18 November 2022

The Hon Clare O'Neil MP
Minister for Home Affairs
Minister for Cyber Security
Parliament House
Canberra ACT 2600

via email: ci.reforms@homeaffairs.gov.au

Dear Minister,

RE: CRITICAL INFRASTRUCTURE REFORMS – RISK MANAGEMENT PROGRAM

The Australian Retailers Association (ARA) welcomes the opportunity to provide comments in relation to the Department of Home Affair's consultation on the Risk Management Program (RMP) component of the reforms to critical infrastructure security and resilience obligations.

The ARA is the oldest, largest and most diverse national retail body, representing a $400 billion sector that employs 1.3 million Australians and is the largest private sector employer in the country. As Australia's peak retail body, representing more than 120,000 retail shop fronts and online stores, the ARA informs, advocates, educates, protects and unifies our independent, national and international retail community.

In this context we are representing our members who are subject to the regulatory framework as it applies to the food and grocery sector.

In principle, we strongly support the need for RMP Rules to ensure Australia's grocery supply chain is protected from foreseeable hazards and risks and our members are appreciative of the level of guidance and information sharing that has been made available by Home Affairs through the Trusted Information Sharing Network (TISN) framework.

The ARA is concerned, though, that the timelines for the food and grocery sector RMP compliance might be brought forward and that a commencement date before the end of 2022 may be under consideration. While our members are actively working towards compliance and forming a clear understanding of their obligations, there is concern that implementation could likely require more time than Government anticipates. Also relevant is that the busy Christmas trading period typically corresponds with an IT blackout period to reduce the impact of change on busier than normal operations, and that the past few summers have been materially interrupted by major weather events.

The ARA recommends that the RMP Rules commence no earlier than March 2023, with announcement of the commencement date to be provided as soon as reasonably practicable to allow time for sufficient budget and resource planning.

We also have concerns around the six-month 'grace period' to comply with the RMP portion of the obligations. We respectfully suggest that a 12-month grace period would be more appropriate, noting that this would not prevent the work starting as soon as the rules commence, but rather allow time to implement the RMP properly. We note that in most instances, organisations may need to obtain Board review and approval for resources that have not been forecast or budgeted for this financial year.

In particular, some of the rules contain obligations which will require significant implementation and ongoing management, including:

Requirement	Impact on Business
Establishing a process to identify and maintain a list of all 'critical workers' (including contractors) (s9).	This will require IT system upgrades. Clarification around which employees are 'critical workers' is also sought as this has the potential to impact significantly on compliance costs.
Establishing a process for assessing the suitability of critical workers on an ongoing basis (s9).	This will potentially require changes to contractual arrangements with third parties. Some employees will potentially require re-assignment due to this requirement. The process will also require the resources of HR management to administer and manage with employees and unions.
Minimising/eliminating the material risks that negligent and malicious insiders may cause to the functioning of critical assets (section 9).	We note that the scope of this obligation is quite broad and is not limited to critical workers.
Minimising/eliminating the material risks from a wide range of specified Supply Chain Hazards (section 10).	This will require close engagement with suppliers throughout the supply chain and potentially require the renegotiation of contracts with many of them.

The ARA recommends that additional time is allowed for compliance with these obligations and that further consideration be given to narrowing the scope of some requirements to make them less onerous.

The ARA also notes the requirement to comply with a cyber-security framework, recommended as being one endorsed by a government or international organisation. However, for large organisations, cybersecurity approaches often require a mix of frameworks rather than any single framework to provide a bespoke solution to unique cybersecurity challenges. We would wish to seek guidance on the criteria the government will use to assess equivalence frameworks, including in scenarios where an organisation uses a combination of frameworks

Finally, we note that the 18-month timeframe for compliance with a cyber-security framework is also somewhat challenging and consider that 24 months (with a potential option to provide progress updates) would be more realistic given that our members maintain highly complex networks of IT systems and applications.

In summary the ARA recommends:

- The rules for the food and grocery sector not commence until at least March 2023
- The grace period for adopting and complying with an RMP be 12 months (not 6 months)
- The grace period for adoption and compliance with one of the prescribed cyber security frameworks be 24 months (not 18 months)
- The government issue further guidance on baseline criteria for equivalence frameworks

Thank you again for the opportunity to provide comments. We would be happy to discuss the issues raised above in more detail and any queries in relation to this submission can be directed to our policy team at

Yours sincerely,

Paul Zahra
Chief Executive Officer