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

14 February 2025

Minister for Home Affairs
Parliament House
Canberra ACT 2600

Dear Minister

Consultation on Subordinate Legislation to the *Cyber Security Act 2024* and *Security of Critical Infrastructure Act 2018*

Thank you for the opportunity to comment on the proposed subordinate legislation to support the cyber security reforms passed by the Parliament in November 2024 and contained in the *Cyber Security Act 2024* (**CS Act**) and *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 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 (**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 a submission to the Parliamentary Joint Committee on Intelligence and Security review of the cyber security legislative reform package in 2024 (**PJCIS submission**), the development of the 2023-2030 Australian Cyber Security Strategy (**Strategy**), previous amendments of SOCI Act and reform of the *Privacy Act 1988* (**Privacy Act**).

We have also supported our membership to improve their knowledge of cyber security best practice through extensive guidance materials and education opportunities, including the AICD Cyber Security Cooperative Research Centre *Cyber Security Governance Principles* (updated in November 2024) and separately the *Governing Through a Cyber Crisis* publication.

1. Executive Summary

The AICD welcomed passage of the cyber security legislative reforms in November 2024 as a milestone in Australia's journey to becoming one of the most cyber secure nations by 2030. The reforms reflect a partnership approach with industry to building cyber security resilience and mostly avoided unnecessary and counterproductive compliance requirements for businesses and their boards. 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.

Our comments on the subordinate legislation package are limited to the *Cyber Security (Ransomware Reporting) Rules 2024* (**Reporting Rules**) and the *Cyber Security (Cyber Incident Review Board) Rules 2024* (**CIRB Rules**). Our key points are:

1. Reporting Rules

- We do not support the ransomware payment reporting threshold being set at $3 million per annum. A threshold this low will result in significant inadvertent non-compliance through small businesses and NFPs not being aware of the obligation. It may also result in contradictory and punitive enforcement outcomes where a small business or NFP is penalised for failing to meet a reporting requirement, in addition to experiencing the material costs and disruption of a ransomware incident.
- We recommend that the turnover threshold is set at a $10 million per annum consistent with the Department of Home Affairs (**Home Affairs**) proposal in 2023. This threshold would capture businesses that have the requisite resources and awareness to meet the reporting obligation. A threshold at $10 million, in addition to capturing all SOCI Act entities, will still provide a robust picture of ransomware activity in Australia.
- At a time of slow economic growth and a pervasive productivity challenge in Australia, it is critical that regulatory obligations, and associated compliance costs, are appropriately contained.

2. CIRB Rules

- We support the proposed eligibility criteria for both board members of the CIRB and members of the expert panel. We recommend that in appointing board and expert panel members that the Minister be guided by a skills matrix that is consistent with the proposed CIRB Rules. The composition of both the board and expert panel should cover a diverse range of relevant skills and experience with a majority of members being appointed from outside of the Australian Public Service.
- We recommend that section 10 of the CIRB Rules be broadened to provide the Chair with discretion to delay a review when there is significant private litigation before the courts and there is a risk that a CIRB review may prejudice these actions.
- We recommend the CIRB publish a board charter and detailed guidance on its review processes, including use of information gathering powers and consultation with the relevant entities.

Threshold for reporting

We do not support the reporting threshold being set at $3 million per annum as proposed under section 6 of the Reporting Rules.

A threshold set at $3 million will capture many small organisations, including NFPs, charities and family-owned businesses, that will have limited awareness and resources to meet the reporting obligation. We consider it likely that Home Affairs will face significant challenges raising awareness amongst these organisations of the new reporting requirement. This will be particularly the case for small businesses and NFPs outside of the SOCI Act umbrella or technology focused industries. Our view is that the practical result of these awareness building challenges is that the objective of improving the visibility of ransomware activity will not be achieved due to inadvertent non-compliance.

To the extent smaller organisations are aware of the reporting requirement they will face difficulties in making the necessary report in the 72-hour window while at the same time effectively responding to a critical cyber security incident, including assessing system damage and data compromise and loss. Our strong view is that in this immediate response phase the directors and managers of a small organisation should be supported through direct Australian Signals Directorate (**ASD**) and Home Affairs advice and technical assistance rather than meeting a reporting requirement.

There is also the potential for a $3 million threshold to result in contradictory and punitive enforcement outcomes where a small business or charity is penalised for inadvertently failing to meet a reporting requirement, in addition to experiencing the material costs and disruption of a ransomware incident. Our strong view is that the focus of ransomware regulatory efforts should be on education of entities' obligations and where they can obtain support, rather than enforcement.

