Australian Information
Industry Association

Australian Information Industry Association

Submission on

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

14 February 2024

Introduction

The Australian Information Industry Association ('AIIA') appreciates the opportunity to provide feedback to the Department of Home Affairs on the Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act). The AIIA has been actively engaged throughout the cyber security legislative reforms and remains committed to supporting a regulatory framework that enhances cyber resilience while ensuring practical and effective implementation for industry.

Cyber security threats continue to evolve at an unprecedented pace, necessitating a framework that is both adaptive and informed by ongoing industry expertise. In this context, we welcome the opportunity to provide industry insights on key aspects of the proposed subordinate legislation, particularly in relation to security standards for smart devices, implementation timeframes, and ransomware reporting requirements.

Security Standards for Smart Devices

The AIIA supports the exemption of devices provided under s8(1)(b) of the proposed Security Standards for Smart Devices Rules[1], in line with our previous recommendations[2]. This exclusion-based approach ensures that devices with more sophisticated security architectures and complex supply chains are not subject to prescriptive cyber security requirements that may be impractical to implement. The government, in collaboration with industry, can explore targeted approaches to addressing cyber security risks associated with these complex devices. The AIIA recommends that any future regulatory consideration should be guided by ongoing technical advice and industry consultation to ensure that bespoke measures are developed where necessary. This will allow for proportionate and effective security requirements without imposing unnecessary compliance burdens that may disrupt innovation or market access.

Additionally, we support the scope of the standards as applying to consumer-grade devices only, ensuring that the regulatory focus remains on products that are widely used by the general public, thereby addressing key security risks without placing unnecessary compliance burdens on business-specific devices. Business and government devices are already covered by Information Security Manual (ISM), Security of Critical Infrastructure Act and Secure by Demand plus sector specific regulations so duplication of existing obligations plus the three abovementioned requirements being a relatively low bar in the government, critical infrastructure and business sectors should be avoided.

Furthermore, the AIIA believes the proposed 12-month implementation timeframe is insufficient for industry to effectively transition to the new requirements. We have

[1] Exposure Draft: *Cyber Security (Security Standards for Smart Devices) Rules* 2024 (Cth).

[2] Australian Information Industry Association, *Submission on Australian Cyber Security Strategy Legislative Reforms*, 1 March 2024, p. 4.

previously recommended a 36-month implementation period[3], in line with the European Union's *Cyber Resilience Act*[4], to allow manufacturers, importers, and suppliers adequate time to meet the mandated security standards. Given that many IoT devices sold in Australia are imported, a longer implementation period would provide global manufacturers with sufficient time to integrate the required security measures into product design and development cycles. To support this transition, we recommend conducting a review concurrent with the first 12 months of the 36-month implementation period. This review should evaluate the impact of the security standards on businesses and the broader industry, identifying potential challenges and regulatory burdens. The findings from this review will be instrumental in informing any necessary adjustments to the regulatory framework, ensuring it remains practical, proportionate, and responsive to industry needs.

Ransomware Reporting

The AIIA supports the proposed $3 million turnover threshold for mandatory ransomware reporting, and commends the government for recognising industry concerns in shaping this requirement. This threshold strikes an appropriate balance between regulatory oversight and minimising compliance burdens on smaller businesses. Additionally, the alignment of this threshold with the *Privacy Act*[5] ensures consistency in regulatory expectations across cyber security and data protection frameworks.

Furthermore, while we recognise that s27 of the *Cyber Security Act*[6] specifies the information that reporting business entities must provide, we recommend the development of additional detailed guidance to support compliance and reduce uncertainty. This information should be presented in a simplified, structured, and user-friendly format that provides clear explanations of each requirement and practical guidance on how to comply. This should include the introduction of standardised reporting templates that clearly outline the required information, level of detail, and submission process. Clear, concise, and structured guidance would streamline the compliance process for businesses, enabling the government to aggregate and analyse ransomware incident data more effectively.

Cyber Incident Review Board

The AIIA supports the establishment of the Cyber Incident Review Board (CIRB) as a mechanism for reviewing significant cyber security incidents and providing recommendations to government and industry. While we acknowledge the role of the

[3] Ibid.
[4] European Parliament and Council, *Cyber Resilience Act*, Regulation (EU) 2024/2847, OJ L 402, 23 October 2024.
[5] *Privacy Act 1988* (Cth), s6D.
[6] *Cyber Security Act 2024* (Cth).

Expert Panel in contributing specialist insights, we recommend a more consistent integration of this expertise into the CIRB's review processes.

Specifically, the AIIA recommends that the legislation explicitly require the inclusion of at least two members from the Expert Panel from the cyber security sector in every CIRB review. This requirement will ensure that each review benefits from comprehensive technical expertise, practical incident response experience, and a deep understanding of evolving cyber threats and business limitations. Mandating the involvement of multiple Expert Panel members will enhance the robustness of the CIRB's deliberations and assist in counterchecking expert advice while avoiding conflict of interests, fostering recommendations that are informed by diverse perspectives and current best practices in cyber security.

Summary of recommendations

1. Security Standards for Smart Devices:

- Complex devices should be excluded from prescriptive security rules.
- Regulations should apply only to consumer-grade devices, avoiding duplication for business and government devices.
- A 36-month implementation period (not 12 months) to align with global standards and allow industry adaptation.
- Conduct a review in the first 12 months to assess impact and refine requirements.

2. Ransomware Reporting

- $3 million turnover threshold balances oversight with minimal burden on small businesses.
- Provide structured templates and guidance to simplify compliance.

3. Cyber Incident Review Board (CIRB)

- Mandate at least two cyber security experts in every review for balanced insights.
- Ensure expert input is consistently integrated into CIRB recommendations.

Conclusion

As cyber threats continue to evolve, it is imperative that regulatory measures remain adaptable and informed by ongoing industry engagement. The AIIA emphasises the importance of meaningful consultation with stakeholders to ensure that security standards, compliance requirements, and implementation timelines are aligned with industry realities. A collaborative approach between government and industry will be essential to maintaining a regulatory framework that is effective, proportionate, and conducive to innovation.

Should you require further information, please contact Ms Siew Lee Seow, General Manager, Policy and Media, at siewlee@aiia.com.au or 0435 620 406, or Mr David Makaryan, Advisor, Policy and Media, at david@aiia.com.au.

Thank you for considering our submission.

Yours sincerely
Simon Bush
CEO, AIIA

***

About the AIIA

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. We are a not-for-profit organisation to benefit members, which represents around 90% of the over one million employed in the technology sector in Australia. We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies