7 June 2018

General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
GPO Box 9836
Sydney NSW 2001

By email: PolicyDevelopment@apra.gov.au

Dear General Manager

Information Security Management Discussion Paper

The Australian Financial Markets Association (AFMA) is a member-driven and policy-focused industry body that represents participants in Australia's financial markets and providers of wholesale banking services. AFMA's membership reflects the spectrum of industry participants including banks, stockbrokers, dealers, market makers, market infrastructure providers and treasury corporations.

AFMA welcomes the opportunity to respond to APRA's Discussion Paper *Information security management: A new cross-industry prudential standard* which discusses the draft prudential standard CPS 234 Information Security. AFMA counts many APRA regulated entities within its membership and the proposed standard could have significant implications for these members.

Increasingly, information security is the primary security matter for banks and financial markets participants. AFMA supports the extension of the prudential standards to information security matters where it is done in a coordinated way that fits well with the other regulatory and legislative initiatives underway.

In this regard we note the need to ensure there is appropriate coordination with the proposed Government requirements to open up customer data to many more firms under the Open Banking framework which applies to information customers have requested be released to third parties including non-ADI firms. Data will be transferred from entities subject to APRA's information security requirements such as in CPS 234 and CPG 235, to entities that are not.

The Open Banking framework proposes a very different model of risk assessment for banks dealing with firms than is envisaged under CPS 234. Open Banking proposes to place limits on the security banks can require when providing customer information to approved external third parties[1], noting that these parties themselves are proposed to be

[1] See Recommendation 5.5 https://treasury.gov.au/consultation/c2018-t247313/

assessed by "qualified third parties"[2]. It is appropriate that APRA ensures that these standards work in a coordinated and efficient way and that any potential information security risks that arise through the transfer of data to non-APRA regulated institutions such as through Open Banking and mandatory Comprehensive Credit Reporting is addressed.

We also note the ongoing work of ASIC in relation to 'cyber resilience' which has the potential to overlap with some of the work that APRA is undertaking. We encourage the regulators as a group to ensure their activities are coordinated to reduce unnecessary overlap.

Please refer to the attached detailed response for our specific concerns in relation to the draft prudential standard. General themes are listed below:

Materiality
As general thematic observations AFMA notes that the standard is currently drafted very broadly without (as the paper states) any limitations based around thresholds of materiality.

While we would agree there are difficulties in applying judgement about what constitutes materiality in information security, in many cases clear distinctions can be made. APRAs proposed approach of disallowing reasonable judgements to be made in relation to materiality risk greatly increases the costs of the proposed standard with in many cases minimal, if any, gains.

AFMA supports the inclusion of materiality provisions even if they must be used with a significant degree of caution as a means to ensure that sensible outcomes can be met in terms of cost, and to avoid inefficient the focus of resources on areas where risks are low.

Members would also welcome clarity that the definition of materiality in CPS 231 also applies to CPS 234. Examples of materiality should then be included in the updated guidance CPG 234.

Third parties
While it is important that third parties are carefully controlled and that ultimate responsibility rests with the ADI, the proposed standard could be better aligned with the standard commercial arrangements, and the limits of these arrangements, with high quality third party outsourcing providers.

AFMA supports a review of the standard to ensure that ADIs are not limited in their ability to use cloud technologies by information security standards that are as drafted more aligned with the more traditional data-centre approach. This includes permitting the use of independent auditors including those engaged by the third party.

Board involvement
Given their ultimate responsibilities, it is fitting that Boards are kept appropriately informed of information security matters, but to avoid making important matters difficult to discern in an overload of information it is appropriate that there is a level of materiality to the issues that under the standard would warrant Board attention. The aim should be to strike a balance between the level of detail enabling challenge but not to overwhelm with technical detail.

[2] *Ibid.*, p. 25.

It would not be appropriate, for example, to inform Boards of ADIs every time a firewall prevents a suspected reconnaissance attack, and the drafting of the standard should reflect these type of thresholds.

APRA Notification

APRA notification should be designed to be efficient. In this regard it should avoid duplicative reporting requirements with other arms of the Australian Government (rather than expressly requiring this) through better coordination between the relevant regulators. It should also not prioritise formal notice activities while in a triage situation which should be focussed on ensuring there is no ongoing risk to customers. We also note that the requirement to report anything that has been reported to regulators in other jurisdictions may need to be refined to avoid branches reporting matters that are not relevant to their Australian operations and to avoid creating a lowest common threshold for reporting to APRA where any report must be duplicated to APRA.

We thank you for considering our comments in relation to draft prudential standard CPS 234. We would be pleased to assist with any further information you may require.

