AUCYBER

Public Submission

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

February 2025

Introduction

AUCyber welcomes the opportunity to respond to the Australian Government's consultation on the proposed Rules within the Cyber Security Legislative Package, following the recent Royal Assent of the Cyber Security Act 2024 and related legislation. We fully support the Government's ambitious goal of becoming a world leader in cyber security by 2030, as outlined in the 2023-2030 Australian Cyber Security Strategy, and commend the efforts made to date towards enhancing Australia's cyber resilience through these new legislative measures and whole-of-nation strategy.

As a key stakeholder and provider of services in Australia's cyber security ecosystem, AUCyber recognises the importance of the proposed Rules, particularly those related to smart devices' security standards, ransomware reporting, critical infrastructure risk management, and telecommunications security. We value the consultative approach, and this submission will provide constructive feedback to ensure that the Rules and related strategy align with industry needs, are designed for practical implementation and contribute to the broader objective of securing Australia's digital infrastructure in the interest of everyday Australians, sovereignty and national security.

In this submission, we outline our observations and related recommendations concerning the proposed Rules. This submission will offer our insights into the potential impact of the proposed Rules on the cyber security community and broader business ecosystem. Specifically, this submission will address the following proposed Rules:

1. Cyber Security (Security Standards for Smart Devices) Rules 2024
2. Cyber Security (Ransomware Reporting) Rules 2024
3. Cyber Security (Cyber Incident Review Board) Rules 2024

We look forward to continued engagement to help shape robust and effective cyber security frameworks for Australia's future.

1. Cyber Security (Security Standards for Smart Devices) Rules 2024

AUCyber fully supports the introduction of mandatory security standards for smart devices. With cyber threats becoming increasingly frequent and sophisticated and playing on the vulnerabilities inherent in smart device use, these users have become prime targets. The current voluntary approach, highlighted by the 2020 Code of Practice: Securing the Internet of Things for Consumers, has resulted in low adoption rates, making it clear that mandatory standards are needed to address the growing risks.

Securing smart devices is crucial for consumer protection, as these devices are deeply integrated into everyday life and often store sensitive personal and commercial data. Australians are increasingly vulnerable to scams and cyberattacks through these devices. Cybercriminals exploit smart device security weaknesses to steal personal information, financial data, or access private networks. The rise of connected devices in households has made us more susceptible to such attacks, with Australian homes now averaging approximately 33 smart devices per household[1]. This dramatic increase in connected devices has amplified access for criminals and increased threat risk, with cybercriminals often targeting connected devices to bypass traditional security measures.

By establishing clear, enforceable security standards, the Australian Government will assist in significantly reducing the risk of exploitation by malicious actors. As the Internet of Things (IoT) continues to expand, securing these devices will help mitigate the broader risks associated with a connected world.

Aligning with global security benchmarks, such as the European Telecommunications Standards Institute (ETSI) standards, will at the same time have the added benefit of ensuring Australian manufacturers meet international best practices, contributing to the country's competitive edge in the global market. Additionally, as smart devices play an increasingly vital role in critical infrastructure, their security directly impacts sovereignty, national and economic security.

AUCyber strongly supports mandatory security standards for smart devices:

- to strengthen Australia's cyber resilience
- to protect consumers
- to support the broader goal of securing the nation's digital infrastructure.

AUCyber acknowledges the need for consideration to be given for a 'grace period' between the commencement of the Act and date of compliance; however, urges an educational push for compliance to be achieved before that period ends. That way, Australians can be assured that their risk of cyber-crime is a concern that is being dealt with appropriately and in a timely manner.

[1] www.statista.com

2. Cyber Security (Ransomware Reporting) Rules 2024

AUCyber recognises and acknowledges that ransomware continues to be one of the most used tactics and 'money-spinners' for cybercriminals, posing a significant threat to organisations and governments worldwide, particularly wealthy countries like Australia. We further understand the ethical, operational, legal and financial dilemma businesses and organisations face when deciding whether to pay a ransom. In response to this growing issue, we support the introduction of mandatory ransomware payment reporting, as it is a vital step in strengthening our collective cyber defences.

AUCyber supports the new legislation requiring organisations that pay a ransom in response to a cyberattack and that earn more than $3 million to mandatorily report the payment to the Australian Government within 72 hours. AUCyber agrees key details such as the amount, payment method, and the identities of the attackers should and need to be reported. Timely reporting is essential to help authorities track cybercrime networks and, in turn, aid in preventing future incidents. By mandating this reporting, organisations are contributing valuable intelligence that strengthens the fight against ransomware and malicious actors. This allows organisations to play an active role in defending the cyber ecosystem and preventing further funding of cybercriminal activities.

