Australian Institute of Company Directors

Level 12, 201 Sussex St
Sydney NSW 2000
t: 1300 739 119
e: contact@aicd.com.au
aicd.com.au
ABN 11 008 484 197

29 August 2025

Department of Home Affairs

Dear Home Affairs

Consultation on Horizon 2 of the *2023-2030 Australian Cyber Security Strategy* – Discussion Paper

Thank you for the opportunity to comment on the Discussion Paper on Horizon 2 of the *2023-2030 Australian Cyber Security Strategy* (**the Strategy**).

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 Strategy, amendments to the *Security of Critical Infrastructure Act 2018* (**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 best practice through extensive guidance materials, including the *Cyber Security Governance Principles* (**Principles**), *Governing Through a Cyber Crisis* and the *Data Governance Foundations for Boards* publications.

1. Executive Summary

The AICD recognises the significant achievements under Horizon One, notably the passage and implementation of the CS Act and amendments to the SOCI Act. Broadly we consider the reforms reflect a partnership approach with industry to building cyber security resilience. The three-year statutory review under section 88 of the CS Act will allow for an assessment of the implementation and efficacy of the reforms.

We are supportive of the focus of Horizon 2 on building the cyber resilience of small and medium sized businesses (**SMBs**) and NFPs. These organisations do face structural barriers to enhancing cyber and data controls associated with their size, competing priorities and limited resources.

The key points in our submission are:

1. SMB and NFP cyber and data resilience

- We support a concentrated and well-resourced campaign to boost the cyber and data resilience of SMBs and NFPs. We recommend this includes expanded guidance, targeted training programs that are differentiated by role (e.g. managers, owners and directors) and

focused on particular sectors and industries, expansion of the Small Business Cyber Resilience Service and micro grants or funding streams for specific NFPs and charities to make targeted cyber investments.

- We support a focus on the key upstream digital providers of SMBs and NFPs, notably managed service providers (**MSPs**) and software as a service (**SaaS**) vendors, for the development of a standard and certification pathway. This reflects how critical these providers are in an SMB digital supply chain and would be a more effective path to building the cyber resilience of SMBs and NFPs than a standard solely focused on small organisations.
- We recommend that Home Affairs undertake a thematic review of the Australian cyber insurance market to comprehensively understand existing market conditions, product design and pricing prior to considering any regulatory interventions.

2. Regulatory complexity

- We do not recommend any further regulatory change to address cyber and data risk weaknesses across the Australian economy. Given the current complexity of cyber and data regulatory obligations and recent significant changes (e.g. introduction of CS Act and amendments to the SOCI Act) any further amendments would be counterproductive and premature. Home Affairs should focus on supporting implementation of recent reforms and addressing ongoing sources of complexity, notable data retention obligations and multiple overlapping reporting requirements. Government should avoid the temptation to continually ratchet up requirements.
- We do not support further amendments to the Privacy Act as a policy or legislative solution to identified weaknesses in cyber security and data resilience of Australian businesses, particularly SMBs. Further reform that only increases the complexity and punitive aspects of the Privacy Act, for instance introducing a direct right of action, will undermine the partnership model of the Strategy and the achievements under Horizon One.

3. 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, including cyber security risks. 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. It is appropriate for Home Affairs to continue to support the regime with further guidance, however we strongly recommend that there are no further legislative changes prior to the independent review later in 2025.

2. SMB and NFP cyber and data resilience

This section response to **questions 7 – 13** of the Discussion Paper.

Building the cyber and data resilience of SMBs and NFPs

We agree there is a currently a maturity gap in the cyber and data resilience of SMBs and NFPs as compared to larger well-resourced organisations. The directors and owners of these organisations can often face resourcing constraints and competing priorities that can result in cyber and data risk controls not receiving appropriate attention.

The Government has a role to play in supporting these SMBs and NFPs boost resilience. Weaknesses in cyber resilience at these organisations can undermine broader community trust in digital environments and services and also impact larger businesses through linkages across supply chains. Further, as

discussed below, many NFPs hold sensitive personal information on vulnerable members of the community.

