AUSTRALIAN INSTITUTE of SUPERANNUATION TRUSTEES

1 February 2022

The Hon Karen Andrews MP
Minister for Home Affairs
Parliament House
CANBERRA ACT 2600

Email: ci.reforms@homeaffairs.gov.au

Dear Minister,

Protecting our Critical Infrastructure and Systems of National Significance - Financial Services and Markets sector - Mandatory Cyber Incident Reporting

Security of Critical Infrastructure (Application) Rules 2021

In brief: The Australian Prudential Regulation Authority (APRA) should be named in the Explanatory Statement for the proposed *Security of Critical Infrastructure (Application) Rules 2021* as the relevant Commonwealth body for reporting cyber incidents relating to critical superannuation assets.

About AIST

Australian Institute of Superannuation Trustees is a national not-for-profit organisation 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 $1.4 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.

Name APRA as the relevant Commonwealth body for cyber-incident reporting

AIST welcomes the opportunity to make a submission on the proposed Rules relating to mandatory cyber incident reporting (Part 2B of the Security of Critical Infrastructure Act 2018 Act) for certain assets.

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

AIST submits that the Explanatory Statement for the proposed Security of Critical Infrastructure (Application) Rules 2021 made under section 61 of the Security of Critical Infrastructure Act 2018 be amended to explicitly identify the Australian Prudential Regulation Authority as the 'relevant Commonwealth body' for responsible entities of critical superannuation assets to report cyber security incidents.

This should be included as a new paragraph following existing paragraphs 4 and 9 of the Explanatory Statement, and as a new paragraph after the fourth paragraph on Section 5 Application of Part 2B of the Act.

Rationale

Where the obligations for risk management programs are to be delivered through superannuation-specific arrangements, this should be aligned with existing regulatory frameworks as far as possible and appropriate.

In the case of superannuation, the obligations in the Explanatory Statement to the Rules should specifically reference APRA as the relevant Commonwealth body for the reporting of cyber-security incidents.

APRA's existing prudential framework, and prudential standards, provides the basis for regulatory compatibility. These include CPS 321 (Outsourcing), CPS 232 (Business Continuity), CPS 234 (Cyber-security), and SPS 220 (Risk Management).

Not only would this mean that the framework was consistent with existing industry requirements in order to reduce regulatory burden, it would allow it to evolve in an efficient manner, while achieving the desired security outcomes.

For further information regarding our submission, please contact AIST Senior Policy Manager David Haynes at [redacted]

Yours sincerely,

[redacted]

Eva Scheerlinck
Chief Executive Officer