Yours sincerely

Damian Jeffree

DETAILED RESPONSE

CPS 234 Clause	Review and Commentary	Proposed Amendments
Definitions	Terms including 'materiality', 'material change' and 'material control weakness' are used throughout the document, and in our view should be used in other places but are not clearly defined. Consequently, many of the obligations are potentially onerous and open to wide interpretation. We recommend 'materiality' be aligned to CPS 231. 'Information Security Incident' is broadly defined in section 11 (e) and does not provide clarity on whether an information data breach (for example: miss-addressed external email) constitutes such an incident. The word 'potential' used in the definition is vague and creates and excessive scope – an event where there was no breach becomes a breach through the use of this word. In combination with the revisions planned for CPG 234 it would be advantageous to include framework definitions for these words and phrases.	Proposed amended drafting: **"Material and Materiality is defined in line with other APRA standards and guidance to mean of significant importance to the regulated entity in the view of that entity.** **Material Change in the context of Information Security means a change that could be reasonably be expected to have a material impact, financial or non-financial, on the institution or on the interests of depositors and/or policyholders.** **Material Control Weakness means a flaw or absence in measures to prevent information security incidents that could be reasonably be expected to produce an unacceptable level of risk, financial or non-financial, to the institution or on the interests of depositors and/or policyholders in the view of the regulated entity.** **Information Security Incident means** ~~t means a confirmed or potential compromise of information security;~~ **an event or series of events that have, or have previously had, a material impact, financial or non-financial, on the institution or on the interests of depositors and/or policyholders."**
Paragraph 13 "The information security-related roles and responsibilities of the Board, and of senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions, must be clearly defined."	At the Board level while it is appropriate to ensure the information security responsibilities are known and understood we would caution against requiring specific roles within the Board in relation to information security. As information security is a specialist discipline it may be an area the Board takes the view given the balance of its business it may be appropriate to rely on senior management rather than dedicate a particular role within the Board. At the senior management level paragraph 13 should be designed to work in closely with BEAR. More generally the extension of the requirements to individuals responsible for "operations and other information security functions" may be too granular and potentially too rigid. Responding to information security matters often requires flexibility and agility in staff. The draft wording may result in an overly rigid approach that may detract from the agility and flexibility needed to deal with rapidly	Proposed amended drafting: "The information security-related ~~roles and~~ responsibilities of the Board **should be clearly understood.** ~~and of~~ **The roles and responsibilities for information security of** senior management, governing bodies and individuals with responsibility for decision-making, approval, **and** oversight, ~~operations and other information security functions,~~ must be clearly defined."

	evolving threats. We would defer to the CPG 234 guidance for operational and other staff.	
Paragraph 15 "Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets."	Paragraph 15 as drafted will capture outsourcings and offshoring that will have otherwise been deemed as non-material. This risks an inappropriate and uneconomic allocation of resources that could have more impact on information security elsewhere. It is preferable that a materiality threshold is introduced at the standard level rather than in the updated guidance. It is appropriate that the standard allows a risk-based approach to be used. This will allow for the appropriate differences in frequency and depth of assessment between newly outsourced functions and well-established functions. Similarly providers that set global standards for outsourcing may require on a risk-adjusted basis lower levels of assessment in comparison to smaller firms. Members also note that many prominent providers of cloud technology have data centres located in multiple places around the globe. Many of these do not allow direct user inspections of these facilities or the security measures used. They will, however, provide copies of independent third party assessments of their security measures. To avoid inadvertently making these types of facilities inaccessible to ADIs it is appropriate that sufficient flexibility is built into the standard to allow these types of assessments and outsourcing to be used.	Proposed amended drafting: "Where information assets are managed by a related party ~~or third party~~, the APRA-regulated entity must assess the information security capability of that party, commensurate with the **materiality and** potential consequences of an information security incident affecting those assets. Where information assets are managed by a ~~related party or~~ third party **and there are material risks,** the APRA-regulated entity must, **on a risk-adjusted basis, take reasonable steps (in some instances this will be restricted to reviewing qualified independent third party assessments) to** assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets."
Paragraph 16 An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.	We note in relation to this paragraph that vulnerabilities and threats are constantly changing. While the intent of the paragraph is not contested members are concerned that the drafting should ensure that perfection is not set as the standard.	Proposed amended drafting: "An APRA-regulated entity must **take reasonable steps to** actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment."
Paragraph 18 "An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security." **Footnote 6** "For the purpose of paragraph 18 of this Prudential Standard, parties includes governing bodies and individuals with responsibilities referenced in paragraph 13, as well as all other staff, contractors, consultants, related parties, third parties and customers." **Paragraph 13**	"Responsibilities" in Paragraph 18 can be read in a number of ways. While we assume the intention is to ensure all parties are informed of their broad responsibilities to protect confidential information, hold to good security practices etc. which is fine, 'responsibilities' can also be read as referring to finely grained role responsibilities particularly when combined with footnote 6 and paragraph 13 (e.g. dictionary definitions of responsibilities include "a thing which one is required to do as part of a job, role, or legal obligation."). Reading it in this way would suggest that all employees	Proposed amended drafting: "An APRA-regulated entity's information security policy framework must provide direction on the **broad high-level** responsibilities of all parties who have an obligation to maintain information security."

