

31 January 2022

Home Affairs Department

via: CI.Reforms@homeaffairs.gov.au

Dear Home Affairs Department (**Home Affairs**)

Exposure Draft - Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Security of Critical Infrastructure (Application) Rules 2021

Thank you for the opportunity to comment on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the **SLACIP Bill**) and separately the proposed Security of Critical Infrastructure (Application) Rules 2021 (**Reporting Rules**).

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 47,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits, large and small businesses and the government sector.

The AICD welcomes the Government's consultation on further measures to strengthen cyber security and resilience of entities owning and managing critical assets across the Australian economy. Australian directors are increasingly focused on the governance of cyber risk given the rapidly changing threat landscape and the increasing prevalence of attacks. The AICD's latest Director Sentiment Index (**DSI**) for the second half of 2021 revealed that cybersecurity is the number one issue keeping directors awake at night.¹

Executive Summary

The AICD supports the broad objectives of the SLACIP Bill to build on the existing regulatory regime under *Security of Critical Infrastructure Act 2018* (Cth) (**Act**) to enhance the security and resilience of critical infrastructure assets and systems of national significance.

The proposed amendments under the SLACIP Bill and the amendments that passed Parliament in November 2021 represent, in totality, a significant expansion of the Act. A large number of entities across an expanded list of industries will be subject to the extensive existing and proposed obligations under the Act, including Government intervention and directions powers. In the context of this expansion, and the importance of protecting Australia's key assets and infrastructure, the AICD encourages the Government to provide extensive guidance and support to entities to meet the objectives of the reforms.

Our key points are as follows:

1. The AICD supports the principles-based drafting of the Risk Management Program (**RMP**) obligations. We also strongly support the flexibility provided to entities to utilise existing risk management requirements to meet the RMP obligations. To ensure the RMP obligations are effective in driving

¹ AICD Director Sentiment Index (December 2021), available [here](#).

effective risk management and governance practices, the AICD recommends extensive guidance and support for entities and directors in understanding the requirements and understanding better practice expectations. It will only be through a collaborative partnership between industry and government that key critical infrastructure assets are appropriately protected.

2. The AICD supports the proposed expanded statutory immunity provisions at sections 38, 41, 43 and 44 of the Exposure Draft.
3. The AICD recommends further work across government to find opportunities to align and/or harmonise existing and proposed cyber security reporting obligations.

1. Risk Management Program

This section responds to the proposed RMP requirements under Part 2A of the Exposure Draft.

The AICD supports the principles-based drafting of the RMP requirements and providing an entity with flexibility to meet the obligations in a manner that fits with its size, complexity and nature of the assets under its ownership. We also support the use of 'reasonably practicable' as the threshold for eliminating or minimising a material risk under the RMP rather than 'reasonably possible' in the previous version of the Bill. This drafting appropriately reflects the challenges entities face in managing cyber security risk, particularly the threat posed by state sponsored actors. Further, as discussed below, the AICD welcomes mechanisms in the Exposure Draft and rules to reduce the regulatory burden on entities that are subject to equivalent risk management obligations.

The RMP requirements and supporting rules are analogous to the risk management obligations placed on Australian Prudential Regulation Authority (**APRA**) regulated entities. APRA, via the prudential framework, such as *Prudential Standard CPS 220 Risk Management*, places extensive risk management obligations on entities with accountability ultimately lying with the Board of each entity. The requirements extend beyond managing financial risks (e.g. liquidity) to risk management across an entity, including information security under *Prudential Standard CPS 234 Information Security (CPS 234)*. The prudential standards are supported by extensive guidance through prudential practice guides, thematic reviews and regular communications to industry. We also understand that APRA adopts a cooperative and facilitative approach with entities to build better practice in risk management.