While the Government should be looking at targeted support and guidance, we do not support imposing new regulation on SMBs and NFPs. As discussed below in respect of regulatory complexity, our strong view is that removing the small business exemption to the Privacy Act would do little to improve data and cyber resilience at these organisations.

There is no silver bullet to building resilience amongst smaller organisations, rather a concentrated and well-resourced campaign focused on awareness, education and support may over time make a material difference. Additional layering of regulation is not the answer.

We **recommend** Home Affairs give consideration to the following initiatives:

- continue to expand and refresh the Australian Signals Directorate (**ASD**) guidance, including Exercise in a Box and small business focused resources (e.g. a small business version of the Essential Eight);
- assess options to expand existing training programs (e.g. CyberWardens) to target particular sectors or individuals within an SMB, including directors and owners (discussed further below in respect of NFPs);
- expand the Small Business Cyber Resilience Service such that it is available to SMBs and NFPs with greater than 19 employees;
- explore standards and certification pathways based on international experience, such as in Canada and Singapore (discussed further below);
- consider a targeted grants program where NFPs are provided with micro funding to invest in cyber and data enhancements (discussed further below); and
- seek innovative ways to communicate and convey key cyber principles to SMBs and NFPs, including through partnering with industry associations, state-based regulators and key service providers of SMBs.

We **recommend** that expanding guidance materials and training opportunities should be supported by a well-resourced awareness raising campaign targeted at SMBs and NFPs. New sources of training and guidance, such as the ACSC Exercise in the Box program, will have limited uptake and impact if managers, directors and owners of SMBs and NFPs are not aware that they exist.

Focus on digital providers to SMBs and NFPs

Many SMBs and NFPs rely on MSPs and SaaS vendors to supply key digital systems, software and infrastructure. These providers are key elements of the overall cyber and data resilience of smaller organisations and in many cases the SMB or NFP has limited discretion or ability to influence the settings of these key suppliers. We **recommend** that Home Affairs explore how it can incentivise these providers to enhance the security offering to SMBs and NFPs.

We have received feedback that SMBs and NFPs will often obtain cyber security software and controls (e.g. threat blocking, email hygiene, phishing testing) from an MSP as a component of an overall bundled service offering. Stakeholders have noted that in some cases the additional security settings offered by the MSP are not appropriate to the organisation or not effective. This may not become apparent until there is a cyber security event or external assurance reveals shortcomings in the security and data protection offering. We note public comments by the Privacy Commissioner on the cyber and

data weaknesses present amongst some MSPs and other providers and a rise in third party suppliers being a source of data breaches.[1]

Separately, stakeholders have noted that large SaaS providers tier product offerings such that entry licences or subscriptions typically used by SMBs and small NFPs may only have baseline security offerings. For example, the entry product offering will not have MFA turned on. To access enhanced cyber and data protection settings the organisation needs to purchase a higher priced licence or subscription, for example an 'enterprise' tier. With limited staff and financial resources it is often not feasible to pay significantly more for SaaS offerings.

We consider that there may be an opportunity for the development of a standard and supporting certification directed at the MSP and SaaS levels of the supply chain. This standard and certification could be designed in a manner that promotes the offering of more comprehensive and effective cyber controls as a part of standard/entry offerings for SMBs and NFPs. Further, it would signal to SMBs and NFPs which providers are meeting baseline security settings and as such provide a competitive advantage to providers that hold the certification. Lastly, the Government could further promote uptake through making certification a condition of tendering for certain government digital contracts.

Given the ubiquity of outsourcing digital systems and infrastructure amongst SMBs and NFPs a standards and certification approach focused on the key providers may be more effective than one that targets small organisations themselves.

