorate in the development of those publications.

1. Executive Summary

The AICD welcomes the Review as a critical opportunity to assess the effectiveness of the SOCI Act.

The SOCI Act has been an important legislative framework in promoting critical asset entities to take proactive steps to address material risks and hazards. We consider the regime has contributed to a strengthening of the operational resilience of critical assets to the benefit of the Australian economy and society.

However, the regime is relatively new and has undergone significant amendment and a broadening of scope since it commenced, with new layers of compliance and complexity. We do not consider there is a strong policy case at this stage for further expansion of the regime's scope or regulatory obligations. We recommend that the focus should be on improving understanding and awareness of the existing obligations and reducing existing complexity through:

- Targeted drafting changes to reduce the uncertainty and complexity of interpreting the core obligations;
- Proactive steps to reduce overlap with other legislative frameworks, including reporting and notification obligations;
- Expanded Cyber and Infrastructure Security Centre (**CISC**) guidance and awareness building to assist entities, management and boards understand and meet the obligations; and
- Consideration of how entities can be supported to manage and oversee systemic risks in digital supply chains.

1. Is the SOCI Act achieving its intended objectives?

We consider the SOCI Act has been a contributing factor in critical asset entities improving risk management practices to identify and mitigate material hazards. In an environment of evolving digital, physical, natural and geopolitical risks there is significant value in Australia having a standalone legislative framework applying to critical asset entities.

Our observation is there has been a significant increase in board attention at SOCI entities to the oversight of material organisational risks, particular cyber security and data governance risks. This attention has been matched with support for capital and operational investments to enhance resilience. This has been a profound change that has been driven both by regulation, including the SOCI Act, but importantly, enhanced awareness of the significant financial, operational and reputation impacts that have resulted from prominent cyber and data incidents in Australia.

The SOCI Act has undergone a number of material changes since the regime commenced in 2018 to reflect an evolving threat landscape, most recently with the passage of the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* in November 2024. The number of entities and industries that are captured has increased significantly as have the obligations on responsible entities, for example establishing and keeping up-to-date a critical infrastructure risk management program (**CIRMP**). Notably, the regime now covers various participants in a critical infrastructure supply chain, in "responsible entities", "reporting entities", "direct interest holders", "managed service providers" and "operators".

We have heard from stakeholders that, as a result of these changes, the SOCI Act is a challenging and complex legislative framework to comply with. This has prompted a compliance-focused culture where many entities rely on external legal advice to understand, and meet, the obligations, particularly CIRMP requirements.

Our strong view is that legislation, and supporting guidance, should not be of such complexity and uncertainty that an organisation is largely reliant on external advice. This dynamic can pose challenges for small and medium sized entities under the SOCI Act that may not have sufficient resources to turn to costly legal advice to meet the requirements. There is also a danger when focusing on narrow compliance, as guided by external advice, that the broader intent of the legislation is missed, in this case a proactive assessment of hazards and taking steps to mitigate the hazards.

As outlined further below, we recommend a number of limited changes to the SOCI Act and see a greater role for Home Affairs in developing guidance on the legislation. However, we are not satisfied that there are any structural deficiencies with the SOCI Act regime that require another round of material amendments or expansion. There is a danger that regular piecemeal reform of a complex regime, such as the SOCI Act, will be counterproductive as entities are overwhelmed by new compliance obligations and the cost of meeting the obligations outweigh any estimated benefits.

2. Is the SOCI Act functioning as intended?

As discussed above, we consider that broadly the SOCI Act is achieving its objectives notwithstanding the complexity of the legislation and a reliance on external advice to meet the core obligations.

We note that the implementation of the SOCI Act and its subsequent various rounds of amendments have not occurred in a legislative and regulatory vacuum. In the past year alone, in addition to amendments to the SOCI Act, there have been significant changes to the *Privacy Act 1988*, the introduction of the *Cyber Security Act 2024* and for Australian Prudential Regulation Authority (**APRA**) regulated entities, the commencement of *CPS 230 Operational Risk Management* (**CPS 230**). At the same time, the Office of the Australian Information Commissioner, APRA and the Australian Securities and Investments Commission have increased enforcement activity associated with risk management failings, including cyber and data breaches.

Many SOCI entities will be subject to multiple, sometimes duplicative, regulatory frameworks that are seeking to strengthen risk management practices. For example, and as discussed below, APRA regulated entities, face several risk management obligations that are intended drive improvements in operational resilience. Given this environment, it is difficult to isolate the impact of the SOCI Act, and the supporting system of national significance framework, in driving improvements in critical asset resilience.

We caution against any calls for further significant reform of the SOCI Act absent a rigorous policy case that clearly highlights that the benefits outweigh further compliance costs, including that demonstrating that existing frameworks are deficient. We highlight recent AICD research by Mandala Partners on federal regulatory accumulation and the key finding that the cost of complying with federal regulation alone has climbed from 4.2% of GDP in 2013 to 5.8% in 2024 ($65 billion to $159 billion). This cost increase has been driven, in-part, by exponential growth in new primary and delegated regulation over the past two decades with limited efforts to reform the stock of existing regulation. The research highlights that there are genuine questions whether this increased cost and its impact on organisational productivity and investment has been justified through welfare enhancements to the Australian community.

Given Australia's significant productivity challenges and the role increasing regulation has played in this our view is that the current focus on the SOCI Act should be on resolving uncertainty and complexity in the primary legislation and supporting interpretation with comprehensive guidance.

