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

25 October 2024

Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Committee Secretary

Exposure Draft Package - Cyber Security legislative reforms

Thank you for the opportunity to comment on the cyber security legislative reform package, comprising the *Cyber Security Bill 2024* (**CS Bill**), *Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024* (**ISA Bill**) and *Security of Critical Infrastructure and Other Legislations (Enhanced Response and Prevention) Bill* (**SOCI Bill**).

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 the *2023–2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper* (**Consultation Paper**) in early 2024, the development of the 2023-2030 Australian Cyber Security Strategy (**Strategy**), previous amendments of *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 best practice through extensive guidance materials and education opportunities, including the AICD-Cyber Security Cooperative Research Centre *Cyber Security Governance Principles* and separately *Governing Through a Cyber Crisis* publication.

AICD's policy positions on the package are based on engagement with cyber security and legal experts, Australian businesses, industry bodies and AICD members.

1. Executive Summary

The AICD strongly supports the policy direction of the proposed reforms set out in the package and accompanying Explanatory Memorandum.

We broadly consider the proposed reforms achieve a balance between new targeted cyber security regulations and avoiding unnecessary and counterproductive compliance requirements for businesses and their boards. We also commend Home Affairs and the Government for the level of consultation undertaken on these reforms and accounting for industry feedback in a number of areas.

Given the short consultation period we have limited our submission to the following:

- **Part 3 CS Bill – Ransomware reporting obligations**
    - We support the introduction of a ransomware payment reporting framework recognising that the objective of this new reporting obligation is to enable a more complete intelligence and threat picture of ransomware activity in the Australian economy. We also consider the framework is an opportunity to enhance support for businesses who have experienced a critical ransomware incident.
    - We recommend that SOCI Act entities be excluded from ransomware payment obligation given the existing notification requirement in the SOCI Act. We also recommend drafting clarification on the application of the obligation to large companies with complex structures, including with international operations.
    - We recommend that the turnover threshold is set at a level (for example $10m) where captured businesses have the requisite resources and awareness to meet the reporting obligation.
- **Part 4 CS Bill; Schedule 1 ISA Bill – Limited use obligation on National Cyber Security Coordinator and Australian Signals Directorate**
    - We strongly support the introduction of a limited use obligation on the National Cyber Security Coordinator (**Cyber Coordinator**) and Australian Signals Directorate (**ASD**).
    - We support the drafting of the cyber security purposes and consider that they balance promoting the voluntary provision of information by a business during an incident, with the need to share information with other Commonwealth parties in limited circumstances.
    - We recommend the obligation be broadened to explicitly cover the 'recovery' phase of an incident and not just the immediate response.
- **Part 5 CS Bill – Cyber Incident Review Board**
    - We support the establishment of a Cyber Incident Review Board (**CIRB**) and recommend the CIRB be allowed to undertake thematic or industry wide reviews.
    - We recommend the CIRB not be allowed to undertake an incident review concurrent with other Commonwealth regulatory investigations.
    - The CIRB should be explicitly required to consult with the impacted business on its reports.
    - The drafting of 'no fault' principle requires strengthening through expressly including individuals, in addition to entities, and meeting the scope of the principle outlined in the Consultation Paper.
    - We strongly support the CIRB being independent and to assist in achieving this objective recommend that a majority of standing members are from outside of the public service.
- **Legislative review of key CS Bill provisions**
    - We recommend that a legislative review be incorporated into the CS Bill. A three-year timeframe would allow for the reforms' impact to be assessed.
- **SOCI Bill Schedule 2 - Ministerial powers to manage consequences of serious incidents**
    - We recommend that the Explanatory Memorandum to the SOCI Act Bill provide further detail and examples on the use of the Ministerial consequence management directions powers. Given the breadth and largely unfettered nature of the proposed powers there is a risk that they will be utilised in instances that are inconsistent with the stated policy intent of responding to national emergency and multi-asset critical failures.

2. Part 3 CS Bill: Ransomware payment reporting obligation

Consistent with our submission to the Consultation Paper we support the establishment of a ransomware payment reporting framework that has the objective of increasing the Government's visibility of the economic and social impact of ransomware in Australia.

We strongly support the decision to remove the ransomware *demand* reporting requirement that was proposed in the Consultation Paper. This obligation would have materially increased the regulatory burden associated with the regime and would have distracted businesses during the immediate response phase of a critical cyber incident.

Application to SOCI entities and protection of information

We recommend that for the purposes of making a ransomware payment report, that a SOCI entity need only report once under the existing notification obligations in Part 2B of the SOCI Act.