NFP challenges and opportunities

Directors of NFPs are very aware that their organisations often hold sensitive information that presents heightened data risks, for example on vulnerable members of the community. However, as noted in the Discussion Paper, many NFPs face resource constraints that can limit their ability to build cyber and data resilience. These resourcing constraints share similarities to SMBs, for example not having dedicated IT staff. Additionally, NFPs and charities can often face uncertainty about future funding, whether that be from private funders or Government programs. Uncertainty about the medium to long term financial stability of an NFP can translate into a board and management being hesitant to make significant capital investments into new digital and data technology, including greater cyber protections.

An additional key difference to SMBs is that at NFPs there is often a reliance on volunteers to undertake key operations and provide services to clients. This dimension means that it can be difficult to promote features of a cyber resilient culture, for example email hygiene, mandatory training and strong password/key practices. A predominantly volunteer workforce may be more likely to take shortcuts in data entry practices or systems access, for example, to expediate offering services to clients.

We **recommend** Home Affairs consider the following options for tailored and cost-effective assistance for NFPs:

1. Explore opportunities with the ASD, Australian Charities and Not-for-profits Commission (**ACNC**) and state based regulatory bodies to develop and communicate industry specific better practice cyber and data guidance to NFPs and charities. The ACNC in July 2025 released findings of its cyber review of a small sample of charities. This is a welcome first step. We support a broader campaign of guidance material, particularly focused at practical operational improvements, and tailored for particular sectors or industries. Guidance of a general nature may limit its traction as opposed to materials that are focused on a particular industry or segment of NFPs, for example NFPs providing

[1] The Guardian, 'Third-party providers a customer data 'weak spot', Australian privacy commissioner says', 6 May 2024.

schooling or education. Such a program could be supported through collaboration with industry representative bodies.

2. Consistent with our recommendation above in respect of SMBs, we consider that Home Affairs should assess the potential for tailored training programs for directors and managers of NFPs and charities on cyber and data protection controls and governance. This would extend beyond the existing CyberWardens program and be specifically tailored for managers and directors in particular sectors or industries, such as care or education. Tailored, industry specific programs, that are freely available may get greater traction with key individuals at these organisations than broader education offerings.

3. As noted above, we recommend expansion of the Small Business Cyber Resilience Service to SMBs and NFPs with greater than 19 employees. Many NFPs above this arbitrary employee threshold face resourcing and budget constraints and would benefit from targeted advice.

4. We note the *Cyber Security Awareness Support for Vulnerable Groups* program and the corresponding $7 million funding. Subject to an assessment of the effectiveness of the first round of grants we encourage Home Affairs to consider whether this program should be expanded, including beyond cyber literacy programs. As noted above, many NFPs face significant financial challenges. An expansion of this program, including to provide funding or micro grants to directly support NFPs to improve their organisational cyber resilience, could be practical step of improving cyber security practices at particular organisations and sectors.

The AICD would welcome the opportunity to directly engage with Home Affairs on how we can assist in reaching NFP and SMB directors with tailored cyber security guidance.

Cyber security standards for small businesses and not for profits

We are supportive of Home Affairs exploring the development of a cyber security standard focused on the needs of small organisations. We agree that SMBs and NFPs can struggle with existing frameworks, such as ISO 27001, as they are drafted in a manner that is appropriate for large organisations with dedicated IT teams. However, as detailed above, our view is that a standard for MSPs and SaaS providers may be more effective than one for solely SMBs and NFPs.

The AICD has sought to support directors of smaller organisations in building cyber and data resilience through tailored guidance, including checklists of the *Principles* and *Data Governance Foundations for Boards*. Separately, in May 2024 we published the *Cyber Security Handbook for Small Business and Not-for-Profit Directors* in partnership with the Australian Information Security Association.

Our experience developing these publications is that there can be challenges in reaching the directors, owners and managers of SMBs. These individuals are time poor, resource constrained and have a long list of competing priorities. Prior to commencing work on a standard, including a potential certification pathway, Home Affairs should understand how it will raise awareness of such a standard and promote uptake.

