31 July 2026

By Upload.

Dear Sir/Madam

Re: Streamlining and Modernising the Security of Critical Infrastructure Act 2018

AFMA welcomes the opportunity to provide comment on the Consultation Paper on the *Streamlining and Modernising the Security of Critical Infrastructure Act 2018*.

AFMA is in general supportive of the proposed changes, which should help to refine the operation of the scheme. The *SoCI Act* is not a set and forget, and we expect it will continue to benefit from regular review and updating as the information security field matures.

While we appreciate the importance of prompt updates to the SoCI Act as the need arises, we note that the four-week consultation period for a 104-page Consultation Paper with 111 questions over a school holiday period limits the potential for the consultation process to be effective.

Our key concerns are as follows:

Measure 17 – Operations and Maintenance and Managed Service Providers

In relation to this measure AFMA agrees that 'The most widespread cost is expected to be the updating of contracts, because it affects existing service agreements.'[1] The renegotiation of contracts is expected to be a large and potentially challenging project.

The safe harbour provisions are welcome and necessary. Where there is limited commercial leverage, particularly where the service provider is located outside of Australia, we seek assurance that the provisions will make appropriate allowances for regulated entities.

Measure 15 – CIRMP Governance and Assurance

AFMA objects to the admissibility of mandatory annual compliance reports as evidence in civil penalty proceedings. This would be an unfortunate foundational change in the regulatory stance and is an entirely separate issue from the views on the inadequacies of penalties in the *Independent Review of the SOCI Act Final Report* (the *Review*). The advantages of preserving the capacity for candid information flows by having separation of regulatory enforcement functions, by mechanisms such as the inadmissibility of compliance reports, was not considered in the Review. We believe

[1] Page 82 Consultation Paper

Australian Financial Markets Association
ABN 69 793 968 987
Level 18, 45 Clarence Street GPO Box 3655 Sydney NSW 2000
Tel: +612 9776 7907 Email: secretariat@afma.com.au Web: www.afma.com.au

these were well-considered when the Act was first drafted and this good work should not now be now undone.

The inadmissibility of these reports is a critical design feature of the SoCI regime, and a major benefit to its operative effectiveness and ensuring the correct collaborative regulatory stance of the Australian Government in relation to information security. The proposed changes are incompatible with the Explanatory Memorandum to the SOCI Act.

The SOCI Act is thoughtfully designed from a regulatory theory perspective. We encourage Home Affairs to take a sophisticated view of what is needed from its interactions from the industry and how the regulatory function is best performed, and ultimately what is in Australia's best interests.

There is no doubt that in Australia regulators across multiple areas of law continue towards enforcement agency arrangements. Under such arrangements, all interactions with the regulator, including mandated compliance reporting interactions of the type under consideration in this consultation, are not shielded from enforcement use against the firm.

While on the surface this appears to have efficiency benefits for the enforcement functions of regulators and can increase the level of fines levied on Australian companies by those regulators, it is not generally in the interests of Australia as a whole. The costs of an enforcement-agency approach are very real and were recognised in the current design of the SOCI Act through the inadmissibility structures.

Firms and industry bodies interact very differently with enforcement agencies than they do with a trusted regulator which has clear separation of functions. Under a traditional regulator structure where the regulator is in good standing, our direct experience is that firms will often go above and beyond to contribute to the common good and provide the regulator with important intelligence on industry developments, risks, and potential solutions. Interactions with enforcement agencies, will in contrast, seek to fully satisfy all legal requirements. Given their fiduciary obligations and the interests of the firms, there are legal restrictions and serious costs in risking going any further.

As AFMA noted in our submission to the Cyber Security Strategy consultation, the better approach generally, but particularly in cyber security, is to align with the approach taken in air safety. Home Affairs should place a premium on the insights that firms can provide in an environment where information can be provided with less risk of punitive action.

As we noted in our previous submission:

> The…key to making cyber security work is to recognise that businesses are already strongly incentivised to get cyber right, that in some cases, for example those involving state actors, the challenge level can be extremely high. We encourage the recognition that an accommodative, supportive stance is the most likely to keep channels of communication and information flow open, and is most likely to support a swift uplift in standards.

Measure 1 – Exemptions Framework

AFMA has consistently supported a single common graded approach to regulated requirements around information security. We have suggested that international standards such as NIST and ISO could be valuable in this regard.

Where regulator standards are prescriptive, they risk becoming out of date with current global best practice. We have particularly supported ASIC's approach which makes good use of international standards.

AFMA supports the exemptions framework and specifically seeks confirmation that APRA's CPS 230 and CPS 234 standards are sufficient alternative regulatory frameworks in most areas and as a result that measures 3, 15, and 19 do not apply to APRA regulated entities.

We do note, more generally, that the multiple competing and inconsistent regulatory frameworks complemented by an overlay standard with exemptions, will become increasingly cumbersome over time and its patchwork approach may risk gaps arising.

AFMA seeks confirmation that banking firms (and others subject to APRA's regulations) are not subject to the CIRMP as APRA's regulations provide an equivalent framework. Where these firms are required to 'secure appropriate arrangements'[2] we seek confirmation that this would be in relation to CPS 230.

Measure 8 – Data Storage or Processing Capture Pathways

AFMA requests clarification whether the current notification of data storage and processing supplier by an entity will be retained.

Measure 20 – Specified Risk Information

AFMA is interested in how the specified risk information will be required to be considered for financial services where a principles- and risk- based approach is in place.

AFMA suggests that the requirement to consider the material that is identified as specific published risk, hazard, standards or guidance material, be for firms to '*undertake a one-off process that considers whether on a risk basis these matters should be included in their CIRMP governance, review and assurance processes'.*

Measure 21 – Critical Workers and Critical Components

AFMA does not object to this proposal but we note that in the context of financial services, the services are a 'virtual' asset which means large segments of an organisation may be captured. Broad roles and criteria, for example staff with security-sensitive access, or staff with operational authority may risk capturing large staff populations unless carefully refined in the final drafting.

We thank you for considering our comments in relation to the proposed Measures.

Yours sincerely

Damian Jeffree
Head of Financial Markets, Exchanges and Digital

[2] Page 78 Consultation Paper