7 June 2018

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

Submitted via email: PolicyDevelopment@apra.gov.au

Re: Consultation on information security requirements for all APRA-regulated entities

Amazon Web Services (AWS) is grateful for the opportunity to provide comments to the Australian Prudential Regulation Authority's (APRA) public consultation on the Discussion Paper '*Information security management: A new cross-industry prudential standard*' (Discussion Paper).

We would be pleased to discuss our submission in greater detail with APRA as it moves to implement a cross-industry prudential standard for the management of information security, as proposed under draft *Prudential Standard CPS 234 Information Security* (Draft CPS 234).

Sincerely,

Simon Edwards
Head of Public Policy, Australia & New Zealand
Amazon Web Services

AWS RESPONSE TO THE DISCUSSION PAPER

PART 1: GENERAL COMMENTS

Subject to the specific comments and recommendations contained in this submission, AWS supports APRA's decision to elevate key principles and guidance contained in *Prudential Standard CPS 220 Risk Management, Prudential Standard SPS 220 Risk Management*, and *Prudential Practice Guide CPG 234 Management of security risk in information and information technology* to the level of a prudential standard in the proposed Draft CPS 234.

PART 2: AWS COMMENTS ON DRAFT CPS 234

2.1 Definition *'information security vulnerability'* - Paragraph 11(h)

Draft CPS 234 definition: *'is a weakness in an information asset or information security controls that could be exploited to compromise information security'*

AWS recommended definition: *'is a weakness in an information asset or information security control~~s~~ that could be exploited to compromise information security'*

AWS recommends this definition be amended to clarify that any information security control, rather than the totality of the information security controls, may create an information security vulnerability. We believe this amendment achieves APRA's stated intent to ensure APRA-regulated entities maintain an information security management framework that is adaptive.

2.2 Incident Management - Paragraph 22

Draft CPS 234 language: *'An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner'.*

AWS recommended language: *'An APRA-regulated entity must have ~~robust~~ mechanisms in place to detect and respond to information security incidents in a timely manner'.*

AWS does not believe additional value is added by use of the adjective 'robust'. We also believe its use may add conjecture to an otherwise clear requirement and that this amendment still achieves APRA's stated intent to ensure that APRA-regulated entities implement mechanisms to quickly detect and respond to attacks when they occur.

2.3 Testing control effectiveness - Paragraph 26(d)

Draft CPS 234 language: *'An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with: ... (d) the risks associated with exposure to untrusted environments, where an entity's ability to enforce its information security policy is impeded'.*

AWS recommended language: *'An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with: ...* (d) *the ~~risks associated with exposure to untrusted environments where an~~ entity's ability to enforce its information security policy ~~is impeded~~'*

AWS acknowledges APRA's concern that an APRA regulated entity's information security controls must be tested through a systematic testing program and that the effectiveness of such a program will depend, in part, upon whether the entity has the ability to enforce its information security policy.

AWS considers the obligations contained in the Draft Standard CPS 234 as to the nature and frequency of an APRA regulated entity's systematic testing should address all circumstances that could impede that entity's ability to enforce its information security policy.

We believe this amendment still achieves APRA's stated intent to ensure that the testing conducted is commensurate with the APRA-regulated entity's exposures to vulnerabilities and threats and the rate at which these exposures evolve.

2.4 APRA Notification - Paragraph 34

2.4(a) Draft CPS 234 language: *'An APRA-regulated entity must notify APRA as soon as possible, and no later than 24 hours, after experiencing an information security incident that:'*

Recommended AWS language: *'An APRA-regulated entity must notify APRA as soon as possible~~,~~ ~~and no later than 24 hours,~~ after ~~experiencing~~ becoming aware of a~~n~~ confirmed compromise of information security ~~incident~~ that:'*

AWS acknowledges the importance of APRA-regulated entities notifying APRA of information security incidents that meet the criteria in paragraph 34(a). However, we do not believe it is feasible for either APRA-regulated entities, or third parties that may maintain information security controls, to comply with this language as currently drafted.

Firstly, AWS believes it is preferable for APRA-regulated entities to notify APRA as soon as possible rather than in a required 24-hour period. We believe APRA-regulated entities, and any third party maintaining information security controls, should be primarily focused on identifying, mitigating and remedying the impact of a security information incident, particularly where consumers may be affected. We also believe this 24-hour period could lead to excessive conservatism, reactive reporting and/or over-reporting of incidents to APRA. We believe the existing language "as soon as possible" should achieve APRA's stated intent to be notified of any information security incidents in a timely manner.

