BCA
Business Council of Australia

14 February 2025
Department of Home Affairs

To whom it may concern,

The Business Council of Australia (BCA) welcomes the opportunity to provide a submission to the Cyber Security Legislative Package – Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act).

The BCA recognises that the legislative changes and draft rules have been thoroughly consulted, and many of industry's previous comments have been taken on board.

This letter outlines the BCA's perspectives on three key initiatives proposed under the Rules:

- Security Standards for Smart Devices
- Ransomware Reporting
- Cyber Incident Review Board (CIRB)

Security standards for smart devices

Smart devices are now woven into the fabric of daily life. The BCA supports the push for mandatory cyber security standards for consumer-grade devices, aligning with global benchmarks like the European Telecommunications Standards Institute (ETSI) and the UK's *Product Security and Telecommunications Infrastructure Act*.

The BCA recommends including a clear definition of the term 'manufacturer' in order to establish a point of accountability. Further, we suggest defining 'product' strictly as physical smart devices—excluding software-only offerings like applications.

The BCA also recommends certain exclusions or modified requirements (e.g. exclusion of products below a certain selling price), or modified requirements on devices like those of the UK's *Product Security and Telecommunications Infrastructure Act*. This may lower the potential regulatory impact on businesses, including associated compliance costs.

The BCA supports the exemptions included in the draft Rules. One exemption of particular interest is therapeutic goods. As noted in the explanatory document, approved therapeutic goods devices are already subject to globally recognised and well-established regulatory compliance controls under the Therapeutic Goods Administration. The BCA suggests that any government communication around the therapeutic goods exemption should highlight the very high standard of cyber security already applied to these devices. This will help avoid misperceptions that exemption means these devices are less secure.

Ransomware reporting

Ransomware is a growing threat that requires a collective defence. The BCA supports mandatory reporting to build intelligence and resilience across industries.

Scope

The BCA suggests the draft Rules more clearly state that the rules are for reporting ransomware *payments*, not all ransomware incidents. Although this becomes clear in the detail, it would also help to change the title to *Cyber Security (Ransomware **Payment** Reporting) Rules 2024* and the second heading to 'Part 2–Ransomware payment reporting obligations'.

The BCA also suggests specifying if the scope of ransomware payment reporting is intended to include examples where malware is not used.

A cyber ransom could be paid without using ransomware or any type of malware. For example, an attacker phishes for credentials, uses them to log into the target system, steals data and extorts the victim. The victim then makes a payment to the attacker. It is unclear if this would be in scope.

Consider including an explicit definition addressing whether 'ransomware' (i.e. a type of malicious software) is a required element of this reporting regime. The *Cyber Security Bill 2024 – Revised Explanatory Memorandum* defines ransomware as 'malicious software to cripple operations by encrypting devices, folders and files, rendering essential computer systems inaccessible unless a ransom is paid.' Apart from this, no explicit definition of ransomware appears in the *Cyber Security Act 2024* nor the draft *Cyber Security (Ransomware Reporting) Rules 2024*.

Reporting timing and content

The draft Rules require reporting ransomware payments within 72 hours. This may present challenges in some incidents. At that early stage, information is often limited as organisations prioritise supporting consumers and suppliers, operational recovery, notifications to boards, and engagement with insurers. With that in mind, the BCA welcomes the included caveat that 'Information is only required to be given to the extent that the reporting business entity knows or is able, by reasonable search or enquiry, to find out within the 72 hour time period for giving the report.'

However, the BCA also suggests that reporting would be made more effective if the 72 hour timeframe is extended to 96 hours and a specific follow-up reporting period be carved out, which may be better suited to intelligence gathering. While there are benefits to speed of reporting—we should also look to maximise the quality of the reporting.

The draft Rules specify mandatory requirements for information that a ransomware payment report must contain. To improve useful information provision, the government should provide more details on what is meant by:

- 'the impact of the incident on the reporting business entity's infrastructure', and
- 'the impact of the incident on the reporting business entity's customers.'

Cyber Incident Review Board (CIRB)

The BCA supports the CIRB's role in conducting impartial reviews of cyber incidents. But transparency is key to maintaining trust. The BCA suggest public disclosure of meeting minutes and decision-making processes will help eliminate any perception of bias.

Sections 20 and 27 of the Rules allow for the termination of Board and Expert Panel members by the Minister for Home Affairs. The BCA recommends that the Rules should include procedural steps for entities to challenge Board and Expert Panel membership appointments and terminations (based on, for example, suspected misconduct, conflict of interest, and identified gaps in assessment). These procedural steps should also include the ability for affected entities to challenge review findings.

The BCA also suggests government provide further guidance on what information can be published in the final review report versus what should be kept in the 'protected review report' (outlined in paragraph 54(1) of the Act).

The BCA recommends the terms of reference for a review should include strict confidentiality requirements for CIRB standing members and Expert Panel members participating in that review

Paragraph 47 of the Act ('Board may discontinue a review') does not require the publication of a report if a review is discontinued. BCA suggests it may be useful for the Rules to include a requirement for the CIRB to publish a final report even if a review is discontinued, which could explain why the review was discontinued and present any relevant findings from the start of the review until the time the review was discontinued.

Thank you again for the opportunity to comment on these draft Rules.

Yours sincerely

Mike Bareja
Director, Digital Technologies, AI, Cyber and Future Industries
Business Council of Australia