Australian Institute of Company Directors

Level 12, Tower 3, Darling Park,
201 Sussex Street,
Sydney NSW 2000

1300 739 119
contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

31 July 2026

Department of Home Affairs
Langton Cres
Parkes ACT 2600

Via online form

Dear Home Affairs

Streamlining and Modernising the *Security of Critical Infrastructure Act 2018*

Thank you for the opportunity to provide a submission to the consultation paper on streamlining and modernising the *Security of Critical Infrastructure Act 2018* (**SOCI Act**).

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 54,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits (**NFPs**), large and small and medium enterprises (**SMEs**) 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. This engagement includes submissions on the 2026 consultation on SOCI Act Ministerial directions powers, the independent review of the SOCI Act, the *Cyber Security Act 2024*, the development of the 2023-2030 Australian Cyber Security Strategy, and amendments *Privacy Act 1988*.[1]

We have also supported directors to improve their knowledge of cyber security and data governance best practice through extensive guidance materials, including the *Cyber Security Governance Principles* (**the Principles**), *Governing Through a Cyber Crisis*, *Data Governance Foundations for Boards* and a joint publications with the Australian Signals Directorate (**ASD**) cyber security priorities for boards in 2025/26 and a forthcoming resource on board oversight of frontier artificial intelligence (**AI**) threats.

1. Executive Summary

The SOCI Act is an important legislative framework in requiring critical asset entities, and their boards, to take proactive steps to address material risks and hazards. The regime has contributed to a strengthening of the operational resilience of critical asset entities to the benefit of the Australian economy and society.

The AICD has received consistent feedback from directors of entities covered by the SOCI Act that the legislation has elevated a focus at senior management and board level on mitigating hazards relevant to critical assets. We recognise that given the recommendations of the independent review there is a strong policy case to reform the regime, including to reduce complexity and overlap with other frameworks.

[1] AICD submission, Independent Review of the SOCI Act, January 2026, available here.

However, we caution against introducing extensive new prescriptive requirements that will ultimately only further entrench a compliance focused mindset rather than an outcomes-based model that seeks to build resilience and address asset hazards.

Building and sustaining the resilience of Australia's critical infrastructure and assets requires a genuine partnership between government and industry. A partnership approach recognises that many of the most significant risks, including cyber threats and supply chain vulnerabilities, are shared challenges that are beyond the domain of individual entities to comprehensively control.

Given the breadth of the consultation paper and the number of proposed measures we have focused on those relevant to the role of the board and which have been informed by consultation with legal experts and members on this and previous consultations.

Our key points are as follows:

- **Measure 1 Exemptions Framework:** We support the development of a clearer and more flexible exemptions framework for entities, or classes of entities, already subject to equivalent regulatory requirements. To maximise clarity and reduce administrative complexity, we recommend that exemptions — particularly in respect of critical infrastructure risk management program (**CIRMP**) obligations — preserve the 'all or nothing' approach where possible, rather than creating fragmented or piecemeal compliance requirements and outcomes.
- **Measure 15 CIRMP Governance and External Assurance:** We support in-principle a proportionate obligation for a CIRMP to be subject to periodic independent assurance. We recommend that any assurance requirement remain principles-based, with boards retaining discretion to determine the appropriate scope and method of review having regard to the nature of critical assets, entity size, complexity and risk profile.
- **Measure 16 – Graduated Civil Penalty Settings:** We support in-principle the introduction of graduated civil penalty settings, provided they are implemented in a measured and proportionate way. The AICD does not consider that an aggressive enforcement posture would be appropriate given the complexity of the SOCI Act, the multiple iterations and changes made to the regime in recent years, and the further changes contemplated in these reforms. We recommend that the Cyber Infrastructure Security Centre (**CISC**) continues to take a facilitative approach focused on education, awareness raising and better-practice guidance, with penalties reserved for serious, reckless, repeated or systemic non-compliance.
- **Measure 19 – Supply Chain Cyber Security Assurance:** We support greater focus by both regulated entities and government on strengthening resilience across key digital supply chains. However, we caution against placing responsibility for supply chain resilience solely on SOCI entities, particularly where risks arise from highly concentrated global digital markets or from suppliers over which entities have limited visibility, leverage or contractual bargaining power. Any new supply chain cyber security assurance obligation should include an "as far as reasonably practicable" overlay, a clear materiality framework, and practical limits around sub-tier dependencies.
- **Regulatory costs –** We recommend Home Affairs assess the cumulative regulatory costs of the reform package as a whole, rather than considering each proposed measure in isolation. The package would impose significant new costs on all entities, including in respect of supplier due diligence and contractual review. This assessment should be published.