Further, key questions we encourage Home Affairs to consider in assessing the need for an SMB and NFP cyber security standard include:

- How any standard would be differentiated or distinct from existing guidance that is targeted at small organisations (e.g. ASD Small Business Cybersecurity Guide)?

- How will the standard align, or be compatible with, international standards and the Essential Eight?

- How will the standard reflect the technical reality that many SMBs and NFPs rely on MSP and SaaS providers for key digital services provision and don't have the ability to influence or alter the security settings of these providers?

- How will the standard reflect the reality that at SMBs and NFPs cyber security is not a neatly delineated risk area but rather overlaps or is interconnected with data and IT practices and the adoption of new technologies (e.g. artificial intelligence)?

- What processes will be put in place to ensure the standard is regularly reviewed and updated to keep it current with broader technological and security control developments?

We note that Singapore, the United Kingdom and Canada have versions of cyber certification programs. We encourage Home Affairs to explore how effective these programs have been, particularly for SMBs.

As discussed above, it may be more effective and efficient to target a standard or certification at entities that provide digital services to SMBs and NFPs, such as MSBs. These providers could obtain certification based on a standard that would provide a degree of confidence to SMBs that the provider was meeting certain baseline cyber settings. In effect the certification reduces the search costs and limited visibility that managers, directors and owners of SMBs have in understanding the cyber and data risk controls of key providers in their supply chain.

We would welcome the opportunity to support Home Affairs' work in considering a SMB and NFP standard, particularly in contributing to components focused on the governance of cyber and data risks.

Access to cyber insurance

We agree that for some organisations cyber insurance can be an important risk mitigant that provides a degree of financial protection in the event of cyber incident. As noted in the Discussion Paper, cyber insurance can also bring benefits in terms of access to external expertise during an incident.

There is limited public data available on the penetration of cyber insurance amongst SMBs and small NFPs. Anecdotally we have been told by industry experts that the majority of large Australian organisations have cyber insurance, however the take-up amongst smaller businesses is far lower. Were this the case, then it would mirror the United Kingdom where recent reporting suggested that only 5 – 10% of small organisations have cyber insurance.[2] This appears consistent with APRA general insurance statistics that indicates that the gross written premiums for cyber insurance are only approximately 15% of the size of premiums for professional indemnity insurance by way of example.[3] While APRA statistics only cover insurance written by APRA regulated entities (i.e. does not include insurance underwritten by Lloyds of London syndicates) they are a proxy for the broader size of the cyber insurance market.

Limited penetration amongst SMBs may be due to the pricing of cyber insurance being prohibitive for smaller organisations and the complexity of the product coverage, including exclusions. We have heard that it can be challenging for SMBs and NFPs to compare insurance products and to understand the breadth of coverage.

Given current information gaps and limited understanding on the cyber insurance market in Australia, we **recommend** that Home Affairs undertake a thematic review of the Australian cyber insurance market to comprehensively understand existing market conditions, product design and pricing. Our view is that a thematic review or study is necessary to establish an evidence base on whether the market is functioning well and the degree of any market failures that limit access, particularly for SMBs. A thematic review

[2] Reinsurance News, 'Cyber insurance premiums stabilise in 2025, but market penetration remains below 10% for SMEs: S&P,' 14 May 2025, available here.

[3] APRA general insurance statistics, financial performance by class of business, December 2024 quarter, available here.

could draw upon existing statistics provided to APRA and market information and intelligence held by large cyber insurance providers and insurance industry associations.

A more detailed picture of the cyber insurance market is necessary before Home Affairs considers any regulatory interventions.

3. Regulatory complexity

This section response to **questions 16 and 17** of the Discussion Paper.

The AICD has consistently received feedback from directors on the existing complexity and overlapping nature of cyber security and data management regulatory obligations in Australia.

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.

Cyber, digital and data requirements at both a federal and state level are characterised by regulatory 'clutter', a phenomenon that is widespread and was highlighted by the Treasurer at the conclusion of the recent Economic Reform Roundtable.

