Australian Institute of Company Directors

18 Jamison Street,
Sydney NSW 2000

t: 1300 739 119
e: contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

6 March 2024

Home Affairs Department

auscyberstrategy@homeaffairs.gov.au

Dear Home Affairs Department (**Department**)

2023–2030 Australian Cyber Security Strategy: Legislative Reforms

Thank you for the opportunity to comment on the consultation paper *2023–2030 Australian Cyber Security Strategy: Legislative Reforms* (**Consultation Paper**) covering proposed standalone cyber security legislation and amendments to 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 51,000 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, including the development of the 2023-2030 Australian Cyber Security Strategy (**Strategy**), previous amendments of the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and reform of the *Privacy Act 1988* (**Privacy Act**). We have also sought to support our membership to improve their knowledge of cyber security better practice through extensive guidance materials and education opportunities, discussed further below.

The AICD's policy positions on the key questions in the Consultation Paper have been informed by engagement with cyber security and legal experts, Australian businesses, industry bodies and AICD members.

1. Executive Summary

The AICD strongly supports the policy objective of the proposed reforms set out in the Consultation Paper and in the broader Strategy. Government and industry working together has the greatest potential to achieve the goal of Australia being a world leader in cyber security by 2030.

As detailed in the submission we support, or in-principle support, almost all of the key reforms and commend the approach the Department has taken to consulting and developing these proposals. AICD members recognise that targeted and low-cost regulatory obligations are appropriate in certain areas, such as ransomware threat intelligence. However, this should be balanced by measures that promote trust between industry and Government, notably through comprehensive protections on how information provided to Government during a critical cyber security incident is used and shared.

Our key points on proposed measures two to eight are as follows:

- **Measure 2**: We in-principle support a ransomware reporting regime applying to large businesses. We recommend the design of the regime minimise duplication with existing reporting and notification obligations, only collect necessary operational information and be based on genuine 'no fault, no liability' principles. We also consider that a $10 million revenue threshold is too low and recommend that the regime apply to all SOCI entities and other businesses with a revenue greater than $50 million.

- **Measure 3**: We strongly support a legislated obligation on the ASD and Cyber Coordinator in respect information provided by an organisation during the response and recovery phases of a significant cyber security incident. We recommend this obligation is expanded beyond 'use' to the 'use, sharing and awareness' of information and separately the cyber security purposes are tightened to provide sufficient comfort to organisations in the rigour of the obligation.

- **Measure 4**: We in-principle support the establishment of a Cyber Incident Review Board (**CIRB**). We recommend that the CIRB is established in a low cost and agile manner that avoids additional regulatory burden and costs on impacted organisations. We also consider its function should encompass thematic cyber security issues and vulnerabilities to preserve a genuine 'no fault' principle.

- **Measure 5**: We in-principle support the proposed approach to clarifying the application of 'business critical data' and data storage systems falling within the scope of the SOCI Act. We support a flexible approach to the definition of 'business critical data' that enables an entity to have discretion of what constitutes 'business critical' based on its unique circumstances, including size, complexity and industry. We also recommend policy coordination to ensure there is not contradictory, or complex overlap with the proposed reforms of the Privacy Act.

- **Measure 6**: We do not support the proposed Ministerial 'consequence management' directions powers. There is not a strong policy case for the new powers, including that existing Ministerial directions powers in the SOCI Act are deficient. In addition, the powers would be inconsistent with the intent of the SOCI Act, unfettered and cover the highly subjective and unclear concept of 'consequence management'.

- **Measure 7**: We support amendments to the protected information provisions of the SOCI Act to reduce current industry uncertainty and enable more agile responses to critical asset incidents.

- **Measure 8**: We in-principle support the proposed Secretary directions power to address 'seriously deficient elements' of an entity's risk management settings. Our support is based on this being a genuinely last resort power. We recommend that the future review of the SOCI Act examine whether the Department be provided with a broader range of regulatory tools to address individual entity compliance failings.

We have not commented on measures one and nine as we see them as beyond the AICD's governance mandate.

