File Name: 2018/17

15 June 2018

General Manager, Policy Development

Policy and Advice Division
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001

via e-mail to: PolicyDevelopment@apra.gov.au

Dear Sir/Madam,

Re: Consultation on *Information security management: A new cross-industry prudential standard*

The Association of Superannuation Funds of Australia (ASFA) is lodging this submission in response to the consultation on APRA's *Information security management: A new cross-industry prudential standard.*

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 $2.6 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 over 90 per cent of the 14.8 million Australians with superannuation.

General observation

ASFA is appreciative of the opportunity to provide comments as part of the consultation on the *Information security management: A new cross-industry prudential standard*.

ASFA supports the introduction of a new prudential standard to strengthen the existing information security requirements for RSE licensees and we welcome any initiative that will help to protect member information.

A common observation made by our members is that it will take time to work out the practical effect of the new requirements and consequently it is difficult to estimate their impact on RSE licensees' systems and resourcing. We have received some cost estimates from members which suggest that there will be significant immediate and recurrent costs. While this of itself provides no reason to question the proposal we urge APRA to consider the costs involved in conforming with the new information security regime and to minimise the impact wherever possible.

ASFA also recommends that consideration be given to the proposed compliance deadlines and that either flexibility or a staggered approach be adopted. A number of our members have suggested that the proposed timeframes will be difficult to achieve particularly where third or related parties are involved.

We would also like to draw attention to the broader reporting and transaction framework in which RSE licensees operate and the need to consider information security not only at the RSE licensee and related party level but also in the wider context. RSE licensees are required to report and transact member specific and other more aggregated data to a range of government agencies including but not limited to the ATO, APRA, ASIC and the Department of Health and Social Security. RSE licensees also receive member information from a range of sources such as gateways, employers, clearing houses, payroll (software) providers, custodians, financial institutions and other funds, some of whom will be bound by APRA's Prudential Standards and some of whom will not.

The Australian superannuation system is also part of an international or global system that has many points of interconnection and it is from this source that many of the risks to the security of member information may come. We recommend that APRA keeps this broader context in mind when assessing fund performance and compliance.

On this topic we would like to make three observations:

1. RSE licensees should be held to account only for those activities undertaken directly or by third or related parties for which they are responsible and a clear distinction recognised where the RSE licensee is the recipient of data by providers over whose information security standards the RSE licensee has no control or influence, including some agencies such as the ATO where legislation[1] requires superannuation funds to send and receive data from the ATO as part of processing member contributions and benefits.

2. While this is tangential to the consultation on the proposed prudential standard we are of the view that the existing patchwork reporting framework between various government agencies represents a security risk to the government and fund members. Alignment between the different agencies that currently collect, manage and in some instances send data would greatly assist in dealing with cyber security threats in a coordinated way.

   As we have argued previously in our letter of 11 April 2018 concerning the D2A replacement Project, this coordinated approach to data collection and exchange and its protection against cyber and other threats could be achieved by the establishment of a body made up of senior representatives from the industry and all relevant government agencies which collect industry data such as the ATO, ASIC, the ABS, APRA and other agencies with IT expertise such as the Department of Finance and the Digital Transformation Agency. We note that the Productivity Commission (PC) has recommended a similar approach (Draft recommendation 22 of the Superannuation: Assessing efficiency and competitiveness PC Draft Report) and while acknowledging the PC's focus is on efficiency we would suggest that it would also greatly strengthen the protections for information security held by government agencies.

[1] Superannuation Data and Payment Standards 2012

3. Whole of Government approach to security and information management - ASFA agrees with the group application approach so that entities that have more than one business that are APRA regulated can leverage off the investment in information security across its different business lines. To avoid unnecessary and costly investment in managing connections with and between different agencies it is important that all agencies adopt, where practical, a consistent approach in respect of security and information management. For example, the ATO has adopted its Operational Framework which applies to all digital service providers and which "…is part of our response to these risks and establishes how we will provide access to and monitor the digital transfer of data through software." Yet, it is still unclear whether this Framework is ATO specific or will be adopted by all agencies.

Specific comments

ASFA would like to raise the following issues with respect to APRA's *Information security management: A new cross-industry prudential standard*:

1. Scope

1.1. The Proposed scope of CPS 234

Draft Prudential Standard CPS 234 is proposed to apply to '*RSE licensees under the SIS Act in respect of their business operations*' (Paragraph 2(e) of draft CPS 234). It notes that an RSE licensee's business operations include '*all activities as an RSE licensee…and all other activities of the RSE licensee to the extent that they are relevant to, or may impact on, its activities as an RSE licensee*'.

The definition appears to suggest a very broad application to superannuation businesses, extending to wholly-owned subsidiaries and partially-owned businesses of a RSE licensee.

The proposed scope of CPS 234 application to superannuation business needs to be well considered and clarified, for example the degree to which it applies to controlled entities and related entities of RSE licensees.

1.2. The need for flexibility in compliance deadlines

A number of ASFA members have indicated that the 1 July 2019 commencement date will be difficult to comply with in full. Funds will also need to update existing contracts and where outsourced providers use other suppliers those contracts would also need to be amended, all of which will take time. This process is made more difficult by the lack of detail regarding what the compliance requirements will mean in practice.

ASFA also suggests that APRA consider softening compliance deadlines where a merger is in the process of being completed or under active consideration as work on updating systems and contracts could be costly and time-consuming for little long-term benefit.