Pause on new regulation

This AICD does not support any new legislation or regulation at this time to address cyber security risks across the Australian economy. Given Australia's current productivity challenges and the recognition by the Government of the burden of regulatory complexity to this problem our view is that contemplating further cyber focused legislative change would be counterproductive. The AICD's submissions to the Productivity Commission's pillars inquiries and separately the Economic Reform Roundtable stress that the heavy weight of regulation is proving to be a significant drag on business investment and productivity.[4]

In the past year there have been significant amendments to the Privacy Act, SOCI Act, the introduction of the CS Act and for APRA regulated entities, the commencement of *CPS 230 Operational Risk Management* (**CPS 230**). At the same time both the Office of the Australian Information Commissioner (**OAIC**) and ASIC have increased enforcement activity associated with cyber risk failings, notably the OAIC recently filing claims against Optus and ASIC taking action against FIIG Securities Limited.

Our observation is that there has been a significant increase in board attention to the oversight of organisational cyber and data risk with corresponding support for capital and operational investments to enhance resilience. This has been a profound change that has been driven both by regulation but importantly enhanced awareness of the significant financial, operational and reputation impacts that have resulted from prominent cyber and data incidents in Australia.

As discussed below, we do not support Home Affairs considering further changes to the SOCI Act prior to an independent review later this year. Making additional amendments to an already complex legislative framework that is still being implemented would be counterproductive. Home Affairs should focus on continuing to support entities meet these obligations and raise awareness of the regime.

[4] AICD submission, Productivity Commission inquiry on the five pillars of productivity – priority reform areas, June 2025, available here; AICD submission, Treasury - Economic Reform Roundtable, July 2025, available here.

We are also strongly of the view, as detailed below, that further legislating changes to the Privacy Act (ie further implementation of the 106 recommendations supported by the Government) would ultimately be damaging to the partnership-based model that has marked the implementation of the Strategy to date.

Reporting

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 (**NDB 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.

We **recommend** that further work is undertaken to harmonise reporting and notification requirements such that that an entity's reporting to different regulators and agencies under different frameworks is consolidated to the greatest extent possible. This focus would be consistent with the Treasurer's announcement from the Economic Reform Roundtable of a 'tell us once' regulatory reform initiative.[5]

Data retention

We also welcome initial steps by the Government to address the current maze of data retention obligations through the Commonwealth Data Retention Review. We understand that this review is at a preliminary stage and is not examining the significant volume of data retention requirements that are at a state and territory level. Allens recently estimated, as a component of the *Data Governance Foundations* publication, that there are over 800 separate data retention requirements across industries and different jurisdictions.[6]

The AICD's view is that data retention complexity is a key contributing factor to entities holding personal information for longer than is necessary, which in turn increases the extent of data loss and potential damage from a significant cyber incident or data breach. Data retention laws are also one of the regulatory barriers to greater uptake of artificial intelligence tools and systems and limit the productivity benefits of these technologies.

We strongly **recommend** that clarifying and consolidating data retention laws be priortised by Home Affairs and the Attorney General's Department as a necessary pre-condition to further changes to the Privacy Act. We also **recommend** that the Government should consider how to incentivise the States and Territories to similarly address their data retention requirements. A principles-based approach that is solely limited to Commonwealth legislation will result in limited gains in addressing the challenge.

Privacy Act

The Privacy Act is a foundational component of the overall mixture of data and cyber security legislation in Australia. APP 11, APP 3 and the NDB Scheme play important roles in setting requirements that incentivise covered entities to appropriately protect personal information. Further, the OAIC through its code-making, guidance and enforcement activities is a key regulator.

---

[5] Treasurer, Press conference: Economic Reform Roundtable, tax, productivity, road user charge, 21 August 2025, available here.

[6] AICD, Allens and Melbourne Business School, Data Governance Foundations for Boards, May 2025, page 58.