While we support ransomware payment reporting applying to all SOCI entities regardless of size our interpretation is that a SOCI entity will report the same ransomware incident and corresponding payment twice under the CS Bill and the SOCI Act. As a result, in the 72-hour period a SOCI entity will make multiple reports under both the SOCI Act and the CS Bill to separate government agencies (ASD in the instance of a critical asset notifiable incident; Home Affairs in the case of a ransomware payment).

AICD members have consistently raised frustrations that multiple cyber incident and data reporting and notification obligations are an unnecessary burden at a time when organisations are attempting to contain and respond to a significant cyber security incident. The Cyber Strategy has a commitment to explore a single, harmonised approach to cyber and data breach reporting and the Government has made some welcome steps to address this issue via the reporting portal on cyber.gov.au. The duplication of ransomware payment reporting for SOCI entities is arguably inconsistent with this policy direction.

We recommend that this duplication be resolved through a minor amendment to the definition of cyber security incident under section 12M of the SOCI Act to explicitly cover a 'ransomware payment' with this definition referencing the CS Bill. SOCI entities would then be carved out of the ransomware reporting regime in the CS Bill.

Threshold for reporting

The revenue threshold will be the subject of a future Ministerial rule making process, including additional consultation. However, such is the centrality of the threshold to the effectiveness of the regime that we consider it important that the PJC recommend that it is set at a level where captured businesses have the requisite resources and awareness to meet the reporting obligation.

We understand that the Government will propose that the turnover threshold is set at $3 million per annum consistent with the Notifiable Data Breaches Scheme under the Privacy Act. Our strong view is that $3 million is too low and that the threshold should be set at a minimum of $10 million.

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

A threshold that is set too low may also 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 and awareness raising of entities' obligations and how to support cyber resilience, rather than enforcement.

We propose that the Committee recommend the Government set a turnover threshold commensurate with organisations that have the resources to be aware of, and comprehensively meet, the reporting requirement.

Application to complex company structures

We understand from consultation with large, listed companies with complex structures that there is significant uncertainty about which entity in a corporate structure will have the reporting obligation. This uncertainty extends to where the corporate structure includes wholly or partially owned subsidiaries operating in international jurisdictions and also where the company participates in joint ventures.

Our understanding is that the intent of the obligation is for an entity with a group structure to report once and contain that reporting to ransomware payments related to an incident in Australia. For example, we would not expect that a company with a partially owned subsidiary in a European country would be required to report a ransomware payment by that subsidiary.

We recommend further consultation with these impacted companies and legal experts on how the drafting can be amended to resolve these uncertainties. At a minimum we would expect that Home Affairs would publish guidance that directly addresses different corporate structures with worked examples.

Penalties and industry support and guidance

We support the civil penalty limit being set at a 'maximum' of 60 penalty units (currently $18,780). While 60 penalty units is a relatively small sum for very large businesses it may represent a significant penalty for small businesses and NFPs (e.g. that are close to the revenue threshold). There should be a level of discretion in applying the penalty to take account of business size, complexity, impact of the ransomware incident and awareness of the obligation.

We note the commitment in the Explanatory Memorandum for Home Affairs to take an 'education first approach' to the reporting obligation.[1] We welcome this policy position. We also recommend that the introduction of the reporting obligation be supported by appropriate resources to raise awareness, particularly amongst SMEs and NFPs. Further, where a business has made a report, they should be offered support and advice to assist them to respond and recover from a critical ransomware incident.

3. Part 4: Coordination of major cyber security incidents – Limited use

The AICD has been a been a long-standing supporter of 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. We in-principle support the construction of the limited use obligation as detailed in the CB Bill and the proposed amendments to the ISA Bill.

We commend Home Affairs for taking on board the feedback from industry that the prescribed cyber security purposes in the Consultation Paper were too broad and open-ended. The purposes as set out in section 40 of the CS Bill and section of ISA Bill strike an appropriate balance between the necessary sharing of information, and providing a degree of comfort to businesses that information voluntarily provided will not be passed on for other regulatory purposes.

[1] Explanatory Memorandum, paragraph 222.

To improve the efficacy of the policy, we recommend the drafting in section 35 of the CS Bill and section 41BA of the ISA Bill be amended to explicitly cover the 'recovery' phase of an incident. Currently the drafting and the Explanatory Memorandum indicate the limited use will only be in effect for the immediate response phase of an incident.