General comments

The AICD strongly supports the broad policy approach of the Government to building cyber resilience in Australia. A partnership model between Government and the private sector has the best chance of making meaningful advances in Australia's overall cyber posture in the coming years to the ultimate benefit of the Australian community. We also welcome the Department's commitment in the Consultation Paper that any new regulatory obligations are easy to comply with and limit regulatory burden.

AICD members are highly engaged on the governance of cyber security and data protection and are motivated to build the cyber resilience of their organisations. Cyber-crime and data security has been consistently the number one issue keeping directors awake at night in the AICD's biannual Director Sentiment Index.[1] Feedback from our members who are on the boards of all sizes of organisations is consistent that they are focused on the profound financial and reputational risks that cyber security threats pose and the damage a significant cyber security incident can do to an organisation and impacted customers.

The AICD has proactively sought to support members in overseeing cyber security risk. In October 2022 we published, in partnership with the Cyber Security Cooperative Research Centre (**CSCRC**), the *Cyber Security Governance Principles* (**Principles**).[2] In February 2024 we complemented the Principles with a new resource *Governing Through a Cyber Crisis* that was also developed in partnership with the CSCRC and professional services firm Ashurst.[3] As with the Principles, this new resource has sought to fill a gap in practical guidance for directors in Australia on how to oversee the response and recovery from a critical cyber incident. Both these resources benefitted greatly from the support of key Government stakeholders, including the Minister for Home Affairs and Cyber Security.

The development of these resources is a template for how a collaborative approach between industry and Government can produce dynamic guidance that drives meaningful improvements in cyber security resilience across the economy.

Measure 2: Ransomware reporting for businesses

The AICD in-principle supports a ransomware reporting regime applying to large businesses. We consider that a reporting regime that has the objective of increasing the Government's understanding of the ransomware threat picture is a balanced policy outcome compared to a prohibition or restriction on the payment of ransoms.

Duplicate existing reporting frameworks

Feedback from AICD members has found concern that the proposed reporting regime will be a new layer of reporting and notification obligations on the existing landscape of multiple reporting and notification requirements. Members have consistently raised frustrations that multiple reporting and notification obligations are an unnecessary, complex and costly burden at a time when organisations are attempting to contain and respond to a significant cyber security incident.

We recognise the Government's commitment in the Strategy to explore a single, harmonised approach to reporting. We also consider the new portal for reporting on cyber.gov.au as a valuable step in that

---

[1] AICD Director Sentiment Index, second half 2023, available here.

[2] *AICD CSCRC Cyber Security Governance Principles*, October 2022, available here.

[3] *Governing Through a Cyber Crisis - Cyber Incident Response and Recovery for Australian Directors*, February 2024, available here.

direction. However, we expect that it will take several years for there to be meaningful progress to a harmonised approach to cyber reporting and in any event distinct regulatory reporting requirements, such as Australian Prudential Regulation Authority (**APRA**) notifications, are likely to remain.

In the context of a new reporting obligation, we recommend the ransomware reporting regime be as contained as possible. For SOCI entities there is already a requirement to report a material ransomware incident as a component of the existing notification obligations under Part 2B of the SOCI Act. Our view is that for SOCI entities the existing reporting obligations should be taken as having met any ransomware reporting requirements. We appreciate that to enable this outcome there is likely to be some legislative changes to Part 2B to specify that a material ransomware demand, and separately a payment, are within scope of section 30BC.

For entities outside of the SOCI regime, we recommend the reporting obligation should be a simple as possible. We recommend that for the ransomware demand that a limited reporting form is developed that asks for readily attainable information, including the list on page 15 of the Consultation Paper, and does not place an undue or unreasonable burden on the entity. This approach would also be consistent with the uncertainty that organisations face in the immediate days following a cyber security incident where there is often very limited, or uncertain information, on the nature of the threat actor and the data or systems that have been compromised. A simple approach would also act to incentivise compliance with the first step of the reporting requirement.

