Ashley Beaudry
Senior International Policy Analyst

June 27, 2018

Ms. Heidi Richards
General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
GPO Box 9836
Sydney NSW 2001
Australia
via policydevelopment@apra.gov.au

Re: APRA Proposed Prudential Standard CPS 234

Dear Ms. Richards:

The American Council of Insurance Insurers (ACLI) is pleased to respond to the Australian Prudential Regulation Authority's (APRA) draft proposed Prudential Standard CPS 234, Information Security (CPS 234). We thank you for the opportunity to submit these comments. We strongly support 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 we believe the APRA's CPS 234 proposes overly prescriptive requirements on life insurers.

ACLI represents approximately 290-member companies dedicated to providing products and services that contribute to consumers' financial and retirement security. ACLI members represent 95 percent of U.S. industry assets, offering life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, dental and vision and other supplemental benefits. As our membership includes companies headquartered in Canada, Europe and Japan as well as the U.S. we believe that our members have a material presence in Australia which is why we wish to engage on this issue.

Financial services companies believe the most effective way to protect their customers' personal information and information technology ("IT") systems is to employ cybersecurity frameworks that are risk-based, flexible, and workable. By contrast, we respectfully submit that the proposed regulation does not appear to reflect this approach and, consequently, poses the following fundamental, overarching concerns:

Burdensome Group Compliance Obligations

Our members seek clarity that, for international insurance groups, certain obligations under CPS 234 could be met using expert group resources located outside Australia. An APRA-supervised entity may access and rely on group resources, including IT infrastructure, to meet certain 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, shall at all times remain ultimately responsible for ensuring that APRA's requirements are met.

Overly Broad Definitions

Information Security Incident

Under the current proposal, the definition of "Information Security Incident" would include numerous unsuccessful attempts to access information assets and daily occurrences of routine network activity and human errors. These occurrences are unlikely to result in material harm to either an APRA-regulated entity or an individual customer. The inclusion of potential or unsuccessful attempts within the scope of the definition of "Information Security Incident," without a clear likelihood of harm to either an entity or customer, would result in multiple daily triggering of the notice and reporting requirements in Paragraph 34.

In fact, compliance with the requirements in Paragraph 34(a) to report any "information security incident" that has a "*potential* to materially affect, financially or non-financially…" (Italics added), is likely to be practically impossible and to unnecessarily overburden resources of regulated entities and APRA without providing commensurate benefit.

ACLI recommends the definition of "information security incident" be changed to better align with the *Privacy Act 1988* (Cth) (Privacy Act) which provides greater clarity around what type of incidents should be covered under CPS 234.

1. *There is unauthorized access to or unauthorized disclosure of personal information, or a loss of personal information, that an entity holds;*
2. *This is likely to result in serious harm to one or more individuals; and*
3. *The entity has not been able to prevent the likely risk of serious harm with remedial action.*

Information Asset

The definition of "information asset" could be construed to include essentially any business information of an APRA-regulated entity or any information about a customer obtained by the entity in connection with the provision of a financial product or service. In its proposal, APRA requires that entities classify information assets based on their criticality and sensitivity. ACLI believes APRA intended this classification to ensure information security measures are commensurate with the size and extent of threats to information assets. However, in practice, this is not clear given the overly broad definition of information asset. ACLI recommends APRA provide further guidance around the terms "criticality and sensitivity" and that *only* those assets determined by the entity to be critical and sensitive be subject to the requirements of CPS 234. This addition would provide for a framework that is risk-based, flexible, and workable.

New Definitions

Materially Affected

ACLI would also recommend APRA provide further guidance around the phrase "materially affected" to again emphasize the reasonable likelihood of material harm to a company or other insurance licensee or to consumers when critical and sensitive information assets are reasonably believed to have been involved in the event.

