Australian Unity
271 Spring Street
Melbourne VIC 3000
T 13 29 39
F 03 8682 5555
W australianunity.com.au

27 August 2021

Department of Home Affairs
(via online submission)

Australian Unity submission

Strengthening Australia's cyber security regulations and incentives

Thank you for the opportunity to comment on the Australian Government's discussion paper, *Strengthening Australia's cyber security regulations and incentives*, on options for regulatory reforms and incentives to strengthen the cyber security of Australia's economy.

With a history of over 180 years, Australian Unity delivers health, wealth and care products and services to over 700,000 customers each year. Our range includes private health and general insurance; banking and financial services; wealth and investment products; aged and disability care; and dental and allied health services. Established in 1840, we were Australia's first member-owned wellbeing company and continue our mutuality to this day—providing us with the freedom to invest back into services and solutions that matter most to our members, customers and the Australian community.

With our breadth of financial and personal service offerings across an extensive and diverse customer cohort, Australian Unity is particularly cognisant of its obligations when managing and protecting personal and financial information and data. We have similarly high expectations of our suppliers, partners and other stakeholders in regard to information and cyber security.

Australian Unity welcomes the Government's commitment to supporting a growing digital economy—and noting a growing threat environment—and offers three points for consideration:

(1) It is not necessary, nor desirable, for additional regulatory requirements relating to the management of cyber security risks to be introduced for entities already regulated by the Australian Prudential Regulation Authority (APRA) or regulated by the Australian Securities and Investments Commission (ASIC) with an Australian Financial Services License (AFSL).

(2) The introduction of a cyber security voluntary code or guiding principles for those not already regulated by APRA or the holder of an AFSL and regulated by ASIC is supported to provide assurance to customers, suppliers and the general public and to strengthen Australia's collective efforts to mitigate cyber security related risks.

(3) It is not necessary, nor desirable, for any further or enhanced governance requirements that may be imposed by Government to alter the existing roles and responsibilities of directors in relation to cyber security.

Commentary

(1) It is not necessary, nor desirable, for additional regulatory requirements relating to the management of cyber security risks to be introduced for entities already regulated by APRA or regulated by ASIC with an AFSL.

To avoid unnecessary regulatory complexity, overlap or potential conflict, Australian Unity considers additional regulatory requirements relating to the management of cyber security risks where an entity or holding entity is regulated by APRA or ASIC with an AFSL is not required.

The Australian Unity Group contains multiple entitles, including Australian Unity Limited which is a Non-Operating Holding Company, that are directly regulated by APRA and required to comply with APRA's Prudential Standard CPS 234 Information Security and other complementary standards for Business Continuity and Outsourcing which also support cyber risk management.

In addition to our entities directly regulated by APRA our non-APRA regulated businesses also consequently comply with many of the CPS 234 requirements given many of our support functions and capabilities are centralised. We consider CPS 234 to provide comprehensive and adequate governance over cyber security risk management for our Group.

CPS 234 is a risk-based standard, which seeks to strengthen an entity's resilience against information security issues, by minimising the likelihood and impact of information security incidents on the confidentiality, integrity or availability of internally and externally managed information assets. The standard requires a focus on testing and continuous review and improvement of controls to reflect the changes to the entity's business environment.

In force since July 2019, CPS 234 has been extensively embedded into Australian Unity's governance and operations arrangements. The below table provides a summary of the key requirements of CPS 234 and the practical outcomes of the application of the standard across our business—demonstrating the adequate coverage of CPS 234 as a cyber security regulatory framework. The requirements apply to all APRA regulated entities and we anticipate that the practical outcomes are similar for such entities.