A specific example of what may cause a delay is provided:

<u>Classification of information assets</u>
CPS 234 paragraph 19 requires an APRA-regulated entity to classify its information assets (including those managed by related parties and third parties) by criticality and sensitivity. Information asset means *information and information technology including software, hardware and data both soft and hard copy*.

Given both existing and new information assets need to be classified, this will be a monumental task from an implementation perspective as it needs to be business-led, supported by an enterprise-wide change management and the use of an Enterprise Content Management Solution.

The proposed 1 July 2019 start date would pose implementation challenges if RSE licensees are expected to be fully compliant by the start date. A pragmatic approach should be adopted such that RSE licensees have a reasonable transition period to formulate an implementation roadmap and work towards a state of full compliance by the end of the transition period.

1.3. APRA notification of a material security incident

As specified in draft CPS 234 paragraph 34, APRA-regulated entities are required to notify APRA as soon as possible and no later than 24 hours after *experiencing* a material information security incident. Information security incident is defined as '*a confirmed or potential compromise of information security*'.

We question the reasonableness of this timing requirement as APRA regulated entities or their related party or third party providers may not have detected an information security incident within 24 hours of it occurring. Equally they may not have the necessary information to determine that the incident is material within the proposed 24-hour timeframe.

We note that the requirement to notify APRA no later than 24 hours after experiencing an information security incident does not align with the 30 day requirement to notify the Office of the Australian Information Commissioner under sub-section 26WH(2) of the Privacy Act.

In addition, it should be recognised that APRA regulated entities are often dependent on related or third party providers for notification of any potential compromise of their information security and the manner in which notification is made can depend on the obligations to report set out in the contract. These situations are not wholly within the control of APRA regulated entities but would give rise to a technical breach of this requirement.

ASFA recommends that the 24-hour notification requirement relate to when an APRA regulated entity discovers or becomes aware of an information security incident which it determines to be material.

1.4. Paragraph 35

In line with 1.3 we question the purpose of the notification required under paragraph 35 and what use APRA would make of the information.

We also would suggest that the five day reporting deadline is unreasonable as the incident may need to be escalated to the Board first together with any actual or potential remedial action. The involvement of the Board may mean that the incident cannot be reported within five days.

The reporting required under paragraphs 34 and 35 could present a risk in the sense that incidents are reported that turn out not to be material or not to have warranted being reported once all relevant facts have been assembled and understood. This could be a waste of the fund's and APRA's time and distract from matters of genuine security significance.

1.5. Technical matters

Our members have raised a number of technical questions relating to the draft CPS 234 where clarification is required:

- Footnote 5, page 5 - This suggests that all information security issues for material outsourced providers are dictated by CPS and SPS 231 rather than CPS 234. Does this mean the notification requirements under CPS 234 do not apply to material outsourced providers?

- Paragraph 25 – Is it expected that the annual confirmation that its information security response plans are effective should form part of the Risk Management Declaration?

- Paragraph 27 - If all third parties are to be tested, this places a financial impost on the fund, the third party or both. APRA need to have a materiality requirement for testing.

- Paragraph 27 – Some third parties, particularly smaller operations such as mail houses and printers, do not have testing performed on their information security controls. Paragraph 27 should indicate what its expectations are in these circumstances.

- Paragraph 28 – There is no materiality requirement in terms of how serious the control deficiency must be before it gets reported to the Board and senior management. Is this intended?

- Paragraph 33 – The requirement that internal audit must assess the information security control assurance provided by that party does not account for the fact that some third parties do not have assurance conducted by themselves. This paragraph should account for circumstances where the fund gets its own assurance.

- Paragraphs 33 and 34 – The references to 'materially affect, financially or non-financially, the entity or the interests of beneficiaries'. Is the term beneficiaries intended to cover them as a group, a sub-section of all the fund's beneficiaries or is it measured based on the impact on individual beneficiaries?

2. Costs

As suggested in the Discussion Paper ASFA has referred its members to the Commonwealth Regulatory Burden Measure tool to assess the costs of implementing CPS 234.

We have received anecdotal evidence which suggests that there would be significant one-off and recurrent costs in changing oversight and monitoring, reporting and other systems. One fund has estimated that the initial cost would be $3.2 M and the recurrent annual cost would be $500,000.

The other consideration is that the detail for some of the requirements is not yet clear or available and it is therefore difficult to be definitive about the likely costs.

ASFA supports CPS 234 but we urge APRA to be conscious of the costs the new standard will represent for funds and to minimise the regulatory burden of this important reform wherever possible.

Greater clarity and guidance from APRA in terms of making reference to readily adopted standards pertaining to security and information management will provide greater certainty and consistency for funds and suppliers and therefore reduce cost.

3. Implementation guidance

A number of ASFA members have suggested that there is little practical guidance on how the new requirements should be implemented and this makes it difficult to assess project compliance timelines and costs. We presume that this guidance will be provided in CPG 234 and we ask APRA to note that it will take RSE licensees time to deal with the practical implications of the new standard and we urge APRA to provide as much practical guidance as possible to help RSE licensees understand the extent and the application of the new requirements.

****

We would like to thank you for the opportunity to provide comments on the *Information security management: A new cross-industry prudential standard*.

Should you have any questions on any of the matters raised in this submission please do not hesitate to contact me on (02) 8079 0808 or gmccrea@superannuatiuon.asn.au or Byron Addison on (02) 8079 0834 or baddison@superannuation.asn.au.

Yours sincerely

Glen McCrea
Deputy CEO and Chief Policy Officer