The AICD encourages Home Affairs to consider the APRA approach as a model for providing extensive guidance and regulator support to entities in meeting the RMP requirements. It is only through a cooperative and collaborative partnership between industry and government that stronger cyber resilience will be achieved. The focus of government should be on building capability within industry, rather than a punitive compliance focused approach.

We recommend that supporting rules and guidance should set out government expectations for meeting the obligations and assist in interpreting the legislation. Guidance would include:

- expectations for approval and ownership of the RMP at the entity;
- monitoring and reporting, including reporting to the board and/or board committees;
- the steps that an entity are expected to take in reviewing its RMP, including internal or external audit expectations, and how frequently reviews are expected to occur; and

- what thresholds or changes would necessitate an update to the RMP and what constitutes taking 'reasonable steps' in making updates to RMPs.

The rules and guidance will be key to the board satisfying itself that it is complying with the obligations and can attest to this in the annual report on the RMP. Any guidance should make clear what Home Affairs considers is *necessary* to meet legal obligations, as well as identify those practices that go *beyond* those minimum standards and constitute better practice.

Annual report

The board of an entity with an RMP will be required to approve an annual report on its RMP under section 30AG.

The Explanatory Document at paragraph 83 states that approval of the annual report by the board is "designed to ensure that the most senior levels of an entity are aware of the risk management practice of the entity and personally accountable [for] compliance with this regime." The Exposure Draft does not have provisions imposing personal liability on directors and our understanding from engagement with Home Affairs is that this is not the intent of the proposed obligations. The role of the board and directors is to have oversight function of risk management at an entity, rather than have personal accountability for meeting regulatory obligations. We recommend this drafting is removed or clarified in the revised explanatory materials to the legislation that is ultimately introduced to Parliament.

As above, guidance on the expectations for the annual report and governance oversight of the RMP will be key to assist directors in meeting the requirements. We consider that guidance would cover what is envisaged by 'up to date' and what assurance or reporting is expected to be obtained by directors in reaching a view on the status of the RMP. Reaching a view on whether an RMP is 'up to date' would be linked to the review and update requirements under sections 30AE and 30AF and any internal or external audit expectations.

We also consider that the drafting of 30AG(2)(f) in respect of detailing hazards during the reporting period could account or recognise reporting of incidents under Part 2B of the Act. Our view is that a hazard that had an impact on an asset during the period may have overlap, particularly if it is significant, with the cyber incident reporting obligations. The drafting would ideally recognise this alignment and not require an entity to report duplicative information. Again, guidance on detailing a hazard and how the RMP mitigated any impact will be key to directors having comfort that it is meeting the annual report obligations.

Finally, we would also welcome clarity in the drafting and explanatory materials on whether there will be an 'approved form' for the annual report in the sense of a template or set reporting document as appears to be contemplated under subsection 30AG(2)(e). An 'approved form' is not referenced in the Explanatory Document and we would caution against a prescriptive requirement that limits an entity's capacity to meet the annual report requirements in its preferred format.

The AICD encourages Home Affairs to consult extensively on the development of the guidance. The AICD stands ready to work with Home Affairs on guidance for directors in meeting the RMP requirements and the broader obligations under the Act, including facilitating targeted engagement with experienced AICD members.

Existing regulatory obligations

The AICD welcomes the proposal outlined in the Explanatory Document that entities already subject to equivalent obligations will not have the duplicative RMP requirements imposed on them. The mechanism for avoiding duplication will be through the Ministerial declaration process under section 30AB where the RMP obligations are applied based on sector.

The proposal recognises there is an existing patchwork of cyber security and risk management related obligations that differ based on industry sector. The AICD in its submission to the Treasury/Home Affairs consultation on 'Strengthening Australia's cyber security regulations and incentives' cited regulatory complexity, including the Act and sectoral specific obligations, as a barrier to directors and organisations understanding existing obligations and building cyber resilience.² The AICD expects that in addition to the defence industry, as cited in the Explanatory Document, that Home Affairs will assess whether it is appropriate for the financial services, energy and communications sectors to not have the RMP requirements applied. This is due to these sectors facing extensive existing risk management obligations.³

As noted above, the rules development process will be critical to how entities meet the RMP requirements. The Explanatory Document at paragraph 72 notes that the rules can recognise existing industry standards and practices as sufficient to meet aspects of the obligation. The Minister also must have regard under section 30AH(6)(a) of the existing regulatory system of the Commonwealth, a State or a Territory that imposes obligations on responsible entities.