CPS 234 key requirement	Practical outcome for Australian Unity
APRA expects the Board of the entity to be ultimately responsible for information security management	The responsibility of the Australian Unity Group Board and management for information security is clearly set out in the Group's *Information Security Management Framework*, which is supported by an *Information Security Policy* that clearly outlines the roles and responsibilities of the Board and management for managing information security. An *Annual Cyber Security Plan* is tabled at the Board for review each year and the Board is kept informed by management of any material security incidents or control weaknesses as they are identified or arise.
The entity is expected to maintain an information security function that is commensurate with the risk profile of the entity. This also includes scenarios where the entity may have chosen to outsource its information systems management	The Annual Cyber Security Plan outlines the resourcing and tools implemented to support the Group's information security capability. The Plan reflects the outcome of an annual risk assessment and a controls assurance testing program performed each year, which together support the overall assessment of the Group's cyber risk profile and the approach to managing cyber security risks. Where elements of the technology environment are outsourced, the risk assessment and controls assurance are extended to include third-party control assurance reviews.
The cyber security risk assessment performed on information assets is expected to reflect both the criticality and sensitivity of the underlying information asset and the interests of various stakeholders	Australian Unity defines 'information assets' broadly as "*any key element of information technology that includes software, hardware and data (both soft and hard copy)*". The Group's information asset classification scheme is based on: • the impact of system loss to the business (*criticality*), and • the underlying data that will be stored and managed via the system (*sensitivity*). The Group has also developed processes, supported by policy and procedures, to address scenarios where a third party manages information assets on behalf of the Australian Unity Group or our subsidiaries.
The organisation must implement information security controls that are commensurate with cyber risk profile of the entity	Benchmarking controls in the entity against an international framework is a key element of our cyber security risks assessment framework. The Group currently benchmarks our control environments against the widely-considered best practice NIST Cyber Security Framework. Controls are continuously reviewed on an annual basis to refine and add/remove controls depending on the Group's changing cyber and technology environment and risk profile.
APRA expects the entity to have mechanisms in place to detect and respond to incidents and ensure that incidents are reported in a timely manner to management and board.	Australian Unity has robust technology incident management and security incident management processes in place. Our security management process is supported by a Security Operations Centre (SOC) and the Security Incident Response Team (SIRT). We have defined playbooks for key common cyber threat scenarios which provide and inform detailed response plans. These playbooks are regulatory practiced throughout the year and are

APRA also expects predefined response plans or playbooks to be maintained which are reviewed and tested annually	reviewed and updated at least annually. Data breach response plans are also in place with supporting governance and notification protocols to our regulators and stakeholders, including APRA, Office of the Australian Information Commissioner and the Australian Securities and Investment Commission (ASIC).
APRA expects a formal program of controls assurance testing is maintained that is commensurate to the risk profile of the organisation	Australian Unity has implemented an IT Controls Assurance Program that is run independently from those within the business who have developed or operate the controls via our second-line Risk and Compliance Team across key technology and information security controls. A level of independence is maintained in the Assurance Program execution between the Information Security Team. The Assurance Program also reviews controls where third parties manage information assets on our behalf. This can include the test of additional internal mitigating or compensating controls that have been specifically designed for areas where the third-party controls assurance is limited.
APRA expects the entity's internal audit function to be able to review the design and operating effectiveness of information security controls	The scope and coverage of Australian Unity's Internal Audit program includes information security controls as well as oversight across the execution of the IT Controls Assurance Program noted above.
APRA expects to be notified of material incidents or control weaknesses within a prescribed time.	The Incident Management and Data Breach Response processes guide the notification of incidents to external regulators, including APRA.

The requirements of APRA's CPS 234 provide a robust, suitable and well-established cyber security regulatory framework for APRA regulated entities, such as Australian Unity.

In addition to being regulated by APRA, the Australian Unity Group also contains multiple entities regulated by ASIC with AFSLs, some of which have been appointed as Responsible Entities for Management Investment Schemes (MIS). To meet obligations set out by ASIC in Regulatory Guides 104 and 259, we are also required to have risk management systems in place that identify, assess and manage all material risks of the business and each MIS operated. In today's business environment it is almost inconceivable that any entity with an AFSL would not consider cyber risk to be a material risk to its business or any MIS it operates.

We consider that requirements to manage cyber risk for entities regulated either by APRA or by ASIC with an AFSL should be taken into consideration by the Government to avoid any unnecessary regulatory overlap or confusion.

(2) The introduction of a cyber security voluntary code or guiding principles for those not already regulated by APRA (or other regulatory regimes) is supported to provide assurance to customers, suppliers and the general public and to strengthen Australia's collective efforts to mitigate cyber security related risks.