2. Measure 1 – Exemptions Framework

The AICD strongly supports the development of a clearer and flexible exemptions framework for an entity, or class of entities, that is already subject to equivalent regulatory requirements

The consultation paper correctly identifies duplication and overlap with other regulatory frameworks as a key concern raised by industry and stakeholders. Regulatory duplication across many sectors and frameworks is consistently raised by AICD members as a significant source of regulatory burden and compliance cost.

We recommend that the framework is simple and clear in its application. A strong advantage of the current CIRMP exemption provisions is that it is 'all or nothing' and in doing so provides clarity to entities. As proposed in the consultation paper, and in the accompanying worked example, the framework could run the risk of being overly complex and convoluted. For example, a transport company may receive an exemption from certain elements of the CIRMP obligations due to existing transport sector requirements but will still be required to meet other CIRMP obligations, such as addressing cyber security hazards.

We are not satisfied that fragmented or piecemeal compliance with CIRMP requirements will result in meaningful compliance saving benefits to the entity. It may ultimately increase uncertainty about which regulatory requirements an entity is meant to comply with as they try to understand and interpret obligations across different frameworks. It may also be difficult for CISC to administer. Where possible, we consider that in respect of CIRMP obligations that the exemptions framework should preserve the 'all or nothing' model.

We note that currently APRA regulated entities are exempt from meeting the CIRMP requirements. Our strong view is that this exemption should be preserved given the comprehensiveness of prudential obligations under prudential standards CPS 230 Operational Risk Management (**CPS 230**) and CPS 234 Information Security and the direct overlap with CIRMP requirements.

It is unclear from the paper whether exemptions would be granted upon application or would be proactively granted by CISC. For efficiency, we recommend that CISC proactively grant exemptions based on its assessment of equivalent regulatory frameworks. This administrative process would be supported by awareness raising amongst impacted entities.

3. Measure 15 – CIRMP Governance and External Assurance

The AICD supports in-principle a proportionate obligation that CIRMPs are subject to periodic independent assurance.

Feedback from our members is that the current self-attestation process is taken seriously by boards and has elevated a focus on the rigour and resilience of critical asset risk controls. We recognise though that external advice and assurance is an important element of strengthening risk controls, particularly cyber security and data governance controls. AICD publications, including the Principles, reflect the value of external assurance to effective governance and the board testing controls. We also understand that for larger entities that it is common for some form of external assurance to currently occur in respect of a CIRMP and broader SOCI Act obligations.

We support the assurance obligations being principles-based and that prescription on the focus and nature of the assurance program is avoided where possible. We recommend the following:

- The board retains discretion to determine the scope and method of the review having regard to the nature of critical assets, size, complexity and risk profile of the entity;
- For larger, more complex and higher-risk entities (e.g. Systems of National Significance) the review should be conducted at least every three years by an external independent reviewer and more frequently if the nature of the asset profile or risk profile has materially changed; and
- For smaller entities with a lower risk profile the review should be conducted at least every three years by internal audit/operationally independent assurance functions or an external independent reviewer.

The consultation paper indicates that SOCI Act Rules may be used to specify reviewer capability, conflicts of interest, report formats and assurance models. We do not support prescription through the Rules given it may result in a narrow, compliance focused exercise that reduces the utility to the entity's board. For boards, a key feature of effective assurance is where it can reflect, and adapt to, the unique circumstances of the entity and the particular risks it may face.

We do though support comprehensive guidance on key elements of the assurance obligations, including reviewer capability and assurance models.

APRA prudential requirements may represent an appropriate model for the framing and drafting of these new requirements. We refer to CPS 220 Risk Management and the principles-based obligations for review of the risk

management framework.[2] APRA prudential practice guide CPG 220 Risk Management also is a model for valuable guidance on independent reviews of risk controls.[3]

4. Measure 16 – Graduated Civil Penalty Settings

The AICD is supportive in-principle of the proposed graduated civil penalty settings in the consultation paper. An appropriate enforcement approach supported by measured penalties is a component of an effective regulatory regime. However, we recommend a measured and proportionate approach given the material changes and complexity of the regime. We also urge consideration of the role of CISC and its resourcing given the proposed expansion of the SOCI Act with a strong focus on accountability.

