AMERICAN INSURANCE ASSOCIATION

555 12th Street NW
Suite 550
Washington, DC 20005
202-828-7100
Fax 202-293-1219
www.aiadc.org

June 20, 2018

General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority

Dear Sir or Madam:

The American Insurance Association (AIA) appreciates the opportunity to submit our views on the Australian Prudential Regulation Authority's (APRA) draft proposed Prudential Standard CPS 234, Information Security (CPS 234).

The AIA is the leading property-casualty (non-life) insurance trade organization in the United States, representing more than 330 companies, which collectively write more than $134 billion in premiums each year**.** AIA member companies, which include the most globally-active insurers, have operations in more than 70 countries, serve customers in more than 170 countries and territories, and offer all types of property-casualty insurance products.

Though we are submitting these comments after the requested submission date, we hope that they will nonetheless be helpful to you. Data security is a priority issue for the insurance industry, and, as such AIA broadly supports the key objective of the proposed standard, "to minimize the likelihood and impact of information security incidents on the confidentiality, integrity, or availability of information assets". However, having consulted with our member companies, we have identified concerns about unintended consequences that may result from the regulations envisioned in the draft. We believe regulatory oversight should be balanced in a manner that is risk-based, flexible, clear and consistent to enhance resiliency. Therefore, we respectfully offer the following observations and recommendations for your consideration.

1. Compliance with obligations by group resources outside of Australia

CPS 234 imposes a number of obligations on APRA-regulated entities to take measures to minimize the risks associated with information security as defined in CPS 234. Our members seek clarification that, for international insurance groups, certain obligations under CPS 234 could be met using expert group resources located outside Australia. For instance, to centralize expertise and efficiently manage global security risks thereby enhancing global and APRA-regulated entity corporate resiliency, APRA-supervised entities may access and rely on group IT resources outside of Australia to meet certain of the requirements in CPS 234. We submit that this approach should be sufficient to satisfy the requirements of CPS 234 while noting that the APRA-supervised entity, together with its Board, would remain ultimately responsible for ensuring that APRA's requirements are met.

2. Classification of information assets – paragraph 19, CPS 234

While the concept of classifying information assets by criticality and sensitivity has merit and suggests an element of flexibility and risk analysis, we are unclear as to what the difference between criticality and sensitivity and if these two concepts are distinct. Therefore, we recommend introducing an overlay of practicality and reasonableness. For example, 'Where practical and reasonable to do so, an APRA-regulated entity must…'. Such an approach would take into account the diversity of information assets.

3. Information security controls for assets held by other parties - paragraph 20, CPS 234

Clause 20 states that the entity itself shall have information security controls to protect its information assets, including those managed by related and third parties. A strict reading of Clause 20 suggests that the APRA regulated entity must implement security controls for the related and third party assets. At a practical level this would seem somewhat impossible given the number of APRA regulated entities that a third party may have a relationship with. The third party could not successfully implement specific security demands from individual APRA-related entities. We respectfully suggest that it should be sufficient for an APRA-regulated entity to determine that its related or third party has information security controls of the type detailed in the draft clause 20. This approach appears to be the intention of clause 20 as clause 21 requires an APRA-regulated entity to evaluate the design and operating effectiveness of that party's information security controls.

4. Definitions

As drafted, the definitions of Information Security Incident and Information Asset are too broad. These are critical definitions for understanding and managing the scope of the obligations outlined in the document. We believe the definition of Information Security Incident is broad enough to include routine instances that are unlikely to cause any material harm. Corporate IT systems are under attack and pinged numerous times a day but because of systems and protocols put in place they will not lead to any material harm. Because of the broad definition, which references the potential to compromise information security and the reporting obligations, APRA may be inundated with meaningless notifications.

Similarly, the definition of Information Asset can be construed to include essentially any business information of an APRA regulated entity or any information about a consumer that such entity has obtained. This definition would require entities to divert human resources and capital to implement IT controls for assets that have no likelihood of causing harm. Arguably, this harms rather than fosters resiliency efforts.

Amendments to narrow the scope of these definitions and to add a definition of the sensitive information to the regulation may help manage some of the unintended consequences of this regulation.

5. Reporting Requirements under paragraphs 34 & 35, CPS 234

Paragraphs 34 and 35 effectively provide for four discreet reporting requirements. Overall, we recommend these requirements be consolidated and, as appropriate, take into account existing mandatory reporting requirements applicable to APRA-regulated entities under Australian law or in operation in other jurisdictions. Our specific concerns are highlighted and discussed in further detail below.

Draft paragraph 34.

(The reference to 'depositors, policyholders, beneficiaries, or other customers' is referred to in this submission collectively as stakeholders.)

> *An APRA-regulated entity must notify APRA as soon as possible, and **no later than 24 hours**, after **experiencing** an information security incident that:*
>
> *(a) materially affected, or **had the potential** to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers; or*
>
> *(b) has been notified to other regulators, either in Australia **or other jurisdictions**.*

Draft paragraph 35.

> *An APRA-regulated entity must notify APRA as soon as possible and no later than five business days after identifying a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.*

Timing – 24 hours

Paragraph 34 requires notification to APRA no later than 24 hours. We believe that this timeframe is too short given the effort APRA regulated entities would be engaged in at that time to comprehend, protect from, and remediate the incident. At the very least we would recommend amending this requirement to 72 hours consistent with the European Union's General Data Protection Regulation and emerging United State laws such as the New York Department of Financial Services Cybersecurity Regulation.

