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

Introduction

The Australian Retailers Association (ARA) and National Retail Association (NRA) welcome the opportunity to provide a submission in response to the Australian Government's proposed subordinate cyber security legislation under the *Cyber Security Act 2024* and the *Security of Critical Infrastructure Act 2018*. The ARA and NRA collectively represent over 190,000 retail shop fronts across the country, our members operate in all categories, including fashion, food, electronics, homewares, manufacturers, QSRs and online retail.

As retail businesses increasingly rely on digital technologies, connected devices, and cloud-based infrastructure, cyber security has become a pressing issue for our sector. The ARA and NRA support a strong and coordinated approach to cyber resilience but urge the government to ensure new regulations do not impose undue compliance burdens, particularly on small and medium-sized businesses. Consistency with existing regulatory frameworks, such as the *Privacy Act* and the AI regulatory framework, is critical to avoiding unnecessary duplication and complexity.

Security Standards for Smart Devices

Retailers rely on smart devices for payment processing, inventory tracking, customer engagement, and store security. Establishing minimum cyber security standards for these devices is an important step in protecting businesses and consumers from cyber threats. However, as confirmed in the Security Standards for Smart Devices Fact Sheet, the responsibility for compliance will rest with manufacturers and suppliers, not retailers. Retailers should not be expected to carry additional regulatory burdens beyond verifying that manufacturers provide statements of compliance.

The ARA and NRA acknowledges that the Department of Home Affairs has already indicated its intention to align security standards with the ETSI standard EN 303 645, which is a well-established European standard with international relevance. While this provides useful clarity, retailers will require practical and accessible guidance to ensure compliance, particularly smaller businesses that may lack in-house cybersecurity expertise. Enforcement mechanisms must ensure that responsibility remains with manufacturers rather than shifting to retail businesses.

We note that the standards extend to *devices that consumers use every day, such as smart TVs, smart watches, home assistants, baby monitors, and consumer energy resources.* We strongly emphasise that many of these products are manufactured, and distributed years in advance, and therefore, we strongly urge the Department to consider that there must be a reasonable extension of time for retailers to continue to supply and sell these products. For example, the Department may consider that current stock of items can be sold for up to five or six years from the legislated enforcement date.

Recommendation: The ARA supports security-by-design principles but calls for clear compliance guidance including resources that specify the obligations of manufacturers, what information retailers should expect from manufacturers, and the potential impact and software changes that consumers may expect. Additionally, there must be strict enforcement of manufacturer responsibilities, and a phased implementation approach over five years, to avoid disruption.

We note that the Department, under the regulations, will have the power to enforce a formal stop, and recall notice, and result in publication on a public website. We emphasise that it is important to provide clear, critical information for all suppliers, and critically to provide culturally and linguistically diverse resources and fact sheets for manufacturers, suppliers and retailers.

Ransomware Reporting Obligations

The ARA and NRA acknowledge that mandatory ransomware reporting requirements have already been set in legislation, with a $3 million annual turnover threshold for reporting entities. Businesses that make ransomware payments will be required to report within 72 hours of payment or becoming aware that a payment has been made, as confirmed in the Ransomware Reporting Fact Sheet.

Given that the Joint Committee on the Cyber Security Act recommended an education-first approach to enforcement, the ARA and NRA believe that compliance will depend on the government providing clear, practical guidance, on how and when to report ransomware

payments. Retailers should have access to standardised reporting templates and advisory support to ensure they meet obligations without unnecessary complexity.

We note that under ATO guidelines, the definition of a small business includes businesses that generate less than $10 million in annual turnover. The $3 million classification system is not clear and requires further industry consultation. We note that many franchisees and small businesses do not have the resources, time, or staff to understand the significance of, or how to report cyber security incidents, and critically how to recognise phishing, or scamming.

Recommendation: The ARA and NRA urge the government to prioritise clear reporting guidelines, providing information on what constitutes a cyber-attack, phishing attack, or information or money related scam, ongoing industry engagement and clear, concise instructions on how to report attacks, and a clear, established form that is easy to access and understand, national reporting tool. Critically, we emphasise that an education-first approach to compliance, as recommended by the Parliamentary Joint Committee.

We recommend that the Department engage with small and medium enterprises (SMEs) to understand the assistant, and resources that are required to support reporting mechanisms and critically, to prevent fines or penalties being placed on businesses unnecessarily.

Cyber Incident Review Board

The Cyber Incident Review Board (CIRB) has been established as a no-fault body, meaning businesses will not face penalties for participating in post-incident reviews. Reviews will be conducted to assess significant cyber incidents and make recommendations to improve national resilience, rather than impose enforcement actions.

To maintain confidence in the CIRB's work, the ARA and NRA supports ensuring that participation remains voluntary, and that confidentiality of shared information is protected. Retailers must have assurances that sensitive business information disclosed during reviews will not be used for regulatory enforcement purposes. A strong industry engagement strategy, and appointment of representatives from industry bodies, and small and medium enterprise (SME) owners is necessary to ensure the private sector sees value in voluntary participation.

Transparency around renumeration must be prioritised, and we note, must fall within reasonable expectations. Many board positions are voluntary, and the expectation from the businesses sector will be that the board serves to educate and communicate with industry, as opposed to receiving large remuneration packages.

Recommendation: The ARA and NRA support the formation of the CIRB but maintains that participation should remain voluntary, with strong confidentiality protections in place to ensure trust in the process. Additionally, the Review Board must include representatives from industry, particularly from the Small Business sector, and industry body representatives. We do not believe a penalty will compel businesses to provide information to the Chair of the Board is the best approach, and instead, recommend that businesses are provided with an opportunity to understand the associated risks of an attack, and why it is important to provide information to a voluntary body. The Cyber Incident Review Board must have clear parameters, and effectively communicate with industry to encourage businesses to be forthcoming with cyber-related incident information.