Secondly, AWS believes notification to APRA should be triggered on the APRA-regulated entity having become aware of an information security incident rather than having experienced it. We believe an APRA-regulated entity can only notify APRA about an information security incident once it has become aware of the incident, given an incident may be experienced without the entity necessarily having an awareness of it. Additionally, given APRA-regulated entities must make a materiality assessment of the information security incident under paragraph 34(a) before making a notification, we believe awareness of the information security incident is a more feasible trigger.

Finally, AWS believes that notification should be required for a confirmed compromise of information security, rather than an 'information security incident' which consists of either a confirmed or potential compromise. We believe it is unfeasible to report potential compromises of information security and that this requirement could lead to excessive conservatism, reactive reporting and/or over-reporting of incidents to APRA. Additionally, we believe this requirement could lead to APRA-regulated entities reporting on events that have no discernable impact to either the APRA-regulated entity or consumers, or reporting a vulnerability either publicly or privately that could create circumstances that increase the potential for the vulnerability to be exploited.

2.4(b) Draft CPS 234 language: *'(b) has been notified to other regulators, either in Australia or other jurisdictions.'*

Recommended AWS language: *'~~(b) has been notified to other regulators, either in Australia or other jurisdictions.~~'*

AWS does not believe it is feasible for either APRA-regulated entities, or third parties that may maintain information security controls, to comply with this language as currently drafted. Firstly, there is no clarification that these regulators must be financial services (or equivalent) regulators and therefore they may have different interests from APRA as a prudential regulator. Secondly, it is possible these regulators have lower thresholds for notification than APRA thereby leading to over-reporting to APRA. Finally, a notification to these regulators may capture circumstances beyond a formal notification required by applicable legislation and/or regulations (i.e. informal notification). We believe that APRA's intent to be notified of information security incidents in a timely manner is still achieved by paragraph 34(a).

2.5 APRA Notification – Paragraph 35

Draft CPS 234 language: *'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.'*

Recommended AWS language: *Not applicable.*

AWS respectfully requests APRA re-consider the need and utility of the obligation proposed in paragraph 35. AWS does not believe it is feasible for either APRA-regulated entities, or third parties that may maintain information security controls, to comply with this language as currently drafted. We believe that the lack of objectively around what constitutes "in a timely manner" could lead to excessive conservatism, reactive reporting and/or over-reporting to APRA. AWS also believes that notification of a material information security control weakness and subsequent collection of these weaknesses into a single, APRA-controlled, register could increase the potential for the weaknesses to be revealed and exploited.

PART 3: ISSUES THAT AWS CONSIDERS SHOULD BE IN CPS 234

AWS recommends APRA include three security control areas, which are not specific to cloud services, in Draft CPS 234. We believe these three security control areas, described below, are sufficiently important for inclusion as mandatory requirements in Draft CPS 234 given their breadth and depth of use across the Australian IT industry.

While we recognize APRA may prefer to include these security controls in a guidance document or other information paper, we believe their inclusion in a Standard, specifically in paragraphs 20 or 21 (Implementation of controls) of Draft CPS 234 would increase their adoption across APRA-regulated entities. The proposed security control areas are:

> **Identity and Access Management:** This could be defined as an "Access Control" and the requirement could be for APRA-regulated entities to have an effective process for providing access to IT assets by only authorising access to IT assets where a valid business need exists and only for as long as access is required. This would make the presence of such a process mandatory, but is flexible enough to allow for different ways of technical implementation.
>
> **Encryption:** This could be defined as a "Cryptographic technique to restrict access" and the requirement could be for APRA-regulated entities to use cryptography to control access to sensitive data/information, both in storage and in transit, for example in the transmission and storage of critical and/or sensitive data/information, detection of any unauthorised alteration of data/information, and verification of the authenticity of transactions or data/information.

Logging and Monitoring: This could be defined as a "Monitoring Process" and the requirement could be for APRA-regulated entities to have a monitoring process in place to identify events and unusual patterns of behaviour that could impact on the security of IT assets. This monitoring process could be based on activity logging including exceptions to approved activity. We recognise that Draft CPS 234 currently requires Incident Management (paragraphs 22 to 25), which AWS agrees with, however Incident Management itself relies on the presence of logging systems which are routinely monitored.