SUBMISSION

Submission to Department of Home Affairs — Strengthening Australia's cyber security regulations and incentives consultation

3 September 2021

The Association of Superannuation Funds of Australia Limited
Level 11, 77 Castlereagh Street
Sydney NSW 2000

PO Box 1485
Sydney NSW 2001

T +61 2 9264 9300
1800 812 798 (outside Sydney)
F 1300 926 484
W www.superannuation.asn.au

ABN 29 002 786 290 CAN 002 786 290

File: 2021/27

The Manager

Department of Home Affairs

GPO Box 241

MELBOURNE VIC 3001

AUSTRALIA

Via email: techpolicy@homeaffairs.gov.au

3 September 2021

Dear Sir/Madam

Strengthening Australia's cyber security regulations and incentives consultation

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to the *Strengthening Australia's cyber security regulations and incentives* consultation.

ASFA is a non-profit, non-political national organisation whose mission is to continuously improve the superannuation system, so all Australians can enjoy a comfortable and dignified retirement. We focus on the issues that affect the entire Australian superannuation system and its $3.1 trillion in retirement savings. Our membership is across all parts of the industry, including corporate, public sector, industry and retail superannuation funds, and associated service providers, representing almost 90 per cent of the 16 million Australians with superannuation.

If you have any queries or comments in relation to the content of our submission, please contact me on (02) 8079 0808 or by email gmccrea@superannuation.asn.au, or Byron Addison, Senior Policy Advisor, on (02) 8079 0834 or by email baddison@superannuation.asn.au. We would welcome the opportunity to discuss our submission and look forward to engaging with you throughout the process to strengthen Australia's cyber resilience.

Yours sincerely

Glen McCrea
Deputy Chief Executive Officer and Chief Policy Officer

A. General observations

ASFA is broadly supportive of any measures that will protect essential services through the enhancement of cyber security and resilience. As the consultation paper points out the finance sector, including the superannuation industry, is a mature regulatory regime with regard to cyber risk (p.13), and many of the proposals in the consultation paper are already largely met under this regime or not of direct relevance to the superannuation industry.

However we would like to make a few general observations about this initiative and its relationship to the superannuation industry and its related service providers.

Regulatory harmonisation

For obvious reasons cybersecurity, along with other threats to critical infrastructure, is attracting considerable and increasing attention from the Government and the regulators, as well as their counterparts overseas. We welcome this however it does pose the threat of overlapping regulation, confused lines of authority and responsibility, and the potential for duplication.

We acknowledge that in this consultation, as well as other critical infrastructure consultations, the Department of Home Affairs has identified as a first priority the need to avoid regulatory overlap and duplication and we do not doubt that every effort will be made to incorporate this into the cyber and critical infrastructure reforms. However in a rapidly evolving domestic and international regulatory environment we consider that it would be beneficial to identify a single regulator for the financial sector with primary responsibility for ensuring regulatory harmonisation.

In our view, APRA should be recognised not only as the regulator primarily responsible for managing risk, including cyber, for the superannuation industry but also as the regulator responsible for ensuring harmonisation between the various regulatory layers that apply to cyber risk and risk more generally. This will support efficiency and is consistent with APRA's role as a prudential regulator with responsibility for the soundness and security of the financial system.

APRA's role in ensuring regulatory harmonisation would have to take account of all the domestic players including the Department of Home Affairs and its related bodies as well as the other regulators such as ASIC and the ATO. It should also have regard to international standards which many local service providers with foreign interests are required to observe.

Unregulated entities

The superannuation system is a complicated ecosystem with many different players and a variety of business models. The Gateway Network Governance Body (GNGB) has developed a chart, as part of its Securing the Future research project, which describes how complex the system is and the great number of players there are in the industry (see Attachment A).

One of the threats to the industry is the potential for the unregulated service providers to be unwitting points of access for cyber attacks to the regulated parts of the superannuation system.

ASFA is committed to exploring ways of strengthening the system's defences against cyber attacks and has launched a number of initiatives in this area. We are grateful for the involvement of Department of Home Affairs' representatives in these initiatives and we look forward to working with the department in the future, and in particular to explore ways to strengthen every part of the ecosystem to ensure every link in the superannuation industry chain is of equal strength.