Notification Trigger – Experiencing an incident

Paragraph 34 refers to the entity 'experiencing an information security incident' (our emphasis). The expression 'experiencing' is a key concept in identifying the trigger for notification to APRA. However, the meaning of the concept of 'experiencing' is not clear in a technological context or as an event by which to define a requirement for reporting. We suggest that the term

"identification" as used in paragraph 35 or preferably "determination" be used in lieu of "experiencing". Further, we recommend that the concept of "identification" or "determination" be used as the common trigger across all reporting requirements in CPS 234. "Determination" builds in an important harm calculation that will alleviate concerns of over-notification. For instance, there would be an investigation to understand the nature, scope and necessary response measures associated with the incident informing the decision as to whether the APRA regulated entity reasonably believes there has been unauthorized access to and acquisition of personally identifiable information. This concept of determination is used in the GDPR and United States' laws.

Notification Trigger – Potential to materially affect entity or stakeholder interests

The second requirement in paragraph 34(a) relates to the 'potential' to materially affect the entity or the stakeholders. This second requirement is too broad and uncertain. If applied as it is currently drafted, the obligation to report incidents that have the 'potential' to materially affect the entity or the interests of stakeholders would involve the reporting of incidents where the nature of any real risk to the entity or its stakeholders remains largely uncertain at the time of reporting. APRA regulated entities should be given the opportunity to investigate and determine the risk of harm before notifying APRA.

We recognize that there is a distinction between privacy and security, but as illustration of the harm analysis we advocate for, we highlight for your consideration the *Privacy Act (Cth)* 1988 (the Privacy Act). The mandatory data breach notification test under the Privacy Act is a useful reference for APRA in that it balances the risk of harm with the interest in regulated entities having sufficient time to properly investigate the matter. The New York Cybersecurity Regulation has similar materiality tests that trigger notification to the New York Department of Financial Services.

In particular, the Privacy Act generally requires entities to provide notice where there are reasonable grounds to believe that an "eligible data breach" has occurred. An eligible data breach will arise where a reasonable person would conclude that there is a likely risk of serious harm to any of the affected individuals because of the unauthorised access or unauthorised disclosure. If an entity only has reasonable grounds to suspect that an eligible data breach has occurred, the notification obligation will not arise. The concept of a serious risk of harm must be real, and not remote, for it to give rise to an obligation to notify. The Act also builds in a 30-day investigation window to make harm determinations.

Under the Act, entities have 30 days to conduct an investigation to determine whether there are reasonable grounds to believe there has been a serious data breach and notification is required.

Accordingly, we submit that consideration should be given to amending the notification requirements to introduce a similar test allowing regulated entities sufficient time to investigate and assess the 'likelihood' of relevant interests being materially affected before making a determination to notify APRA. We believe such procedures are a more appropriate threshold test for reporting obligations.

Scope – Incident notified to other regulators

Paragraph 34(b) contemplates an APRA-regulated entity reporting to APRA an 'experience' of that entity where notification was made by the entity itself or by a related corporate body in another jurisdiction. If correct, this raises serious compliance challenges for globally regulated groups. First, reporting thresholds vary by global jurisdictions and additionally an experience in another jurisdiction may have no nexus to the APRA regulated entity or its consumers. It does not serve APRA or industry's interests for APRA-regulated entities to report every notification made in other jurisdictions. Industry should have the responsibility and the onus to notify APRA only in respect of relevant matters.

Additionally, the draft provision does not address a situation where an APRA-regulated entity experiences an information security incident in relation to which a notification is made to another regulator sometime in the future (e.g. seven days after the 'experiencing'). On the face of it, the reporting requirement in paragraph 34(b) would not extend to those circumstances as the report must be made within 24 hours of the 'experiencing'. This is likely a drafting issue that APRA may wish to clarify.

Notification of information security control weakness

The test for notification in paragraph 35 does not include an element of detriment or harm. Nor is there a requirement for potential harm or detriment. The language is broad and arguably would require notification of a range of issues. Care should also be exercised in the need for this reporting requirement and protections around any information provided to APRA. Caution should be made to avoid attachments of liability and increasing the vulnerability of a weakness.

Again, we recommend amending paragraph 35 to introduce a form of notification test that draws on the concepts underpinning the mandatory data breach notification-reporting requirement under the Privacy Act. In addition, we suggest that the notification requirement in paragraph 35 can be combined with that part of the notification requirement in paragraph 34(a), which relates to the "potential" to "materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers". As such, the reporting requirements under CPS 234 would be streamlined and effectively reduced to three.

As noted above in relation to the other reporting requirements, consideration should be given to providing entities with sufficient time in which to investigate and assess the nature of an information security control weakness during which time the entity may be able to identify a way to remediate the weakness. We believe it is unlikely that five days would be sufficient for regulated entities to make a meaningful assessment of an information security control weakness, particularly if information must be gathered from multiple sources and expert technical advice is required.

6. Relationship between CPS 231 & CPS 234

Finally, a number of footnotes in CPS 234 mention that certain paragraphs of CPS 234 are not applicable if related or third parties are 'captured as service providers of outsourced material business activities' under CPS 231. Our members believe that CPS 231 may not fully address the subject matter of the relevant paragraphs of CPS 234. The footnotes in CPS 234 may raise questions as to how outsourced providers, as defined in CPS 231, would comply with the various information security obligations under CPS 234.

Thank you again for the opportunity to provide the thoughts of the U.S. property and casualty insurance industry. Please do not hesitate to call on us if we can be of any further help or provide any additional information.

Yours very sincerely,

Stephen Simchak
Vice President and Chief International Counsel
American Insurance Association (AIA)