We appreciate that for the second step that the Government will expect additional information to obtain a more complete threat picture. However, we consider that the information sought should be limited to the operational and technical elements of the ransomware payment, for instance the amount and how it was technically transferred to the threat actor. It would be inconsistent with the stated objective of the reporting regime and the 'no fault, no liability' principles for the Government to ask for details of the organisation's decision making behind making a payment.

Timing and definition

We support that both steps in the reporting framework align with the 72-hour period for making a notification under the SOCI Act. That is, an organisation has 72 hours from the point it has confirmed it is a genuine material ransomware incident to make the notification, and separately 72 hours from the point it makes a payment. The entity should be provided with discretion to make its own determination on what constitutes a genuine and material ransomware incident at which point the 72-hour period would commence.

We recommend that it be clearly defined, with supporting detail in guidance, on what constitutes a ransomware incident with a clear materiality threshold. We understand that organisations regularly receive demands for payment for data or system compromise with many of these being ultimately determined to be spurious or false. It would be onerous and counterproductive for an entity to be required to report all ransomware demands. Rather, a significance or materiality threshold should reflect that it is only incidents that impact an organisation's critical data and systems that will be required to be reported.

Finally, we also support clarity on the definition of ransomware attack or cyber extortion event. In particular, the definition should encompass both the theft or extortion of data and also the seizure or crippling of systems and software with an accompanying demand for payment.

Reporting threshold

Consistent with our submission to the consultation on the development of the Strategy we remain concerned that a $10 million annual turnover threshold is too low.

A threshold set at this level would capture many medium sized businesses that will have limited awareness and resources to meet the reporting obligations. We consider it likely that the Department would face significant challenges raising awareness amongst medium sized businesses of this new reporting requirement with the practical result that the objective of improving visibility will not be achieved due to inadvertent non-compliance. We consider this will be particularly the case for medium sized businesses outside of the SOCI regime or technology focused industries.

Further, a threshold that is set too low may result in contradictory enforcement outcomes where a medium sized business or NFP is penalised for inadvertently failing to meet a reporting requirement, in addition to experiencing the material costs and disruption of a ransomware incident.

We propose that the reporting regime threshold be set as *all SOCI entities and all large businesses with a turnover greater than $50 million*. This design would ensure that all critical asset owners and businesses with the resources to understand and meet the reporting regime are captured. This design would still provide the Government with a sufficiently robust sample of ransomware activity to produce a more complete picture of the cyber threat environment.

Were the Department to proceed with a $10 million threshold, despite stakeholders' objections, we recommend that it be supported by appropriate resources to raise awareness of the obligation, particularly amongst medium sized businesses, and also support for these organisations during a critical incident.

No fault, no liability

The AICD supports the ransomware reporting regime incorporating 'no fault, no liability' to the greatest extent possible. A framework with these overarching assurances is critical to incentivise timely and complete reporting.

Nonetheless, we recognise that there will be challenges in providing industry with the necessary confidence that reporting will genuinely be 'no liability'. For instance, we understand that this principle will not extend to anti-money laundering, sanctions and counter-terrorism requirements on businesses. We encourage the Department to undertake targeted consultation with legal experts on how a meaningful 'no fault, no liability' element can be core to the proposed regime.

We also would be concerned were the reporting regime to be utilised by the Government as a mechanism to pressure businesses to not make a ransomware payment. For example, a business in good faith reports the ransomware demand and then is encouraged by the Government to not make a payment. We would see this as inconsistent with the stated policy objective of the reporting regime. We recommend the Explanatory Memorandum clearly express that the objective of the regime is limited to collecting intelligence on the ransomware threat landscape.

Measure 3: Limited use obligation on the ASD and the Cyber Coordinator

The AICD strongly supports a legislated limited use obligation on the ASD and Cyber Coordinator for information provided by an organisation during the response and recovery phases of a significant cyber security incident. Consistent with the Consultation Paper, feedback from AICD members has indicated

that organisations are increasingly reluctant to share information with the ASD during a cyber incident due to concerns it will be shared with other Government regulators.