We recognise that the independent review identified concerns that the current enforcement posture may not sufficiently incentivise effective risk management and accountability and there has been a perception that the regime is 'toothless'. We do not share this view. Consistent feedback from our members is that the SOCI Act has prompted a step change in the risk management practices of entities subject to the regime. Board focus on the SOCI Act and entity CIRMPs has been elevated by the annual attestation.

While the SOCI Act has been in place for eight years it has undergone four sets of significant reforms, including new asset sectors and the introduction of CIRMP obligations in 2022. The regime has consistently evolved and with it the complexity has increased as recognised in the independent review. Entities have struggled to understand the obligations and have relied on external advisers to navigate the framework.

The consultation paper contemplates further significant reform that would reshape many obligations and bring further compliance challenges for entities. Given this dynamic our strong view is that an aggressive enforcement posture is not appropriate as it is likely many breaches will be inadvertent and administrative in nature. We support CISC taking a facilitative approach to breaches with the focus continuing to be on education and awareness raising with penalties reserved for serious, reckless and repeat/systemic non-compliance.

An overly punitive framework and approach to enforcement also risks discouraging transparency and cooperation between industry and government.

Enforcement and the role of CISC

The consultation paper is largely silent on the role of CISC. We support greater resources for CISC, particularly if there will be a greater expectation for enforcement activity.

We strongly support CISC continuing to raise awareness of the SOCI Act and working with entities to understand the core obligations and what better practice looks like.

We see value in CISC issuing additional guidance on what constitutes better practice in respect of developing and updating 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 audits a sample of entity reports and supporting information.

Guidance on better practice CIRMP processes, including board oversight, would be a valuable contribution to driving overall industry risk management and governance practice. Further, it may reduce the necessity of entities to rely on external firms to meet core SOCI Act obligations and the corresponding costs of compliance.

5. Measure 19 – Supply Chain Cyber Security Assurance

The AICD supports greater focus by both SOCI entities and government on building resilience across key digital supply chains. However, we caution against a policy approach that places responsibility for addressing risks in supply chains solely with entities.

Senior directors of entities subject to the SOCI Act have noted the significant concentration risks in digital supply chains. The markets for supply of key digital services and platforms to large Australian organisations can be highly concentrated with only a handful of substitutable global providers or hyper scalers. A reliability or integrity failure at a key provider (e.g. cloud computing provider) can have significant flow on effects to the business operations of the

[2] CPS 220 Risk Management, paragraphs 44 – 48.
[3] CPG 220 Risk Management, paragraphs 83 – 92.

company. The vulnerability of systemically important digital providers was highlighted by the CrowdStrike failure in 2024.

These digital supply chain hazards are very challenging for a company to mitigate in isolation due to limited options for redundancy and reduced bargaining power or leverage with the supplier to incentivise resilience improvements. Enhanced obligations should recognise these practical limitations and avoid creating obligations that effectively require entities to guarantee the security posture of external suppliers.

In particular, we are concerned with the framing of contractual measures in the consultation paper as 'responsible entities would be expected to address supplier cyber risk through contractual or equivalent measures'. As the consultation paper indicates this may not be possible for many entities, particularly those of a smaller size or with relatively limited bargaining power. In the case of 'hyper scalers' all Australian entities have limited bargaining power and often accept standard terms and conditions.

We strongly support a 'as far as reasonably practicable' overlay to the obligation to reflect this dynamic. This appears to be contemplated in the consultation paper.

Our other recommendations are:

- Clarity on requirements to address risks with 'sub-tier dependencies'. It is very challenging for a SOCI entity to have visibility of risks in tiers below the immediate vendor, let alone direct or influence resilience changes in companies that the entity does not directly contract with. Measure 19 should avoid obligations or expectations that are simply impractical or borderline impossible for an entity to meet.
- The proposal is limited to 'cyber risk'. The common understanding of this term is generally limited to unauthorised access or compromise of systems or data. Our interpretation of Measure 19 is that it is intended to capture a broader hardening of supply chain resilience, including covering digital infrastructure and systems outages and faults (i.e. not solely the result of threat actors). We recommend this intent is clarified.
- A clear materiality framework where an entity is only required to meet this elevated supply chain obligation for suppliers that are essential or critical to the entity's operations and resilience of the asset(s). We also support guidance that an entity is not expected to meet these obligations in respect common or widely used software-as-a-service products. For example, Microsoft productivity software is essential to many Australian businesses, however we question the utility of requiring a SOCI entity in isolation to attempt to negotiate with Microsoft on the security settings of this software.
- An appropriate transition period. Discussed further below.

