Insurance Council of Australia

11 September 2024

Via email: ci.reforms@homeaffairs.gov.au

Dear Sir/Madam

Exposure Draft Package Cyber Security legislative reforms

Thank you for the opportunity to comment on this important draft legislation package. The Insurance Council of Australia supports the intent of this legislation. We offer the below comments to improve the legislation's effectiveness.

We note the extremely limited consultation period provided. We also note the request not to share the draft legislation with members not included by Home Affairs. This short timeframe and limited capacity to share the draft with our members has hampered our ability to effectively assess, understand, and test the impact of the legislation across our members' complex operations. In particular, we note that given the diverse nature of the insurance sector, we are concerned that there may be unintended consequences for some of our smaller members who were either not consulted or have not had capacity to respond in the required timeframes.

Given the criticality of cyber security for the ongoing robustness of the financial services sector and the Australian economy more broadly, we respectfully urge the Government to consider providing adequate capacity to consult across members of industry associations in future.

We make the following additional comments.

Cyber Security Bill 2024

Secure-by-design standards for internet of things devices
We recommend the Bill be amended to clarify that software is not covered by the *Secure-by-design* provisions.

Ransomware reporting obligation
We support the ransomware reporting obligation. However, we have identified two examples of situations that may be inadvertently captured by the Bill's ransomware reporting obligation in its current form:

1. Businesses may at times purchase small amounts of stolen data to identify which user within their system has been compromised. Information gleaned from such purchases then allows the business to take the necessary steps to reduce the risk to their systems and organisation.
2. Businesses may pay 'bug bounties' to independent cyber researchers to identify security vulnerabilities. These cyber researchers may come through formal programs or approach businesses directly to provide information about a vulnerability they have identified in exchange for a fee. Without clarity, payments to cyber researchers under the latter may be captured by the draft legislation.

Having to report incidents such as these examples would add significant impost for businesses with limited value. The Bill should be clarified to ensure such incidents are not reportable, defining "ransomware" may alleviate this issue.

Insurance Council of Australia

Additionally, we note section 27(2) and supporting comments on page 7 of the accompanying explanatory document. We recommend the Bill further clarify that protection from contractual breaches will be granted to entities required to terminate an agreement with a third party who cannot or is unwilling to comply with a government direction or obligation under the *Security of Critical Infrastructure Act 2018*.

Further, and while it may be addressed at a later date, we urge early consideration of how data collected under the ransomware reporting obligation can be shared with cyber insurers to support improved underwriting practices. We recommend further engagement with the cyber insurance industry to ascertain what information will be most useful for this purpose.

Cyber Incident Review Board
In a situation where a third party provider (to a critical infrastructure operator) is the subject of a review by the Cyber Incident Review Board (CIRB), we query if a customer could be compelled to provide confidential information that was in turn provided by the third party provider. If so, this outcome could unintentionally reduce the willingness of third party providers to share details of a cyber incident with customers given those customers may be compelled to share that information.

We believe the Bill could further clarify the obligations of the CIRB to protect legally privileged information which they have been provided. Our members have queried if legal precedence might determine that sharing privileged information with the CIRB under this Bill would waive privilege. Further consideration may need to be given to this outcome.

We also recommend the inclusion of a legislated review process for the CIRB. A review would allow the Government, with input from industry, to ensure the CIRB's objective continue to be met in what may be an entirely different threat landscape.

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

Data storage systems that hold business critical data
We recommend the legislation confirm that other than the reporting of security incidents there are no additional impacts to obligations for critical infrastructure operators in the financial services sector.

Thank you for the opportunity to comment. We trust that our initial observations are of assistance, and we look forward to continuing our engagement with the Government on this important topic.

Regards

[redacted]

Andrew Hall
CEO and Managing Director