Application and prescribed cyber security purposes

We recognise the balancing act in designing a limited use obligation that provides comfort to organisations sharing information with the ASD and Cyber Coordinator and does not unduly restrict the activities of Government regulators and law enforcement agencies. However, we consider that as set out in the Consultation Paper the obligation being limited to 'use' rather than 'share, use and awareness' will diminish the comfort it provides to industry. As a consequence, there is a risk that existing concerns about sharing information with the ASD and Cyber Coordinator will only grow in an environment of increasing regulatory focus on cyber security incidents and private litigation.

Our interpretation of the proposal in the Consultation Paper is that there would no restriction on the ASD and Cyber Coordinator sharing information with other agencies or regulators or making them aware such information exists. The restriction would be limited to the *use* of such information. As proposed, a regulator or agency other than the ASD or Cyber Coordinator could utilise its respective information gathering powers to obtain the relevant information for its purposes knowing it exists. Were this interpretation to be borne out in practice, then it is unlikely the obligation would reduce the current concerns about sharing information with the ASD and Cyber Coordinator or engender trust and cooperation during a critical cyber incident.

We recommend that the limited use obligation explicitly covers the *use, sharing and/or awareness* of information by the ASD and the Cyber Coordinator.

We are also concerned that the proposed cyber security purposes are overly vague in nature and were they to be legislated would provide little comfort to organisations. Our concerns include:

- It is unclear what is meant by 'to facilitate consequence management'. As discussed below in respect of the proposed SOCI Act amendments, this term is very broad and subjective and may be interpreted by an organisation as entailing regulatory investigations into how the organisation responded to the incident. It is not clear there is a strong policy case for this purpose and we recommend it be removed.

- The inclusion of 'for law enforcement purposes' is, as above, very broad and may be interpreted as enabling the ASD and Cyber Coordinator to share any business information with a regulator or law enforcement agency, including information which may go to the decision making and actions of the business prior to the cyber incident. We understand this purpose is focused on law enforcement and intelligence activity related to investigating the *perpetrators* of cyber crime, rather than the business that has experienced the crime. We recommend this be clarified.

The AICD also recommends the drafting of the obligation provide certainty on when the limited use obligation is in effect with these details communicated to the relevant organisation. For instance, it may be appropriate for the ASD/Cyber Coordinator to provide a notice to the organisation that the limited use obligation was in effect from the point the incident was notified and then separately when it is no longer in effect (i.e. the incident is considered to be resolved by the ASD/Cyber Coordinator). Transparency of this nature will assist an organisation assess what information it shares with Government agencies.

Measure 4: Cyber Incident Review Board

The AICD in-principle supports the establishment of a Cyber Incident Review Board (**CIRB**) as a potentially valuable mechanism to disseminate analysis and lessons learnt from critical cyber incidents. Despite many high-profile cyber incidents in Australia in recent years there is limited industry and public understanding about the causes of these incidents, how the response and recovery was managed, the effectiveness of Government actions and what lessons can be taken from these incidents. A well designed CIRB may fill this information gap.

As discussed below, we consider that the current dynamic of heightened regulatory and legal risk that follows a significant cyber security incident means that the role of the CIRB should be broader than solely examining an isolated cyber security incident. A mandate that also encompasses examining industry wide security practices and vulnerabilities would also assist in preserving a genuine 'no fault' principle.

We are also cautious that a CIRB does not become a new source of Government bureaucracy and intervention during a significant cyber incident. Directors who have experienced a significant cyber incident have provided feedback on how the management of the organisation can be overwhelmed by regulatory, law enforcement and government agency requests during the initial response phase. At its worst, this dynamic can divert resources and attention from responding to the cyber incident and returning business operations to normal.

We support further detailed consultation on the structure, powers and objectives of the CIRB.

Overlap with regulatory activity and private litigation

A significant cyber incident can trigger a cascade of regulatory, law enforcement and private litigation activity. These investigations place enormous strain and costs on an organisation, including responding to voluminous mandatory information requests during the immediate response phase. This pressure is likely to increase as the Government contemplates introducing a direct right of action under Privacy Act reforms potentially stimulating significant class action activity associated with data breaches.