Data Storage Systems and Critical Infrastructure Risk Management

The Data Storage Systems Rules only apply to entities connected to critical infrastructure, rather than broadly to all businesses storing sensitive data. As confirmed in the Data Storage Systems Fact Sheet, the changes focus on ensuring business-critical data storage linked to critical infrastructure meets security obligations.

The ARA and NRA seek clear confirmation that standard retail data storage systems will not be captured under these rules. While large retailers operate significant customer databases, their systems should not automatically be classified as critical infrastructure unless they meet strict, risk-based criteria. If a retailer is classified under these obligations, a grace period should be sufficient for compliance adjustments. In addition, ongoing industry consultation is required, to ensure the process is efficient, fit-for purpose and can be streamlined. Critically, retailers must be able to provide guidance to customers on the new requirements and how this information will be used and stored.

Recommendation: The ARA and NRA support enhancing data security protections but calls for clear definitions on applicability, a risk-based approach, and explicit confirmation that retail businesses without direct links to critical infrastructure will not be classified under these obligations.

Telecommunications Security Rules & Critical Telecommunications Assets

The Telecommunications Security Rules and Critical Telecommunications Asset Amendments bring telecommunications security under the Security of Critical Infrastructure Act (SOCI Act). As stated in the Telecommunications Security Fact Sheet, the new Telecommunications Security and Risk Management Program (TSRMP) will apply only to a subset of critical telecommunications assets rather than all businesses with telecommunications networks.

The ARA and NRA remain concerned about the potential for large e-commerce platforms and cloud systems to be captured under these regulations, which could impose unintended compliance burdens on retailers. Given that the government has outlined a bespoke risk management program for these assets, further engagement is required to determine if major retailers running cloud-based retail operations could be classified as critical telecommunications entities.

We note that compliance and enforcement will fall under the SOCI Act, and critically, that businesses may be liable for penalties and enforcement under the Act. We emphasise that businesses must understand their obligations, and how to communicate this internally, establish procedures, and critically, inform customers of the required changes and subsequent obligations to be borne by businesses.

Recommendation: The ARA and NRA seek additional engagement to determine if major retail platforms could be captured under these rules and urges the government to provide further clarity on applicability. Additionally, ongoing consultation with industry to understand the resources, equipment and technology that will be required to comply, and report, must be a priority for the government.

Limited Use for the National Cyber Security Coordinator

The ARA and NRA support efforts to foster trust and collaboration between businesses and the government, to ensure that sensitive information shared during cyber security incidents is handled appropriately with strict confidentiality, and for the sole purpose of increase cyber resilience. We note that the role of the National Cyber Security Coordinator is to work collaboratively with industry to address, and mitigate serious cyber related incidents.

Conclusion and Key Recommendations

The ARA and NRA supports efforts to enhance cyber security resilience but maintains that regulatory measures must be proportionate, practical, and aligned with existing frameworks. We share the following concerns, and request that the Department consider the following, potential risks to businesses.

Security Standards for Smart Devices:

- **Compliance Requirements:** Small businesses involved in manufacturing, importing, or selling such devices must ensure their products comply with these standards, which may necessitate updates to product designs and security features.
- **Obligations to Provide Compliance Statements:** Businesses are required to supply a statement confirming compliance with the security standards for their products. This adds an administrative responsibility, potentially increasing operational costs for small enterprises.

2. Ransomware Reporting Obligations:

- **Mandatory Reporting:** In the event of a ransomware attack resulting in payment, businesses are obligated to report the incident to the relevant authorities. While this requirement aims to enhance national cyber threat intelligence, it will inadvertently impose additional reporting duties on small businesses. Additionally, businesses do not have enough information to understand what constitutes a cyber or phishing attack, and how to diligently recognise, address, and report an attack. We note, that many businesses are not aware of an attack, until considerable time after the event has occurred. We emphasise that education is the best approach to mitigate the risk to businesses, and so they can report attacks.

Potential Implications for Small Businesses:

- **Increased Compliance Costs:** Adhering to new security standards and reporting obligations may lead to higher operational expenses, which could be challenging for small businesses with limited resources.
- **Administrative Burden:** The need to maintain compliance documentation and submit incident reports may require additional administrative efforts, diverting resources from core business activities.

To ensure that these regulations achieve their intended outcomes without unnecessarily burdening retailers, the government should:

- Provide clear guidance and phased implementation for security standards on smart devices, ensuring alignment with international frameworks and maintaining enforcement at the manufacturer level.
- Ensure ransomware reporting obligations are practical, with clear reporting templates, advisory support, and an education-first compliance approach.
- Maintain voluntary participation in the Cyber Incident Review Board to encourage collaboration while safeguarding business confidentiality and include Board representatives across the SME and retail sectors, and industry bodies.
- Define clear thresholds for data storage system regulations, applying a risk-based approach and confirming that standard retail data storage systems will not be classified as critical infrastructure.
- Ensure telecommunications security requirements do not result in increased costs for retailers and provide industry-specific guidance on compliance expectations.
- Further assess whether large e-commerce and cloud-based retail platforms could be unintentionally classified as critical telecommunications entities.

The ARA and NRA welcome further engagement with the government to ensure that cyber security obligations are fit for purpose and effectively support retailers in strengthening cyber resilience without creating unnecessary compliance challenges. For further discussion, please contact policy@retail.org.au