AUSTRALIAN INSTITUTE of SUPERANNUATION TRUSTEES

27 August 2021

Department of Home Affairs
4 National Circuit
BARTON ACT 2600

Via online submissions portal

Dear Sir/Madam,

Re: Strengthening Australia's cyber security regulations and incentives

In brief: AIST is supportive of efforts to strengthen corporate governance of cyber security risk across the economy. However, the current regulatory settings in the superannuation sector can respond to emerging cyber related governance risks.

About AIST

Australian Institute of Superannuation Trustees ("AIST") is a national not-for-profit organization whose membership consists of the trustee directors and staff of industry, corporate and public sector superannuation funds.

As the principal advocate and peak representative body for the $1.5 trillion profit-to-members superannuation sector, AIST plays a key role in policy development and is a leading provider of research.

AIST advocates for financial wellbeing in retirement for all Australians regardless of gender, culture, education, or socio-economic background. Through leadership and excellence, AIST supports profit-to-member funds to achieve member-first outcomes and fairness across the retirement system.

As an industry association representing the interest of the profit-to-member superannuation sector, our comments are limited to the issues around the imposition of mandatory governance standards for larger businesses and minimum standards for personal information.

General comments

Superannuation trustee directors are acutely aware of the need to appropriately manage cyber security risks within their respective funds. Trustee directors are required, by law, to act in the best financial interest of members. Safeguarding super fund assets from a cyber security incident is consistent with this duty. Similarly, ensuring that a fund's systems and processes are properly instituted to appropriately respond, manage, and report on cyber security incidents is further

Level 23, 150 Lonsdale Street
Melbourne VIC 3000

T +61 3 8677 3800
F +61 3 8677 3801

info@aist.asn.au
www.aist.asn.au

consistent with this duty. There is also further obligation for a trustee to act with care, skill and diligence in the operation of a superannuation fund, and part of meeting this is ensuring cyber risk is managed appropriately

In recognition of this important area of risk, trustee directors who participate in AIST's Advanced Trustee Director Course are required to undertake a risk module that involves a cyber security component. This module involves a simulation exercise where directors are required to respond to a cyber-attack within a superannuation fund. Exercises such as this ensure that trustee directors are made aware of the impact a cyber-attack may have on a fund and equip them with the practical knowledge and skills to respond to a cyber incident. AIST would welcome collaboration with Home Affairs on this training material to ensure that future directors are supported in their cyber security skills.

Superannuation funds are also required to comply with several prudential standards relevant to cyber security. These regulatory standards include CPS 321 - Outsourcing, CPS 232 – Business Continuity, CPS 234 – Information Security and SPS 220 – Risk Management. Collectively these prudential standards provide a comprehensive framework on how superannuation funds respond to both physical and cyber based security threats.

Governance standards – Cyber Security

What is the best approach to strengthening corporate governance of cyber security risk? Why?

Strengthening corporate governance of cyber security risk can be achieved through a series of mechanisms. Two of the three options canvassed in the consultation paper are likely to have an impact on the way management and the board respond to cyber security risk. AIST rejects the notion that the status quo option yields no benefits. The current regulatory standards in the superannuation industry are sufficiently comprehensive. The recently proposed Security Legislation Amendment (Critical Infrastructure) Bill 2020 will further enhance cyber security capabilities across the targeted industries (including superannuation).

We note that regulatory instruments and broader compliance is not the only approach for strengthening corporate governance. Awareness and education are effective tools for improving governance around cyber security risk. To better achieve this department should consider engaging with industry associations and professional bodies to collaborate on education and awareness initiatives aimed at managing cyber security risk.

What cyber security support, if any, should be provided to directors of small and medium companies?

Directors of small and medium size companies may require additional support in safeguarding their businesses from cyber security threats. These organisations should be supported as best they can without the imposition of further burdensome regulations.

Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Increased collaboration between government and relevant industry associations would be an effective way to develop education and awareness initiatives for senior business leaders. Information sharing between government and the private sector will improve the overall content of the education and awareness programs and continue to strengthen responses to cyber security risks wherever they emerge.

Minimum standards for personal information

Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

The development of a cyber security code under the Privacy Act may be an effective way to promote the uptake of cyber security standards in certain industries. The superannuation industry has a robust regulatory framework that suitably governs fund operations. The imposition of a cyber security code, particularly in the superannuation industry, will likely result in a more complex and costly regulatory environment. Moreover, security by its very nature works as much on observation as it does protection. Some of the requirements of security directly oppose the *principles* of the Privacy Act by its nature (monitoring email, decrypting web traffic, investigations etc.). Embedding a cyber security code within the Privacy Act risks undermining both the intents of the privacy legislation and the goals of security – particularly if cyber security exemptions are incorporated into the legislation. It may be more appropriate to develop industry specific guidelines on how assets need to be protected.

Notwithstanding, Section 34C of the Superannuation Industry (Supervision) Act 1993 provides the industry regulator APRA with the power to determine prudential standards. If regulatory gaps exist, these gaps could be addressed through updated prudential standards. This may be a more appropriate alternative than the development of an industry wide cyber security code.

We further note that it would be premature to consider the imposition of a cyber security code under the Privacy Act before the critical infrastructure rules have been finalised.

For further information regarding our submission, please contact Samuel Lynch on [redacted] or via email at [redacted].

Yours sincerely,

[redacted]

Eva Scheerlinck
Chief Executive Officer