The design of the CIRB and its process for undertaking a review should account for this dynamic and not seek to place an additional burden on the impacted organisation. We consider that a grace period of six months from an incident to commencing a review may assist in reducing this burden.

We also note that ongoing regulatory and private litigation activity may restrict the CIRB from progressing and completing a review. For instance, a regulator investigation and subsequent court action against a company can take years to be resolved and this ongoing activity may limit the CIRB in making findings on a particular incident out of concern of influencing an investigation/court action or being inconsistent with the 'no-fault' regime. As discussed below, we recommend that the scope of matters the CIRB can review be broadened beyond a sole incident to examine thematic trends across Australia.

No fault

The AICD strongly supports the CIRB undertaking reviews on a 'no-fault' basis modelled off the regime adopted by the Australian Transport Safety Bureau under the *Transport Safety Investigations Act 2003*.

We in-principle support the list of factors on page 24 that CIRB may not consider, action or report on when undertaking a review. We urge the Department when considering the drafting of these provisions to undertake targeted consultation with legal experts to ensure the 'no-fault' framework is rigorous.

A principle of not allowing any inference to be drawn from an incident on the fault of the organisation may be challenging to implement in practice. In particular, the development and publication of such a report may have material bearing on ongoing regulatory investigations and private litigation. This potential to influence or prejudice a regulatory investigation or class action may prevent the CIRB from making public its findings from a particular incident for a number of years or limit the cooperation which an impacted entity affords to the review process.

Scope of CIRB reviews

The establishing legislation for the CIRB should clearly set out the mandate of the CIRB and the scope of the review process. We recommend that an incident review examine it in totality, including underlying causes, impact on customers and the role of Government support and coordination activities.

We also consider that the role of the CIRB is broadened to look beyond isolated cyber security incidents to thematic or industry-wide cyber security practices and vulnerabilities. This function would be consistent with the design of the Cyber Safety Review Board (**CSRB**) in the United States. In recent years the CSRB has conducted reviews into the Lapsus$ threat group, Log4j vulnerabilities and has commenced an inquiry into cloud computing service security.

The CIRB undertaking broader thematic reviews would assist in meeting the 'no fault' principle, avoid interference with regulatory enforcement activities and private litigation and also lower the burden on a particular organisation that is recovering from a critical cyber security incident.

Structure and membership

We recommend the Department consider agile and low-cost structures for establishing a CIRB. Although there may be benefits in establishing the CIRB as a standalone statutory body, such as to allow for unfettered review of the Government's response role, there is a risk that it could ultimately pursue its function in a narrow and isolated manner.

We support a model whereby the CIRB be 'stood-up' based on a 'blend' of standing and pool members. Both the standing and pool members would be drawn from a cross section of Government representatives, cyber security experts and individuals with extensive private sector management and governance experience. Our view is that diversity of perspectives will assist in the CIRB in producing insightful and detail rich reviews that reflect the realities of dealing with such incidents.

We consider that there would be governance benefits in a standing chairperson of the CIRB and consider it appropriate that this role is a statutory appointment by the Government.

Review process

The AICD supports a legislated materiality or significance threshold for initiating a review. We also support an obligation on the CIRB to detail in writing how the review meets this criterion upon commencing a review.

The AICD considers that the power to commence a review should reside with the chairperson of the CIRB. The chair is likely to be best placed to assess whether the criteria for commencing a review has been met and account for particular issues or organisational challenges associated with the incident.

In establishing the CIRB, consideration should be given to legislating a grace period for commencing a review to allow for the organisation, and affected stakeholders, to appropriately recover from the

incident. This period would also provide time for the organisation to focus on the initial response phase where the priority of the organisation is addressing immediate security gaps, engaging with Government and communicating with stakeholders. We consider that a grace period of no shorter than six months would allow the organisation to move through the initial response period and be able to appropriately engage with a CIRB review.

Investigatory powers and limited use provision

We recognise that to be effective the CIRB should have limited compulsory information gathering powers. These powers should be modest and used only in exceptional circumstances or as a last resort. We do not support the CIRB having intrusive powers, such as entering premises under a search warrant.