However, there are limitations with the scope of the Privacy Act in that it only covers personal information and not broader cyber security and data risks, such operational technology risks, non-personal data compromise and extortion, or digital supply chain and infrastructure risks. Further, as recently found by the Productivity Commission, the Privacy Act is costly and complex to understand and comply with and there is a compliance/control focus rather than one on outcomes.[7]

We note that at the end of 2024 the Government legislated the first tranche of Privacy Act Review reforms, that included a statutory tort for privacy and increased penalty provisions. We understand that the Government is considering a second tranche of reforms that would seek to legislate additional proposals from the Privacy Act Review. We remain very concerned that the direction of the Privacy Act reforms conflicts with the Government's focus on capacity-building and collaboration to build cyber security resilience under the Strategy. We highlight two areas that demonstrate the disconnect:

1. The introduction of a direct right of action, with a low threshold for access and harm, that would allow class actions against businesses associated with a data breach even where the business is found to have met all reasonable steps under APP 11.

2. The removal of the small business exemption. We consider this is an impractical policy proposal that ignores the reality of how limited the resourcing and capacity is of small businesses. Applying the Privacy Act to small businesses will result in no meaningful improvements in cyber and data resilience, and instead introduce a significant new compliance cost to thousands of small businesses.

We do not support further amendments to the Privacy Act as a policy or legislative solution to identified weaknesses in cyber security resilience of Australian businesses, particularly SMBs. We **recommend** that there is greater coordination across Home Affairs and the Attorney's General's Department on the approach to building cyber and data resilience. A focus on partnerships under the Strategy would be undermined if there were corresponding increases in compliance burden and punitive measures in the Privacy Act.

4. Effectiveness of the SOCI Act

This section response to **questions 33 – 36** of the Discussion Paper.

We consider that the SOCI Act has been an important legislative framework in promoting critical asset entities to take proactive steps to address material risks and hazards, including cyber security risks. 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. It is appropriate for Home Affairs to continue to support the regime with further guidance, however we strongly **recommend** that there are no further legislative changes prior to the independent review.

The SOCI Act has undergone a number 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 and that many entities rely on external legal advice to understand, and meet, the obligations.

[7] Productivity Commission, *Interim Report: Harness data and digital technology*, July 2025, pages 54 – 55.

Further, it is unclear if all entities caught under the SOCI Act are aware of the framework and/or the specific obligations. We suspect that particularly amongst small and medium entities that there may continue to be awareness raising challenges.

It is difficult to assess the effectiveness of the SOCI Act, and the supporting system of national significance framework (**SONS**), in driving improvements in cyber security and data resilience. We also note that the implementation of the SOCI Act and the SONS has coincided with a greater regulatory and law enforcement focus on cyber and data resilience, including via changes to industry specific requirements. Notably, feedback from directors of APRA regulated entities has noted that the introduction by APRA of prudential standards *CPS 234 Information Security* and separately *CPS 230* has made a material impact on how financial services entities manage cyber and data risks, and the level of oversight of the board undertaken as a part of the independent review. These broader regulatory changes make it difficult to attribute or isolate the impact of the SOCI Act on cyber and resilience. Our view is that this analysis should appropriately form a component of the broader independent review.

We **recommend** that the Government not consider further changes or amendments to the SOCI Act regime prior to the independent review due at the end of 2025. The independent review is an opportunity to comprehensively assess its effectiveness and areas of challenge and complexity. Further tinkering with the regime prior to this review would be premature and run the real risk of adding to existing complexity and density of SOCI Act obligations.

In the interim, we **recommend** that Home Affairs 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 Home Affairs 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'. Guidance based on Home Affairs intelligence and analysis of CIRMP practices, 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.

5. Next Steps

We hope our submission will be of assistance. If you would like to discuss any aspects further, please contact Simon Mitchell, Senior Policy Adviser at smitchell@aicd.com.au or Christian Gergis, Head of Policy at cgergis@aicd.com.au.

Yours sincerely,

Louise Petschler GAICD
General Manager, Education & Policy Leadership