The AICD strongly supports the rules recognising existing obligations and standards as a mechanism to avoid duplication and reduce regulatory costs for entities. Existing requirements can be industry specific, such as CPS 234 applying to APRA regulated entities, or across industries, for example *Privacy Act 1988* obligations. Further, many Australian businesses seek to meet international regulatory frameworks (e.g. General Data Protection Regulation (**GDPR**)), or standards (e.g. ISO 27000 series) by virtue of overseas customers or partners. *Article 32 Security Processing* of the GDPR, for example, imposes obligations on securing personal data and is likely to be relevant to an entity meeting its RMP obligations.

Rather than attempting to comprehensively list all existing obligations, the rules should provide discretion to an entity to determine whether compliance with another regulatory or industry framework represents equivalence with the RMP requirements. As an accountability mechanism, the entity could then detail where it has determined equivalence in its annual report on the RMP.

2. Statutory immunities

This section responds to the drafting of the statutory immunity provisions at sections 38, 41, 43 and 44 of the Exposure Draft.

The AICD welcomes the proposed amendments that recognises the role of employees and directors of related entities in meeting the directions and notification requirements under the Act. The AICD was concerned that the current immunity provisions (e.g. section 30BE) may expose a director of a related entity to personal liability in the event the related entity assists in complying with a direction or notification

² AICD submission, Strengthening Australia's cyber security regulation and incentives, 27 August 2021, available [here](#).

³ Existing risk management obligations include APRA prudential standards, the *Telecommunications Act 1997*, obligations under National Electricity Rules and National Gas Rules.

requirement under the Act.⁴ The personal liability may arise due to the assistance bringing about a conflict with a director's duties under the *Corporations Act 2001* (Cth).

The AICD encourages consideration of whether the immunity provisions could be further broadened to cover actions related to meeting all obligations under the Act, not just the directions and notification provisions. For instance, the officers of an entity that is responsible for a system of national significance may face a conflict with other duties in complying with an obligation under Part 2C. A comprehensive approach to providing immunity would provide comfort to decision makers of entities, including directors, that there is appropriate protection if complying with or meeting the intent of an obligation under the Act results in conflict with other legal obligations.

3. Cyber incident reporting

This section responds to the proposed reporting rules that will be made by the Minister.

The AICD does not have specific comments on the drafting of the proposed Reporting Rules. However, we recommend Home Affairs assess opportunities across government to align or harmonise existing and proposed cyber security reporting obligations. In addition to existing obligations, such as notification requirements for APRA regulated entities under CPS 234, the Government has proposed introducing a ransomware reporting framework.

As a starting point, we do not consider that an entity should have to make multiple reports for the same incident/event to different government regulators. For example, it is possible that in the future a superannuation entity that experiences a ransomware incident related to member data would separately have to report in different forms to APRA, the Office of the Australian Information Commissioner, the Australian Cyber Security Centre and meet the proposed ransomware reporting requirements. Multiple differing reports for the same incident will impose a compliance burden on entities and importantly divert management attention from resolving the incident.

Again, the AICD stands prepared to assist Home Affairs on reporting obligations, including utilising the expertise of AICD members with experience in designing and implementing reporting frameworks.

4. Next Steps

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

Yours sincerely,



Louise Petschler GAICD
General Manager, Advocacy

⁴ AICD letter to Minister for Home Affairs re Critical Infrastructure Bill, 26 August 2021, available [here](#).