Where possible the CIRB should exhaust all avenues to voluntarily obtain information from an organisation(s) that is relevant to a review prior to issuing a compulsory information gathering notice. The CIRB should also publish guidance on under what circumstances it would issue a compulsory notice. The Australian Competition and Consumer Commission, by way of example, has published extensive guidance on its use of section 155 notices under the *Competition and Consumer Act 2010*.[4] We recommend the Department draw upon these comparable regimes and the supporting guidance when developing the legislation.

We also strongly support the limited use provision applying to the CIRB as an important element of an organisation having confidence in freely sharing information.

Measure 5: Data storage systems and business critical data

The AICD in-principle supports the proposed approach of specifying that 'business critical data' and supporting data storage systems fall within the scope of the SOCI Act asset class definitions and critical infrastructure risk management program (**CIRMP**) obligations. We understand that for many SOCI entities this is a clarification of existing data and risk management practices.

The definition of 'business critical data' will be key to entities interpreting and meeting this change, including in their risk management programs. We recommend the definition is principles based and retains flexibility for an entity to reach its own conclusion about what constitutes 'business critical' based on its unique circumstances, including size, complexity and industry. For instance, it may be the case that research data for many SOCI entities is not business critical and were it to be compromised, or lost, would have no bearing on the management and operation of a critical asset(s).

As reflected in the Consultation Paper, there can be considerable complexity in the supply chain of how, where and with whom business data is stored and managed. It is now common for business data to be stored with third parties, such as cloud of software as service providers, that in turn will utilise a network of systems and infrastructure to manage and store data. Frequently an organisation will have limited visibility on exactly where the data is located and limited ability to influence the risk management and data governance practices of the external third party. This is particularly the case for smaller SOCI entities. We recommend the Department produce comprehensive guidance on the expectations for entities in navigating this dynamic.

[4] ACCC, *A basic guide for individuals and small businesses*, October 2022.

Board sign-off

The Consultation Paper on page 40 noted that the list of expected risk management measures would be 'signed off by the company's board'. This appears to be a better practice expectation that is separate, or distinct, from the existing annual attestation process for the entity's CIRMP. Consistent with previous submissions and engagement with the Department, we strongly encourage guidance on expectations for the board in reviewing a CIRMP and attesting that it is 'up to date' in the annual report to the Department.

Where there are other risk governance practices that the Department considers that a SOCI entity's board should be undertaking, for example in respect of business critical data, we recommend this be consolidated with the development of standalone governance guidance under the Strategy (Initiative 5.1).[5] Where possible we consider the goal should be one Government source of governance guidance on cyber security, rather than disparate sources across Government that will create uncertainty or a lack of awareness.

Overlap with the Privacy Act

The Consultation Paper recognises that there will inevitably be overlap between business critical data and the definition of personal information under the Privacy Act.

Our view is that the overlap is likely to be far more pronounced than recognised in the Consultation Paper (see page 39). This is due to the interconnected nature of where personal and business data is stored, personal information being the key component of 'business critical data' for many entities and the cascading nature of an incident where a critical asset failing can morph into both a business data and personal information incident.

We strongly support close collaboration between the Department and the Attorney General's Department on how to align and harmonise the changes to the SOCI Act with the proposed changes to the Privacy Act. By way of example, the Privacy Act proposes to introduce the 'processor and controller' distinctions that will result in different obligations based on the classification of the business. Additionally, changes to APP 11 Protection of Personal Information are proposed. These two examples demonstrate the capacity for misaligned or contradictory regulatory obligations on entities that coordination between the two Departments should actively seek to avoid.

Measure 6: Consequence management powers

The AICD does not support the proposed Ministerial consequence management directions powers.

Based on the detail in the Consultation Paper there is not a strong policy case for these new powers. The existing Ministerial directions powers under Part 3 of the SOCI Act already provide avenues for a Minister to intervene during, and in the immediate aftermath of, a critical cyber security incident at a SOCI entity. These powers do not appear to have been exhausted and it is not clear from the Consultation Paper how they may be deficient.

