AUSTRALIAN RETAIL COUNCIL

Let's talk shop.

Level 29
31 Market Street
Sydney NSW 2000

Proposed amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act* 2018

May 2026

The Australian Retail Council (ARC) welcomes the opportunity to provide feedback to the Department of Home Affairs consultation regarding the proposed amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act* 2018 (SOCI Act).

ARC represents the Australian retail sector. Valued at $444 billion, the retail sector is the largest private sector employer in the nation. Retail employs more than 1.4 million Australians (one in ten workers) and is the single largest employer of young Australians aged 15 to 24 years.

ARC's membership spans the full breadth of Australian retail: from family-owned small and independent businesses, comprising 95 per cent of our membership, to large national and international retailers supporting thousands of jobs and sustaining communities across metropolitan and regional Australia. The sector operates more than 155,000 retail outlets nationwide, with the majority also represented by an online or e-commerce presence. A significant portion of every dollar spent in retail flows back to employees, suppliers, superannuation funds, and local communities.

ARC is committed to supporting Australian retailers by collaborating and advocating for policy and reform that drive growth, resilience, and long-term prosperity for Australian retail and the millions who rely on it.

General comments

This feedback is submitted on behalf of ARC members who are designated as "responsible entities" under the SOCI Act as they own, operate, or have direct interest in critical infrastructure assets. Our members seek a regulatory framework which proportionately balances regulatory burden, with productivity and operational efficiency. We also note that individual operators need to have processes and systems which are fit for purpose in the industries they operate in, and a blanket approach to regulation, including in relation to cyber threats, may not be fit for purpose.

The proposed amendments to the powers of the Minister under Part 3 of the SOCI Act, are significant for the food and grocery sector. They represent a broad and significant expansion of Government powers to intervene in the governance (and operations) of the sector, including on an ongoing basis. In our view, the expansion of these powers:

- may impact good governance and decision-making processes,
- duplicate other legislative and regulatory frameworks,
- impact relationships with suppliers (risking competitive advantage or disadvantage, and customer trust), and
- impose new layers of regulatory compliance and complexity, on an already heavily regulated sector.

Level 29
31 Market Street
Sydney NSW 2000

Given the highly interdependent food and grocery sector, including in relation to both physical and digital infrastructure, clear guidance regarding the implementation of any such directions or conditions will be critical. For example, where a direction requires action that depends on, or must be carried out by, a supplier, how does the obligation apply? If compliance requires an entity to act in relation to a supplier, is that supplier also bound by the direction, and if so, by what mechanism? Guidance should also address post-incident disclosure expectations, including coordination and reporting to relevant regulators.

ARC also has concerns regarding the potential negative consequences flowing from compliance with Ministerial directions. There can be negative consequences resulting from entities taking directed action including financial costs and exposure to contractual claims. However, it is unclear where the liability sits for the consequences of actions taken at the direction of the Government.

Additionally, where SOCI obligations cut across other regulatory regimes, such as the *Corporations Act*, ASIC rules, ASX Listing Rules, the *Privacy Act*, and directors' duties, clear legal safe harbours should apply, or duplicative reporting obligations should be reduced through a "report once" framework.

Detailed submissions

1. Measure 2: We understand this power will enable the Minister to impose targeted, fit-for-purpose "conditions" on supermarket retailers where ownership, control, or governance arrangements create a "material risk to national security that cannot be sufficiently mitigated through existing regulatory obligations or voluntary measures".

   This proposed measure is incredibly broad and has the potential to conflict with other legislative frameworks, including under the *Corporations Act and* for Ministerial directions to impact good governance processes and decision making.