Definitions and notification requirements

Entities are required in the annual report under section 30AC to provide details on any hazards that had a 'significant relevant impact' during the period. The legislation does not define 'significant relevant impact', rather it defines 'significant impact' in respect of cyber security incidents under section 30BEA and also 'relevant impact' for other hazards under section 8G. We understand that the broad definition of 'relevant impact' (e.g. any impact to availability) is resulting in entities including excessive detail on incidents that had no material impact on the integrity and reliability of an asset due to an abundance of caution. We recommend that the Review consider where this terminology can be standardised as a practical step to improving interpretation and reducing a reliance on external advice.

We have also received feedback that the definition of 'business critical data' under section 5 is being interpreted in an overly broad manner and capturing data that is not essential to the operation of the asset. This definition has flow-on effects to what 'data storage systems' are caught under the regime. We recommend this definition be reconsidered and/or guidance issued that clarifies the intent of what should be captured.

Lastly, there is a policy case to harmonise the notification and reporting of significant cyber security and all other hazards incidents. Currently a cyber incident has distinct notification obligations to other hazard

incidents (e.g. a bush fire). A consistent approach to how an entity notifies CISC and the Australian Signals Directorate (**ASD**) may provide clarity to entities and reduce confusion during the immediate response phases to an incident.

Guidance and thematic reviews

We recommend that CISC consider how it can further support entities in meeting the SOCI Act obligations, including through further training and awareness raising. In particular we see value in CISC issuing additional guidance on what constitutes better practice in respect of a CIRMP, including expectations for the annual attestation by the board that the CIRMP is 'up to date'.

This guidance may be informed by thematic reviews where CISC examines a sample of entity annual reports and supporting information to reach a comprehensive view on what 'good looks like'. Guidance on better practice CIRMP processes, including board oversight, would be a valuable contribution to driving overall industry risk management improvement and assist in understanding when a CIRMP will be determined to be deficient under the recent reforms

3. Is the SOCI Act having any unintended consequences?

The AICD has consistently received feedback from directors on the existing complexity and overlapping nature of cyber security, risk management and data governance regulatory obligations in Australia. As reflected above, we are supportive of the objective and operation of the SOCI Act, however a clear-eyed review of the legislation should recognise the legislation has caused regulatory complexity.

Directors report that this complexity has increased with amendments to the SOCI Act, more prescriptive and onerous APRA prudential requirements, amendments to the Privacy Act and the introduction of the CS Act. Reporting and notification requirements, data retention obligations, risk management obligations and expectations as well as roles of key regulators are areas raised as requiring streamlining and harmonisation. This complexity extends across both federal and state legislation, general obligations and industry specific.

Cyber, digital and data reporting and notification requirements at both a federal and state level are a particular pain point. We recognise the work done by the Government in establishing a single reporting portal at cyber.gov.au. This an important step in providing visibility to businesses in meeting multiple reporting obligations. However, it does not address the underlying issue that a business in many cases has to report the same incident to multiple regulators via multiple different mechanisms.

Further, this problem was compounded last year with the introduction of the ransomware payment reporting requirement. An entity that has made a payment has to make a report under section 27 of the CS Act in addition to meeting other obligations, for example SOCI Act and Notifiable Data Breaches scheme reports. Our strong view is that this was a missed opportunity to signal the Government's commitment to harmonisation of reporting, for instance through allowing SOCI Act entities to report a ransom payment as a component of the broader notification obligations under Part 2B.

We recognise that the SOCI Act is only one component of this broader regulatory complexity. However, we recommend it consider how targeted changes to primary legislation could be a step forward to promote harmonised reporting and notification requirements. For instance, the CIRMP Rules exclude APRA regulated entities recognising they already face specific risk management prudential requirements. Drafting changes could allow an APRA regulated entity to make one report to APRA of a notifiable event under CPS 234 Information Security as this notification would meet the entity's requirements to notify the ASD under the SOCI Act.

A focus on resolving these costly and duplicate requirements would be consistent with the Treasurer's announcement from the Economic Reform Roundtable of a 'tell us once' regulatory reform initiative.[1]

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

Senior directors have in recent months raised with us concerns about concentration risks in digital supply chains. The markets for the supply of key digital services and platforms to Australian organisations can be highly concentrated with only a handful of substitutable global providers. Examples of these markets include cloud storage/hosting, productivity and messaging software, customer relationship management and supply chain management platforms.

A reliability or integrity failure of one these providers inevitably has flow on effects to the SOCI entity and its operation of the critical asset(s). Directors have highlighted recent outages at Amazon Web Services data centres, Salesforce services and the CrowdStrike failure in 2024 as demonstrating the vulnerability of globally systemically important digital providers. These digital supply chain hazards are very challenging for a SOCI entity to mitigate in isolation due to limited options for redundancy and limited bargaining power or leverage with the supplier to incentivise resilience improvements. There may be a role for the Government to play to address this market failure through assisting entities mitigate the hazard in key digital supply chains.

In general, the SOCI Act considers critical assets in isolation. We recommend the Review consider how there can be a greater focus on concentration and systemic risks across digital supply chains in manner that builds national resilience and does not impose further obligations on entities to manage these risks in isolation.

We would be happy to facilitate direct engagement between the Review, CISC and senior directors to discuss this issue.

Next Steps

We hope our submission will be of assistance. If you would like to discuss any aspects further, please contact [redacted], [redacted] at [redacted]

Yours sincerely,

[redacted]

[redacted]

[1] Treasurer media release, *Regulatory reform to reduce red tape and ease burden on businesses*, 5 September 2025, available here.