The proposed scope of the powers is exceedingly broad covering the highly subjective and unclear concept of 'consequence management'. In addition, they go beyond the objective and intent of the SOCI Act. For example, extending from the SOCI Act focus on critical infrastructure protection to the replacement of customer identity documents. As recognised in the Consultation Paper, it is likely that such powers would overlap with existing regulatory frameworks and regulatory powers. The Privacy Act

[5] 2023-30 Australian Cyber Security Strategy, November 2023, page 24.

clearly applies to how an entity engages with impacted individuals following the loss or damage to personal information, including avenues for individuals to seek compensation. If the Government considers there are gaps in how an individual can have identity documents replaced then this should be addressed in proposed reforms to the Privacy Act, rather than a broad directions power in the SOCI Act.

The AICD and our members would welcome a more comprehensive evidence base to justify the proposed powers.

Were the Government to proceed with the proposed directions powers we recommend:

- 'consequence management' be comprehensively defined in a manner that is consistent with the intent of the SOCI Act and provides clarity on how these directions powers are distinct from the existing Ministerial and Home Affairs Secretary powers;
- the proposed scope of the directions power to encompass the replacement of documents of an impacted individual or business is removed;
- there is comprehensive immunity or protections for officers of an entity that are required to undertake an action that may be inconsistent with the best interests of the entity or otherwise bring about a conflict with existing director duties';
- the directions power be subject to the existing entity consultation requirements set out in section 33 of the SOCI Act; and
- clarification is provided on how the costs of comply with a direction(s) would be allocated and whether there are avenues for the entity to seek compensation from the Government.

We would welcome further discussions with the Department especially on ensuring there are comprehensive protections for directors of an entity subject to a consequence management direction.

Measure 7: Protected information provisions

The AICD supports amendments to the protected information provisions of the SOCI Act to reduce current industry uncertainty and enable more agile responses to critical asset incidents.

We support the proposed 'harms based' approach detail in the Consultation Paper to amending the definition of 'protected information'. It is appropriate that the entity itself retains discretion to assess the potential harm from any disclosure. This amendment should be supported by guidance from the Department on how an entity should undertake this assessment.

We also support greater flexibility for the disclosure of protected information by the Government to other Commonwealth and state regulators and agencies. However, we note the intersection with the proposed limited use obligation on the ASD and Cyber Coordinator. In particular, there may be an inherent tension or conflict with a comprehensive limited use obligation and broader disclosure practices by the Government of protected information under the SOCI Act.

We recommend that in the 'proscribed cyber security purposes' of the limited use obligation that is clarified that disclosure is permitted in the context of a SOCI entity experiencing a significant incident that may impact the security of critical infrastructure or protecting national security.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

The AICD supports in-principle the proposed directions power in Part 2A of the SOCI Act to address 'seriously deficient elements' of a CIRMP. Our support is based on the detail set out in the Consultation Paper that this power would in practice be last resort and limited to circumstances where the consequences of the deficiency may impact national security or socioeconomic stability. We recommend that the definition of 'seriously deficient' be comprehensively defined in the legislation and/or Explanatory Memorandum.

As noted in the Consultation Paper, an independent review of the SOCI Act will commence after the CIRMP obligations are in full effect. Our view is that this review should consider whether the Department should be equipped with a range of enforcement and penalty powers that allows for greater discretion or nuance when identifying deficiencies with CIRMP obligations. For instance, an enforceable undertaking is a regulatory tool that economic and financial regulators frequently utilise in Australia, including the Australian Prudential Regulation Authority (**APRA**) and the Australian Securities Investments Commission. Notably APRA utilises undertakings to address identified risk deficiencies at entities.[6] Regulatory tools of this nature would avoid the necessity of the Department having to utilise a Home Affairs Secretary directions order in instances where it is uncertain about whether the deficiencies meet the relevant national security and socioeconomic stability threshold.

We also support continuing efforts by the Department to educate and raise awareness amongst SOCI entities of expectations for CIRMP best practice.

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

[6] https://www.apra.gov.au/news-and-publications/apra-agrees-to-court-enforceable-undertaking-from-bank-of-queensland