   In particular, many of the illustrative examples of conditions that could be imposed would be extremely prescriptive and burdensome on entities to implement. The most concerning examples, outside of the board-related examples conflicting with the Corporations Act, are:

   - Requirements to implement specified cybersecurity baseline controls. Without a clear definition of what 'baseline controls' entail, such conditions could be extremely extensive in scope, as the definition in what is considered baseline by the cyber security industry is constantly shifting. Imposing prescriptive, externally defined baseline controls risks overriding entities existing, sophisticated risk-management frameworks, potentially forcing the adoption of redundant or incompatible security architectures at significant and unnecessary expense.
   - Mandated segregation of critical systems, networks, logs, or sensitive data from parent company or shareholder environments, including prohibitions on offshore access, support, or administration for critical systems. Mandating the physical and logical segregation of critical systems from established parent-company environments may impose prohibitive costs on entities by forcing the wholesale duplication of infrastructure and security architectures. Furthermore, prohibiting offshore access and administration would severely constrain the ability of entities to leverage global technical expertise and 24/7 "follow-the-sun" support, potentially increasing operational risk by creating isolated, less resilient silos of maintenance.

Level 29
31 Market Street
Sydney NSW 2000

Examples of conditions that have the potential to conflict with the *Corporations Act* include a condition to exclude a director/s from voting that may impact critical entity decision making and undermine the role of the board. Decisions that materially affect the security posture of an asset such as procurement, network architecture, operational arrangements, or high-impact financial decisions linked to asset resilience. Further, directions regarding board positions for security-cleared directors, may impact timely decision-making about board composition and could undermine the ability of Australian companies to appropriately leverage global talent pools for their boards.

2. Measure 3: The proposed "high-risk vendors, products or services direction power" will enable the Minister to issue targeted directions to responsible entities, either individually or by class.

   If exercised, the effect of this power can force the removal or restriction of a vendor which could result in serious operational impacts on entities and the products they supply. We request that the criteria for the identification of "high-risk vendors" be transparent, clear and objective.

   Also, in relation to the Ministerial decision-making process, to ensure the Minister is aware of the impacts and consequences of any proposed direction, a thorough impact analysis would be essential prior to the making of any such direction, including in consultation with the sector. Supermarket retailers operate in highly integrated environments, and the removal or restriction of one component can have wide reaching impacts and costs.

   Additionally, the power to make directions to isolate, segment or remediate identified technologies; and/or implement compensating security controls, would similarly place massive operational and capital burdens on a responsible entity.

   We also note that it is proposed that directions would accommodate "reasonable transition timeframes". This accommodation is critical. Ministerial directions that result in the removal, remediation or restrictions of products, equipment, services or technologies are significant disruptions to embedded supply-chains and may expose entities to contractual claims. Even minor changes to supply chains may require significant capital expenditure and require multi-year lead times. Vendor concentration, limited substitutability and global supply chain constraints may restrict diversification options in certain categories.

3. Measures 4: This proposed power enables a temporary delay to the public disclosure of cyber incidents that could threaten national security or public safety.

   ARC does not support this measure as we are concerned that the impacts of delaying an official ASX disclosure could lead to market speculation, share price volatility and, in the context of retail, in-store panic buying and potential civil unrest. This measure would likely act in conflict with commensurate transparency obligations for other reporting regimes, such as notifiable data regimes in Australia and overseas. This may mean that market sensitive information could be made publicly available, prior to an ASX disclosure. There needs to be a clear mechanism within Government for managing ongoing and clear public messaging to mitigate any customer and public trust issues that might arise to mitigate the impacts of any delay. The solution is not simply delaying an ASX disclosure, particularly in a situation where the existence of a cyber incident may be disclosed other than through official channels.

AUSTRALIAN RETAIL COUNCIL

Let's talk shop.

Level 29
31 Market Street
Sydney NSW 2000

Alternatively, any such power to delay an ASX disclosure should instead be able to be optionally exercised by the responsible entity, who is in the best position to determine whether it is appropriate and reasonable to exercise such delay, in conjunction with consultation with the Government on any national security risks that may be associated with such disclosure.

4. Measure 5: The proposal to increase civil penalties under the SOCI Act is not supported. We do not agree that the current penalty does not provide a credible compliance incentive, especially in the context of an ambiguous, broad-reaching cyber security regulatory framework. Australian supermarket retailers have sought to comply with the SOCI Act and taken proactive steps to address material risks and hazards.

Thank you again for the opportunity to participate in this consultation. Please direct any queries in relation to this submission to our policy team at policy@retail.org.au.