Overly Broad Requirements

Regarding Third Party Relationships

Paragraph 15 provides that entities must "assess" the capabilities of third parties. To comply with this type of requirement it would be helpful to have guidance as to what is meant by an assessment. This would include perhaps a definition or providing examples such as onsite visits, contractual representations, vendor certifications and re-certification or the like.

Similarly, paragraph 21 states entities must "evaluate the design and operating effectiveness" of third party controls. To understand what this requirement requires for practical compliance purposes it would be helpful to provide concrete examples or define this phrase. Often companies may have to rely on information provided by a vendor that we cannot precisely verify without going to the location of data processing or storage which could be anywhere in the world. It would be helpful to know what level of evaluation is going to be expected.

Both paragraph 15 and 21 could perhaps be addressed by setting some reasonable and customary standards or explicit clarity as to whether we can rely on third party self-assessments or certifications or not.

Incident Management

Paragraph 22 contains the term "robust" and paragraph 23 contains the phrase "plausibly occur" and these descriptions do not provide particularly clear guidance as to when the requirement in each paragraph would be triggered. In order to understand what is expected for compliance it would be helpful to have these defined or to have examples of what each term or phrase is meant to encompass.

Paragraph 25 provides that entities must prove effectiveness of their program annually. It would be helpful to understand how this is to be completed. Perhaps this could this be satisfied by a report that there were no incidents or perhaps a report that there were fewer than a certain number of incidents.

Reporting Requirements

Experience versus Determination

Paragraphs 34(a) and (b) refer to the entity "*experiencing* an information security incident" (italics added). The meaning of "experiencing" an incident is not clearly defined. Furthermore, the phrase is not helpful as a harm trigger for notification. We submit a more appropriate trigger would be 'determination' and the suggested language would be as follows:

> *34. An APRA-regulated entity must notify APRA within 72 hours from determination of an information security incident or without unreasonable delay that:*
>
> *(a) materially affected, 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.*

Determination would be defined as when a company, during its investigation to understand the nature and scope of the security incident and to undertake appropriate responsive measures, reasonably believes that unauthorized access to and/or acquisition of personally identifiable information has occurred. US cybersecurity laws and the EU's GDPR both use the concept of determination rather than experience. If APRA insists on using the term "experience," ACLI would recommend it provide a definition which takes into account the time needed to understand the nature and scope of a security incident. The *Privacy Act 1988* (Cth) (Privacy Act) also builds in a 30-day window to perform an investigation concerning harm.

Time Frame

The time frame for notification should be extended to 72 hours from determination to align with existing international cybersecurity regulations, such as those issued by the New York Department of Financial Services as well as the EU's GDPR.

Scope

Paragraph 34(a) refers to the "potential" to affect the entity. Echoing our concerns above about the use of 'potential,' it is once again likely to be practically impossible and to unnecessarily overburden resources of regulated entities and APRA without providing commensurate benefit. Notification to APRA should only occur when it has been determined that critical and sensitive information was affected and likely to result in serious harm. ACLI believes the concern with the word "potential" can be mitigated with the previously requested change to the definition of information security incident.

Notifications in Other Jurisdictions

Paragraph 34(b) requires notification to APRA if another jurisdiction's regulators have been notified. It is certainly reasonable to require notification to APRA if an entity notified another Australian government agency. However, requirements in some foreign jurisdictions are very low and notification to APRA would unnecessarily overburden resources of regulated entities as well as APRA without providing commensurate benefit. Only those incidents which meet APRA's harm trigger and materially affects Australian consumers should be reported.

Notification of 'Weakness'

Paragraph 35 contains a requirement to notify APRA after "identifying a material information security control weakness." This language is very broad and would require notification of a range of potential issues which have caused no harm to the entity or consumers. There is also no clear understanding of what would constitute a security control weakness.

ACLI would welcome the opportunity to discuss our concerns about the Draft Prudential Standard. We thank you for your consideration.

Sincerely,

Ashley Beaudry
Senior International Policy Analyst
American Council of Life Insurers