Our view is that the limited use should not be time bound to a particular arbitrary moment in an incident. Discussions with senior directors who have lived through a significant incident have indicated that the response and the recovery phases are often blurry and the support from the ASD and Cyber Coordinator can go on beyond the immediate triage and containment of the incident. A definition of an incident that encompasses recovery will provide further assurance to impacted businesses that they can continue to voluntarily share and obtain assistance from the ASD and Cyber Coordinator during the critical periods of rebuilding systems and operations, supporting employees and remediating impacted customers.

We recommend the Cyber Coordinator and ASD support the introduction of the limited use obligation with guidance on how it will be implemented and interpreted. This guidance would include how the agencies will define 'information'. Our expectation is that 'information' would cover all pertinent data or communications provided or obtained from the entity during the incident, including oral/verbal communication, meeting notes, logs or technical data in addition to written information provided by the entity.

4. Part 5: Cyber Incident Review Board

Consistent with our submission to the Consultation Paper, we support the establishment of a Cyber Incident Review Board (**CIRB**). 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 will help fill this information gap and lift collective national resilience.

We make the following recommendations to improve the design of the CIRB, detailed further below:

- Expand the scope of reviews from beyond 'incidents' to thematic or industry-wide cyber vulnerabilities under subsection 46(3) of the CS Bill;
- CIRB is only able to initiate reviews following the conclusion of other Commonwealth regulatory or enforcement action to avoid processes that overlap and potentially duplicate one another;
- The 'no fault' principle be strengthened under subsection 46(4) of the CS Bill and the CIRB discretion in respect of consulting with an entity is removed under subsection 45(2) – such consultation should be mandatory to allow for the most effective, well-informed reviews and to uphold the principle of procedural fairness; and
- The eligibility requirements for CIRB standing members encompass members that are from industry and have skills and experience in critical cyber incident response and recovery.

Scope of reviews

We remain of the view that the scope of CIRB reviews should be broader than 'incident or series of incidents' as defined in subsections 46(2) – (3) of the CS Bill. A scope that allows for thematic or industry-wide cyber security practices and vulnerabilities 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.

A mandate for reviews that is broader than just 'incidents' will also reduce the risk that the work of the CIRB is hamstrung or delayed by concurrent regulatory action and private litigation, discussed below.

Concurrent regulatory action

The Explanatory Memorandum notes that a CIRB review may take place concurrently with other regulatory or law enforcement investigations.[2] We are concerned that this will be difficult to achieve in practice, may prejudice the relevant investigations, imperil the 'no fault' principle and at a minimum impose a significant burden on the impacted business or businesses.

As detailed in our submission to the Consultation Paper, we are of the view that conducting reviews concurrent with a separate regulatory investigation has a risk of impeding a genuine no-fault principle. For instance, it may be challenging for the CIRB to produce a comprehensive and insightful review report that has no inference about fault. At the same time there may be a separate Commonwealth regulator (e.g. OAIC, ASIC) that is taking enforcement action against the entity, or its directors, with the express goal of establishing fault.

Concurrent reviews and investigations would also pose significant burden and cost on the impacted entity or entities in that they are having to respond to information requests and engagement with separate arms of the Government.

For the above reasons, we strongly recommend CIRB not be able to initiate reviews until all Commonwealth regulatory investigations and/or proceedings have been concluded. While we recognise this may curtail the timeliness of CIRB and reviews, we consider that allowing the CIRB to conduct broader thematic or industry-based reviews, as discussed above, would be a mechanism to mitigate this concern and avoid the risk of impacted entities taking an overly legalistic approach to cooperation with the CIRB for fear of prejudicing their legal position in future actions by third parties (whether regulators or private litigants).

No fault and consultation

We welcome the no fault elements detailed in subsection 52(4) of the CS Bill. We note however that the no fault principle is limited to entities and is not as comprehensive as was envisaged in the Consultation Paper. Notably, the elements of no fault do not include 'assist in court proceedings between parties relating to a cyber incident' or 'allow any adverse inference to be drawn from the fact than an entity was involved in a cyber incident'. We strongly recommend these elements of the no fault principle are reflected in subsection 46(4).

Further, we recommend that the drafting specifically covers individuals in addition to entities. This approach to no fault would be consistent with that taken by the Australian Transport Safety Bureau under the *Transport Safety Investigations Act 2003*.

A comprehensive no fault framework is fundamental to the design of the CIRB and incentivising entity, individual and broader industry cooperation and transparency, particularly in the context of the CIRB's proposed mandatory information gathering powers.