Gateway Network Governance Body

Diagram 1

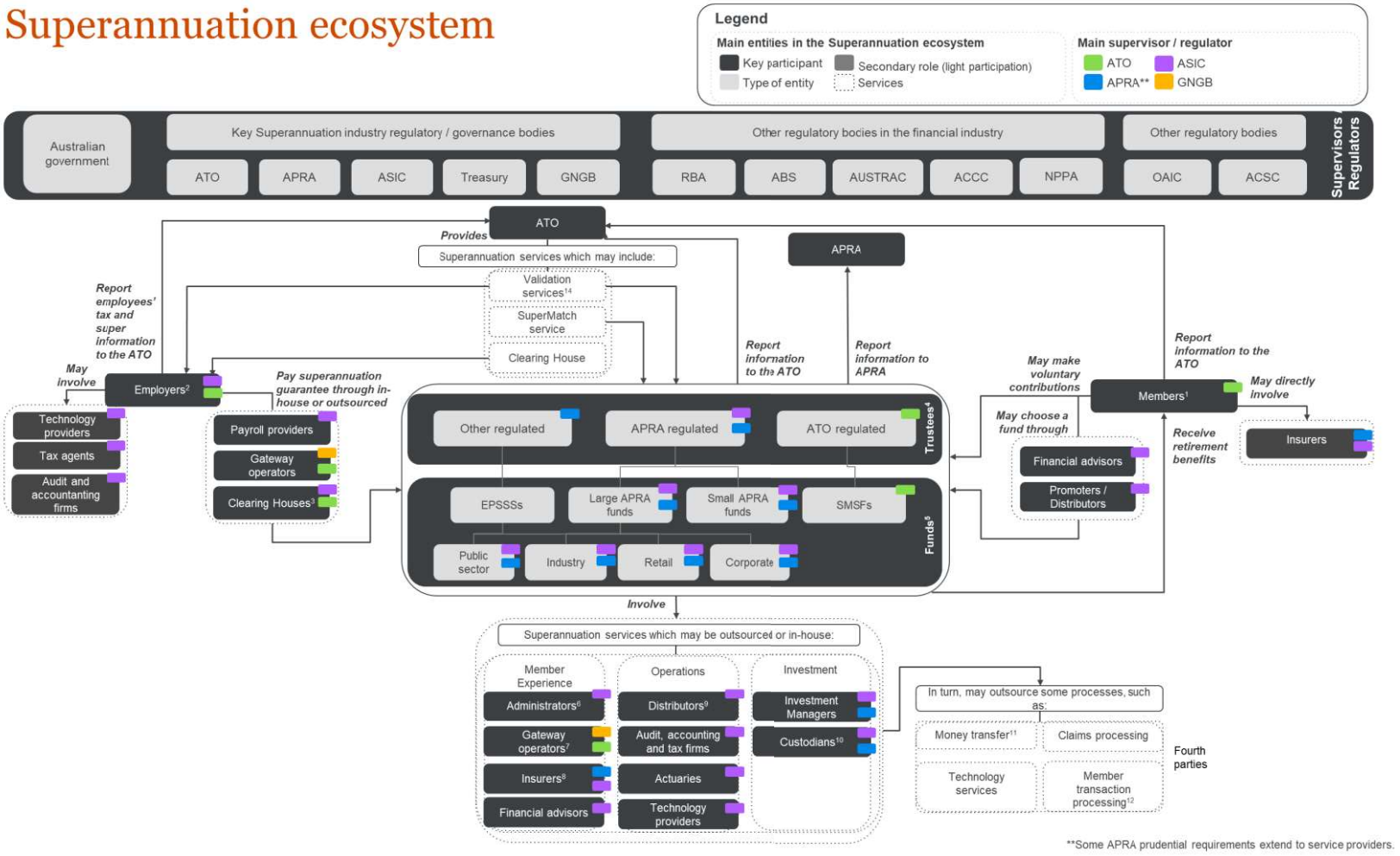

Diagram 1 outlines the complexity of the superannuation ecosystem and its regulatory environment. Coloured squares on each entity designates its main regulator(s) which in a large number of cases is ASIC in relation to Corporate Governance. ASIC cyber security objectives are largely currently met via the enforcement of Director accountabilities and duties.