Board oversight of supply chains

Senior directors have raised with the AICD the significant challenges in having confidence in the resilience of key suppliers and the great difficulty in attesting annually that a CIRMP is 'up to date' given this uncertainty. Directors have noted that visibility of supplier resilience, let alone directing improvements, is in most cases outside the span of the control of the entity.

Measure 19 may make it more challenging for boards to review a CIRMP and attest that it is effective (i.e. 'up to date'). As stressed above, we strongly support a 'as far as reasonably practicable' overlay. We also recommend that Home Affairs consider how the attestation obligation can be reframed to reflect the reality that mitigating hazards associated with suppliers is very challenging.

At a minimum, we support comprehensive guidance from CISC on how boards can oversee key supply chain risk controls when assessing the CIRMP and reaching a view on its effectiveness.

Government industry partnership model

Reflecting strong member feedback we consider there is an important role for Home Affairs and government more broadly in building resilience across key digital supply chains. This is an issue that industry cannot be expected, or required, to tackle alone given the importance to broader national resilience and security.

A broad industry partnership model has been progressed under the *2023-2030 Australian Cyber Security Strategy* and we consider this may form the template of a similar approach to build digital resilience more generally. A focus solely on more legislation and obligations on entities is likely to produce limited gains.

We recognise that this is a priority area for Home Affairs and that important progress has already been made, including entering a Memorandum of Understanding with Microsoft. We also understand that joint resilience planning occurs to some limited extent in certain industries, including sector/industry mapping and simulation exercises. We support further expansion of these activities and a prioritisation of agreements with systemically important international providers.

The AICD welcomes further engagement with Home Affairs in this area.

CPS 230 implementation and transition

As Home Affairs is aware the APRA regulated population has undergone a significant risk and resilience uplift to comply with CPS 230 obligations. Measure 19 has parallels with prudential requirements that APRA put in place under CPS 230 and we encourage close collaboration with APRA to inform the drafting of this requirement and implementation.

Feedback from directors of APRA entities has been that implementation was a significant exercise that incurred high costs for all entities. An extended implementation and transition period was essential to meeting the new obligations and managing entity costs and resourcing. The APRA implementation timeframe was:

- Finalisation of CPS 230 in July 2023;
- Commencement for large entities in July 2025 and for small entities in July 2026;
- Transition for all entities up to the earlier of the next contract renewal date or 1 July 2026.

In effect entities had up to three years to meet the new obligations reflecting the standard contract term. We strongly recommend that were Measure 19 to be implemented that at least a three-year period for compliance is necessary. Entities should not be expected to break or renegotiate a contract that is already in place and a three-year period aligns with a standard length for most service agreements.

6. Cumulative regulatory costs

The consultation paper largely assesses the regulatory costs and implementation impacts of each proposed measure in isolation. While this approach assists consideration of individual reforms, it risks understating the cumulative burden that regulated entities may face if a significant number of the 21 proposed measures are ultimately adopted.

The package includes a range of proposals that would require significant new compliance costs, including external assurance activities, supplier due diligence and contractual reviews and amendments. Considered individually these obligations may appear proportionate. However, the practical reality is that costs are experienced collectively and should be assessed in totality to understand the true implementation burden.

The Independent Review itself identified concerns regarding regulatory duplication, administrative burden and higher-than-expected compliance costs under the existing SOCI framework.[4]

The AICD has had a long-standing policy position calling for a more rigorous impact analysis for new policy processes across federal government. This position is informed by 2025 AICD Mandala Partners research on regulatory accumulation that found that complying with federal regulation has increased to 5.8% of GDP from 4.2% of GDP in 2013.[5] As noted above, we are in-principle supportive of reforms of the SOCI Act. The proposals will

[4] SOCI Act Independent Review, 2026, Page 40.

[5] AICD Mandala Partners research, *$160 billion and counting: The cost of Commonwealth regulatory complexity*, November 2025, available here.

though add materially to the regulatory costs to entities and should be closely assessed against the estimated benefits.

The AICD strongly encourages Home Affairs to undertake and publish an assessment of the aggregate regulatory costs of the proposals in the consultation paper.

7. Next Steps

We hope our submission will be of assistance. We welcome further engagement with Home Affairs as it works through the complexity of further reform of the SOCI Act.

If you would like to discuss any aspects of our submission further, please contact Simon Mitchell, Acting Head of Policy (smitchell@aicd.com.au).

Yours sincerely,

Louise Petschler GAICD
GM, Education and Policy Leadership