



1 May 2026

By Upload.

Dear Sir/Madam

Re: Ministerial Directions Powers Consultation Paper

AFMA welcomes the opportunity to provide comment on the Consultation Paper on the *Proposed Amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act*.

We support the Australian Government's initiative to develop its capacity to respond quickly to national security threats, in particular technology and cyber threats, while maintaining the original goals of 'restraint, legitimacy and coherence across the SOCI framework'.

AFMA is keen that the framework for proactive advice and intelligence distribution amongst potentially at-risk entities continues to be developed, and, given the complex interdependencies within the economy, we see benefit in developing wider distribution channels for prompt delivery of security information during incidents to all potentially affected or relevant service providers.

Once the Government has assessed the feedback from this consultation and crafted the Exposure Draft, we would support further consultation on that draft given the potential impact to the industry or individual firm if the amended legislative power is used.

Across all the proposed changes, to assist the industry and Government assess the calibration of the proposed changes we request Home Affairs consider drafting a comparison of legislative or other solutions implemented in other jurisdictions and the associated impacts, advantages, and disadvantages of each option.

We thank you for considering our comments in relation to each proposal below.

Yours sincerely

Damian Jeffree

Head of Financial Markets, Exchanges and Digital

Measure 1 - Amendments to the existing directions power in section 32

AFMA supports the proposed amendments in principle.

The industry would benefit from examples of how a 'material risk' and 'a direction is reasonably necessary and proportionate' would be determined.

Further information on how assessment and/or verification of whether actions associated with a direction are sufficient would be achieved, including whether the timeframes for implementation will be agreed or imposed, and where the division for associated costs for such actions would be drawn. Firms should not be required to pay costs that are unreasonable in the circumstances.

We note that 'Where entities choose to make disclosures required under other laws, they may reference a direction where legally necessary and consistent with protected information-handling obligations under the SOCI Act.' We note that the use of a direction may indicate there is a 'material risk' for the organisation and this may need to be disclosed to regulators and potentially relevant stock exchange(s).

We request that more information be given about the interaction with director duties and management responsibilities and their respective liabilities.

AFMA suggests that consideration be given to standard sunset arrangement for directions.

Where an entity chooses or is compelled to make disclosures under other Australian or overseas laws further information is requested on the required interaction with the Australian Government and whether limitations may apply if the direction is subject to secrecy.

AFMA requests more information on how the Government would work with firms indirectly impacted by requirements due to the affected organisation's position in relevant supply chains.

We note that financial institutions subject to requirements such as CPS 234 have an obligation to report a material control weakness that they are unable to remediate in a timely manner. We request consideration be given to the view that a direction under this measure could be interpreted to indicate or imply a material control weakness.

Measure 2 – Conditions Power

AFMA supports the proposed measure and supports the proposals to require the Minister be satisfied conditions are 'reasonably necessary to mitigate or eliminate the risk, and that good-faith efforts have been made to negotiate a voluntary solution with the affected entity or individual before a direction is given'. We also support the requirement to require the review of conditions directions within 12 months and thereafter at least every 24 months.

We seek more information on how 'reasonably necessary' is intended to be defined and how compliance with the targeted conditions would be verified and who would bear any related costs.

Further information on how assessment and/or verification of whether actions associated with a condition are sufficient, including whether the timeframes for implementation will be agreed or imposed, and where the division for associated costs for such actions would be drawn.

Members note that some directors may need access to certain information to fulfil their duties and that some directors who are also employees will be exposed to information as a part of their role.

Measure 3 Restrictions on the use of high-risk vendors, products or services

AFMA supports the proposal in principle. We request further information on how the Australian Government would manage an orderly removal of technologies or services where there is national security risk.

Where an organization also operates outside of Australia and therefore has technologies deployed globally, the industry will need practical solutions that can be implemented within a reasonable timeframe. AFMA seeks more information on the intended scope and boundaries of any such direction, for example would it be limited (or typically limited) to Australian-entity relevant data or operations?

For global organisations with group-wide services it is possible that such a change to different technology could take multiple years and require significant cost, even if limited to Australia relevant infrastructure. AFMA requests that the framework allows for a negotiated transition period to achieve compliance. This would help ensure changes can be implemented safely and in an orderly manner, without unintended impacts on customers or operational resilience.

Measure 4 - Delay continuous disclosure requirements

AFMA members note that the use of Option 2, a new power under the SOCI Act is likely to provide more clarity and cater for other unforeseen circumstances. It would automatically override other requirements for disclosure and this simplicity can be helpful during incidents.

In the US there is a Securities and Exchange Commission (SEC) rule on public company cybersecurity disclosures that provides for delay of the disclosure "if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing."^[1] The rule also caters for further delay in the disclosure. The US financial services industry is currently seeking improvements to the US mechanism. Financial services are highly regulated and must comply with multiple regulatory regimes,

^[1] [SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies.](https://www.sec.gov/news/press/2018/20180814.htm)

in addition to any applicable delay mechanism. Sector-specific regulators may be well-placed to promptly process and approve disclosure delays in line with existing supervisory frameworks.

A new power under the SOCI Act accessible by both the Minister (where initiated by the Government) and the sector regulator (on request from the relevant firm) could provide the flexibility needed by the Government while benefiting from refinements suggested by the US experience.

We recommend that Home Affairs consider the experience of firms requesting disclosure requirements in the United States and consider using sectorial regulators such as APRA and ASIC to assist where firms wish to apply for delayed disclosure.

AFMA suggests that careful consideration also be given to support information sharing with other organisations to be able to respond to the incident and share incident intelligence.

The interaction of the disclosure delay may interact with disclosure requirements many firms have in other jurisdictions. For example, it is noted that the Coupang data breach incident has resulted in a consortium of U.S. investment firms submitting a notice of intent in late January 2026 to inform the South Korea's Ministry of Justice that they intend to launch an Investor-State Dispute Settlement against the South Korean government¹.

Measure 5

AFMA seeks confirmation that if a 'direction' composed of multiple actions to achieve the desired outcome will be treated as one direction in relation to penalties. For example, to move to a new technology may require multiple actions, including interim measures before the final strategic solution is implemented.

¹ [Coupang investors seek US probe over South Korea's handling of data leak | Reuters](#)