We note that concerns with the burden of a reporting threshold set at $3 million is shared by the Council of Small Business Organisations Australia and the Customer Owned Banking Association.[1]

We recommend the threshold be set at $10 million consistent with Home Affairs consultation on the Strategy.[2] That consultation noted that a $10 million threshold aligns with the small business threshold used by the Australian Tax Office. This threshold is more likely to capture organisations that will have resources to be aware of, and comprehensively meet, the reporting requirement. Further, through a $10 million threshold covering all medium and large organisations (in addition to all SOCI Act entities), the reporting framework will provide a robust sample size of ransomware payments that will allow to Home Affairs and ASD to form a quantitative picture of the impact of ransomware in Australia.

At a time when economic growth remains tepid, and business challenged by low productivity and rising compliance costs, it is imperative that any new regulatory obligations are appropriately targeted.

Guidance on reporting requirements

We strongly encourage Home Affairs and the ASD to develop guidance to assist an organisation make the necessary report consistent with the requirements under section 7 of the Reporting Rules. This support would include the development of a targeted reporting form available through the existing reporting and notification portal on cyber.gov.au.

The form and supporting guidance should recognise that each ransomware incident is unique and there is often imperfect, limited and potentially an incorrect understanding the incident at the time a payment and a corresponding report is made. For instance, an organisation may not fully understand the impact of the incident on its infrastructure and customers. It can take a number of weeks or months to comprehensively understand these impacts. The Home Affairs and ASD expectations for meeting these information requirements should be flexible and recognise this dynamic.

The guidance should also cover expectations for a SOCI entity meeting the existing notification requirements under Part 2B of the SOCI Act and the new ransomware payment reporting requirement under section 27 of the CS Act. While two duplicative reports will be required, the guidance should detail how a SOCI entity can reduce this burden, for instance through enabling a SOCI entity to reference information made in the SOCI report for the purposes of meeting the ransomware payment reporting requirement.

3. CIRB Rules

Eligibility criteria

We support the proposed eligibility criteria for both board members of the CIRB and members of the expert panel. These criteria should enable the Minister to appoint members that have the relevant skills and experience to meaningfully contribute to the CIRB review process.

---

[1] Council of Small Business Organisations Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, October 2024; Customer Owned Banking Association, Submission to Parliamentary Joint Committee on Intelligence and Security, October 2024.

[2] Home Affairs, *Consultation Paper - 2023–2030 Australian Cyber Security Strategy: Legislative Reforms*, page 18.

We recommend that both standing and expert panel members appointments are guided by a skills matrix that is consistent with the proposed CIRB Rules. The composition of both the board and expert panel should entail a diverse range of relevant skills and experience that is commensurate with the multi-faceted complexity of significant cyber events. Consistent with our previous submissions, we also recommend that a majority of both the standing board and the expert panel are drawn from outside the Australian Public Service (**APS**). The independence and the effectiveness of the CIRB would be undermined were the Minister to appoint a majority of board members from the APS.

Timing of reviews - Non-interference

The AICD supports section 10 under which CIRB will not conduct a review at a particular time when the Chair determines that such a review may interfere or prejudice a separate investigation or court proceedings by a Commonwealth or State law enforcement agency or regulator. This provision is consistent with our policy position in previous submissions on the real risk that a CIRB review may prejudice existing regulatory action associated with a particular cyber security incident and undermine the CIRB's 'no-fault' principle.

We continue to also see a risk that that a CIRB review may interfere or prejudice private litigation that is connected to a cyber security incident. For example, there is currently significant class actions focused on prominent cyber security incidents in Australia in recent years and the resulting data breaches. There is a potential for an increase in private litigation linked to cyber incidents in coming years with the introduction of the statutory tort for privacy under recent Privacy Act changes and the separate proposed direct right of action.

To address this concern, we recommend that section 10 also provide the discretion to the Chair to delay a review when there is significant private litigation before the courts and there is a risk that a CIRB review may impact these actions.

Guidance on CIRB governance and review processes

Consistent with sound public sector governance practice, the AICD recommends the CIRB publicly document its governance and review processes. Transparency on the governance and operation of the CIRB would demonstrate its commitment to operating as an independent and rigorous review body.

We recommend the CIRB publish a charter that is consistent with the CS Act and the proposed CIRB Rules. The charter would detail roles and responsibilities, composition, meetings, delegations and the management of conflicts of interest. As recognised in the CIRB Rules under sections 16 and 25, there is an expectation that from time to time a board member or expert panel member will have a conflict that may be relevant to a particular review. Our view is that the CIRB should detail how these conflicts are identified and managed as central to the CIRB maintaining objectivity. We note that the United States Cyber Safety Review Board has such a charter.[3]

Furthermore, clear documentation of the Board's review processes - including its use of its information gathering powers, stakeholder engagement and consultation on draft reports, root cause analysis, and development of recommendations - will allow organisations to better positioned to contribute to CIRB processes. The publication of this information would be consistent with other Commonwealth review and investigatory bodies, including the Australian Transport Safety Bureau.[4]

[3] Cyber Safety Review Board Charter is available here.
[4] Information on the Australian Transport Safety Bureau investigation process is available here.

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