We also recommend that subsection 51(4) be strengthened in that the CIRB 'must' consult on a draft report with the entity or entities that have are the subject of the review rather than 'may'. We also recommend this drafting is tightened in that the entire draft report is provided rather than the option of providing a 'extract'. This is a key provision to ensure that any confidential information provided to the CIRB under the voluntary, or mandatory information gathering powers, is not contained in the report and

[2] Explanatory Memorandum, paragraph 368.

the entity is afforded due process to review whether the report meets the 'no fault' principles. Of course, we recognise that ultimately it will be a matter for the CIRB to determine what it publishes, subject to any agreed confidentiality arrangements.

The policy basis for allowing the CIRB discretion regarding whether it consults with the entity or entities on the draft report and information contained in it is unclear.

Although the process is meant to operate on a no-fault basis, in reality, there is likely to be some reputational (both corporate and individual) damage as a result of such a review. Indeed, the CIRB's report may also assist other potential litigants (private or public) in future legal proceedings. Accordingly, it is entirely appropriate that procedural fairness be afforded to individuals and corporates whom a negative inference may be drawn from a CIRB report. Further, there is a real risk that a CIRB report may inadvertently disclose sensitive and confidential information if entities are not offered an opportunity to review the draft report.

Appointment of members and expert panel

We strongly support the CIRB being independent as detailed in the Explanatory Memorandum and under section 63 of the CS Bill. We are also supportive of the CIRB Chair and standing members being appointed by the Minister recognising that this is consistent with how similar government committees, reviews and oversight bodies are established.

To achieve the objective of the CIRB being independent in appearance and practice, we recommend that the appointment process of the Chair, standing members and expert panels follows well-established governance practice in that it is transparent, rigorous and based on well-considered skill matrix. The eligibility requirements for standing members that will be set in a future rule making process should encompass relevant skills and experience with cyber security incident response and recovery in addition to an understanding of the broader cyber threat landscape.

Our view is that these eligibility requirements should ensure there is a majority of non-public service or Government members of the CIRB and ideally all standing members would be from outside of the public service, in addition to members of the Expert Panel. This model would be consistent with the Takeovers Panel for example, in recognition of the often-technical nature of key issues. In addition to assisting the CIRB's independence it will also ensure the CIRB has the requisite skills and experience to undertake meaningful reviews, well-informed by practical industry insights.

We recommend that the PJC note that in the future rule-making process for eligibility requirements under subsection 66(4), that standing members should be drawn from outside of the public service with appointments based on skills and experience in cyber incident response and recovery being one of the key criteria.

5. SOCI Act Amendments

Based on feedback from members and engagement with industry AICD is supportive of the following amendments to the SOCI Act:

- capturing data storage systems and business critical data within the relevant definitions under Schedule 1 of the SOCI Bill;
- use and disclosure of protected information under Schedule 3 of the SOCI Bill;
- risk management review and remedy powers under Schedule 4 of the SOCI Bill.

The AICD does not have a well-informed policy position on the consolidation of the telecommunication security requirements into the SOCI Act, and will leave it to other stakeholders to comment.

For each of the above reforms, we strongly recommend that Home Affairs support industry through comprehensive guidance. In particular, there is currently limited understanding of what constitutes better practice in respect of a critical infrastructure risk management program (**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 section 30AI of the SOCI Bill.

Ministerial directions powers

The AICD retains concerns with the breadth of the new Ministerial directions' powers contained in Schedule 2 of the SOCI Bill.

We understand from further information provided by Home Affairs and detail in the Explanatory Memorandum that the proposed new consequence management powers are intended to be a last resort mechanism that would only be utilised in very critical situations and national emergencies.

While we do not question that this is the intent, nonetheless, from a sound policy making perspective, introducing largely unfettered powers runs the risk of potential Government overreach into business decision-making and accountability. The guardrails or threshold that the Minister or Home Affairs Secretary should account for under subsections 35AB(1)(b) – (d) of the SOCI Act are very broad and subjective, including the definition of 'relevant impact'. We are concerned that these powers would allow a Minister to inappropriately give directions to an entity in instances where there are not national emergency or critical asset conditions.

The Explanatory Memorandum notes that the powers would be utilised in 'multi-asset' incidents however the drafting in the SOCI Bill does not limit the use of the powers to incidents covering multiple critical assets.[3] In addition there is one limited example based on bushfire event impacting electricity distribution assets. We recommend that the Explanatory Memorandum provide further detail on when these powers will be utilised, including additional worked examples.

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

[3] Explanatory Memorandum, paragraph 38.