In Australia, organisations responsible for critical infrastructure and those with annual revenue of more than $3 million are particularly impacted by this obligation. AUCyber encourages all organisations, both globally and locally, to review their Cyber Incident Response plans and collaborate with leadership teams to create clear policies on when and how to report ransom payments. Establishing these processes will ensure compliance with the new law and support the wider goal of disrupting criminal operations.

AUCyber acknowledges the concerns and challenges that businesses and organisations may face when it comes to reporting, understanding their obligations, and sharing this information with other government agencies, as well as any perceived flow-on effects. We understand that the new ransomware payment reporting requirements may feel overwhelming, especially for smaller businesses with limited resources. It is essential that the government supports this initiative with education, clear guidance, and ongoing support to ensure all organisations paying ransoms are not only aware of their obligations but are also comfortable with the reporting process and the associated events. Providing clarity on the process and purpose of the legislation, the reasons behind it, and the broader impact will help businesses of all sizes navigate these requirements with confidence, ensuring compliance while contributing to the collective fight against cybercrime.

3. Cyber Security (Cyber Incident Review Board) Rules 2024

AUCyber recognises the vital role of the Cyber Incident Review Board (CIRB), established under the Cyber Security Act 2024, in enhancing Australia's cyber resilience. We support the CIRB approach to conducting no-fault, post-incident reviews of major cyber security events and providing recommendations to both the Australian Government and industry on improving future incident prevention, detection, and response strategies. One of the CIRB's key functions is its authority to compel organisations to supply information when voluntary cooperation is unsuccessful. We believe this provision will help encourage transparency and promote a culture of learning from past incidents to better protect national security.

At the same time, we recognise that the introduction of the CIRB will have a substantial impact on organisations involved in cyber incidents. In order to meet the CIRB's information requests, businesses must form a coordinated response team made up of legal, risk, compliance, security and IT professionals. This team will oversee the management of requests and ensure that sensitive information is handled appropriately, including safeguarding legal professional privilege when necessary.

Organisations may face challenges in this process and will be required to review any draft reports or findings provided by the CIRB, offering timely feedback where appropriate. Additionally, businesses will need to assess the CIRB's recommendations and implement them where suitable, in order to strengthen their cyber security practices. Companies should be mindful of their obligation to adopt these recommendations and prepare for the potential public release of CIRB reports. This preparation should include strategies for communicating with stakeholders and the media, to ensure transparency.

AUCyber emphasises the importance of integrating the CIRB process into Cyber Incident Response Plans, enabling organisations to meet their legal obligations while also contributing to the overall enhancement of Australia's cyber resilience. We also recognise the role of the CIRB in guiding businesses through the entire process, from investigation to reporting. Furthermore, it is crucial for the government to educate businesses on the CIRB's role, processes, and obligations.

Conclusion

Every day the Australian governments and businesses trust AUCyber to safeguard their most important assets, data, brand reputation and people. AUCyber empowers Australian enterprise and government customers with the latest sovereign cloud infrastructure, cyber security solutions and managed IT services. Our cyber security solutions protect Australian businesses and government entities, while our sovereign cloud infrastructure and managed backup services ensure data security, sovereign control and business continuity. AUCyber supports the Australian Government's efforts to strengthen the nation's cyber resilience through the proposed Cyber Security Rules within the Cyber Security Legislative Package. We believe that mandatory security standards for smart devices, the introduction of ransomware payment reporting, and enhanced cyber incident management are crucial steps in protecting both businesses, government and consumers from evolving cyber threats. While we acknowledge the challenges organisations may face in complying with these new requirements, we encourage continued education and collaboration between industry and government to ensure these measures are practical, effective and contribute to a safer digital environment. As a key stakeholder in helping to protect Australian organisations AUCyber remains committed to working alongside all stakeholders and government to help shape and implement these important cyber security frameworks to protect Australia's future.

AUCYBER

Protecting Australian Data.

Every day Australian businesses and governments trust us to safeguard their most important assets, data, brand reputation and people. AUCyber empowers Australian enterprise and government customers with the latest sovereign cloud infrastructure, cyber security solutions and managed IT services.

Our cyber security solutions protect Australian businesses and governments, while our sovereign cloud infrastructure and managed backup services ensure data security, sovereign control and business continuity. AUCyber's managed IT services deliver on-demand, cost-effective and scalable support. With a unique blend of integrated technologies, skilled professionals and top-tier security, we're dedicated to securing the Australia of today, for tomorrow.

Discover AUCyber's award winning solutions today:

- Sovereign cloud services
- Managed cyber security solutions
- Governance risk & compliance (GRC)
- Testing & assurance
- Managed IT services
- Strategy & consulting

1800 282 568

aucyber.com.au