Where entities are not regulated by APRA or similar regulations or legislation, Australian Unity supports the introduction of a voluntary compliance regime consisting of principles that support management of information security based on the risk profile of an entity.

We consider that a risk-based approach that recognises scale, size of operations and allows for development across industries provides a better outcome for business of varying sizes and complexity. Where there is no, or limited, existing regulation, we support the introduction of clear minimum expectations for businesses to manage cyber security, guided by *principles* that are applied based on *risk* and supported by demonstrable *controls testing*. Specifically, we would encourage and support the introduction of:

- **Principles** similar to the Commonwealth Government's *Essential Eight* principles expanded to address all key control areas for cyber security in line with international frameworks, such as the NIST Cyber Security Framework, to support a consistent minimum standard of cyber security risk management.
- **A risk-based approach to compliance** to those principles, involving a formal information security risk assessment and appropriate controls being put in place to support a minimum standard. Entities

could be encouraged to call out specifically the principles that are being excluded and their rationale.

- **Testing of controls** through an independent assurance program should be encouraged for entities to confirm/demonstrate compliance with the principles. For instance, depending on the size and complexity of an entity, controls testing could be required to be performed independently to the control developers and operators. In most larger entities, this independent testing could be performed by internal risk and compliance functions or internal audit. Entities should be encouraged to demonstrate their testing of controls in the same manner in which controls managed by third parties have been reviewed and assessed.

Entities who conform to a voluntary regime could be publicly listed or accredited as doing so, which would provide assurance to buyers, other suppliers and the general public dealing with the entity. Australian Unity would see benefit in this in supporting our procurement, supply and partnership activities.

(3) It is not necessary, nor desirable, for any further or enhanced governance requirements that may be imposed by Government to alter the existing roles and responsibilities of directors in relation to cyber security.

Existing legislation and legal principles provide adequate guidance and expectations in relation to the role of directors in overseeing the management of cyber and other risks. We do not consider it necessary, or desirable, to increase directors' obligations over and above existing duties, including those set out in sections 180 and 181 of the *Corporations Act 2001* (the Act). Additionally, it is appropriate to maintain a distinction between the functions of directors and management.

Section 180 of the Act requires directors to discharge their duties with due care and diligence and section 181 of the Act requires directors to act in the interests of the company. It has been well established by the court that these duties require directors to have regard to the company's activities, policies, circumstances, environment and known business risks.

In the context of cyber security, and depending upon the nature of the entity, we consider that these duties already require directors to, amongst other things:

- have oversight across an entity's cyber security profile, including ensuring there is an appropriate cyber security strategy, framework and policies in place commensurate with the risks faced by the entity;
- have an understanding of the cyber risks and vulnerabilities relevant to the entity, review and challenge the cyber security risks and strategy of the organisation;
- understand applicable legal and regulatory obligations;
- ensure cyber security is a topic of regular board discussion;
- monitor the effectiveness of management's implementation of the cyber security strategy, including the allocation of sufficient resources;
- review and assess the outcome of performed testing undertaken by management;
- awareness of security incidents and any remediation activities.

As detailed above, directors also already have specific cyber-security related responsibilities if they are a director of an APRA regulated entity. Additionally, directors of publicly listed companies already have specific additional cyber-security obligations with regard to reporting breaches and disclosing risks.

We consider that the following should remain the functions and accountabilities of management:

- implement the entity's cyber-security strategy effectively;
- designing and implementing specific tools and controls to manage cyber risk;
- allocating resources to manage the risks and execute the strategy;
- undertaking adequate testing;
- reporting on security incidents and undertaking remediation activities;
- review relevant relationships with partners, suppliers and affiliates.

Australian Unity views the preservation of these accountabilities is essential to strong governance arrangements.

Again, on behalf of Australian Unity, I thank you for the opportunity to provide comment. Should you wish to further discuss any aspect of our submission, please contact Alison Bright (General Manager, Group Risk and Compliance) on [redacted] or [redacted].

Yours sincerely

[redacted]

Rohan Mead
Group Managing Director & CEO
Australian Unity