Insurance Council of Australia

14 February 2025

Department of Home Affairs

Via upload

Dear Sir/Madam

Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to provide comment on these important legislative measures.

The Insurance Council of Australia (ICA) is the representative body for the general insurance industry of Australia. Our members represent approximately 90 per cent of total premium income written by private sector general insurers, spanning both insurers and reinsurers. Our work with our members, consumer groups and all levels of government serves to support consumers and communities when they need it most.

As a foundational component of the Australian economy the general insurance industry employs approximately 46,000 people, generates gross written premium of $66 billion per annum, and on average pays out $159 million in claims each working day ($39.4 billion paid out per year).

We offer the following comments on specific aspects of the subordinate legislation package.

Ransomware Reporting Rules

With regard to S7(4)(c) and (d) of the *Cyber Security (Ransomware Reporting) Rules 2024* exposure draft (the Rules), we do not believe it is clear how reporting entities should best measure the impact to their infrastructure and customers. We recommend that supporting guidance is provided alongside the reporting portal to help reporting entities determine what information is sought for disclosure.

Further, we are aware there are currently no plans for the Government to share information reported under the Rules with industry. The information captured can help industry build a greater understanding of the threat environment. Such information sharing would help Australia achieve "world-class threat sharing" and contribute to the Government's goal of Australia being a "world leader in cyber security".[1]

Given this, we recommend the Government consider how information captured under the ransomware reporting obligation can be shared in a deidentified form with industry and ensure the rules are designed to facilitate that sharing.

We also recommend the Government consider how information reported under the Rules that must also be shared with other government bodies, could be shared with those agencies through the

[1] The Australian Government's goal of Australia being a world leader in cyber security by 2030 and Shield 3 "World-class threat sharing and blocking" are outlined in the *2023-2030 Australian Cyber Security Strategy*.

reporting framework under a “tell us once approach”. This would limit the government touchpoints for reporting entities and allow them to focus on incident recovery.

Finally, we suggest that the Government may find it useful to collect information on whether a reporting entity has cyber insurance at the time of reporting. This may help the government gain a better understanding of the cyber insurance market’s penetration.

Cyber Incident Review Board Rules

We note the requirement that a person may only be eligible for appointment to the Cyber Incident Review Board (the Board) if they hold or are eligible to hold a security clearance that allows “access to information that has a security classification of at least secret”.[2]

While we acknowledge that the Board will be reviewing nationally significant cyber incidents, we are concerned that requirements for secret level security clearances will skew the Board’s make up towards public servants, limiting the important insights that can be brought from the private sector. The presence of public servants on the Board is not inherently negative. However, informed by experience and priorities, public servants and persons from the private sector are likely to have differing considerations on cyber incident response and recovery. It is important to balance industry and government viewpoints

Given this, we recommend the Government consider how it can be ensured that business is appropriately represented on the Board.

Thank you for the opportunity to comment. If you have any queries, please contact Eamon Sloane, Adviser, Strategic Policy at esloane@insurancecouncil.com.au.

Regards

Andrew Hall
Executive Director and CEO

[2] *Cyber Security (Cyber Incident Review Board) Rules 2024* (Exposure Draft) s13(1)(a)(i).