"The information security-related roles and responsibilities of the Board, and of senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions, must be clearly defined."	including information security operations must have their exact responsibilities (e.g. which networks and services they are responsible for) spelled out in the policy framework, which is not an appropriate level of detail for framework policy documents.	
Paragraph 19 "An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. Criticality and sensitivity is the degree to which an information security incident affecting that information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers."	This paragraph requires information assets managed by related parties and third parties to be classified as though they are controlled by the APRA regulated entity. Given the lack of a materiality threshold under the standard this could apply to a large number of related parties and third parties. It is impractical, unduly onerous and difficult to implement. AFMA recommends classification of information assets be limited to those that are under its direct management. For information assets managed and/or held by related parties and third parties, the organization should implement control measures such as: • contractual obligations • periodic oversight • regular reporting This will ensure that affiliates and third parties apply adequate controls/safeguards. APRA should also consider providing general guidance in the amended CPG 234 on how information classification should be performed. The criticality and sensitivity requires tighter definition. The current definition may be construed to require the identification of critical processes across the prudential entities.	Proposed amended drafting: "An APRA-regulated entity must classify its information assets **where material risks are assessed to exist**, including those managed by related parties ~~and third parties,~~ by criticality and sensitivity. Criticality and sensitivity is the degree to which an information security incident affecting that information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers. **Where information assets managed by third parties have material risks associated with them these should be subject to appropriate governance controls.**"
Paragraph 20 "An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with: (a) vulnerabilities and threats to the information assets; (b) the criticality and sensitivity of the information assets; (c) the stage at which the information assets are within their life cycle; and (d) the potential consequences of an information security incident."	AFMA notes that information security controls in an enterprise context have upgrade programs that are often planned out over multi-year periods. While this is a reasonable and responsible approach given the scale and complexity of these upgrade and implementation programs it is unclear how this would fit with the phrasing "timely manner".	Proposed amended drafting: "An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a**n appropriate timeframe** ~~timely manner~~ and that are commensurate with: (a) vulnerabilities and threats to the information assets; (b) the criticality and sensitivity of the information assets; (c) the stage at which the information assets are within their life cycle; ~~and~~ (d) the potential consequences of an information security incident**; and** **(e) the materiality of the information assets**"
Paragraph 21 "Where information assets are managed by a related party or third party, an APRA regulated entity must evaluate the design and operating effectiveness of that party's information security controls."	AFMA recommends that this paragraph be reviewed to allow for risk-adjusted 'scaling' of the obligation e.g. to specify that this evaluation process must be commensurate with various factors (such as those in paragraph 20 of the draft CPS).	Proposed amended drafting: "Where information assets are managed by a related party or third party, an APRA regulated entity must evaluate the design and operating effectiveness of that party's information security controls.

	We also note similar concerns raised in relation to paragraph 15 in light of the limited ability of ADIs to gain access to some leading cloud (and other) provider's security information management systems (noting they do provide copies of independent reviews).	Where information assets are managed by a related party or third party, **and there are material risks,** the APRA-regulated entity must, **on a risk-adjusted basis, take reasonable steps (in some instances this will be restricted to reviewing qualified independent third party assessments) to** evaluate the design and operating effectiveness of that party's information security controls."
Paragraph 22 "An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner."	AFMA notes that while there should be appropriate governance arrangements in place with third parties (such as Service Level Agreements) these cannot force compliance *at the time* and are instead ways to put pressure on third parties to respond and to sue in the event of a breach of the agreements at a later time.	Proposed amended drafting: "An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner. **Where functions involve third parties appropriate governance arrangements should be in place to contractually require timely detection and response.**"
Paragraph 24 (b) "An APRA-regulated entity's information security response plans must include the mechanisms in place for: … (b) escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate."	APRA may wish to consider leaving this to out given the substantial overlap with CPS 220 – paragraph 36 (d). We note it also has some overlap with business continuity management and CPS 220. If kept as part of this standard for clarity we suggest the addition of a 'materiality' qualifier for the word appropriate.	Proposed amended drafting: "An APRA-regulated entity's information security response plans must include the mechanisms in place for: … (b) escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate **given the level of materiality of the incident**."
Paragraph 25 "An APRA-regulated entity must annually confirm that its information security response plans are effective."	AFMA members advise us that this may already be a part of the existing CPS 220 annual attestation and that creating a separate attestation under CPS 234 may be duplicative. In the event that the existing CPS 220 attestation is insufficient it may be appropriate to provide more guidance on this requirement including: • Definition of the scope and extent of the entity's information security response plan that is subject of confirmation; • Description of the evidence expected to support the confirmation • The specification and delivery mechanism for the confirmation; and • By who the confirmation is to be provided by and to whom within APRA.	Suggest leave to CPS 220 or amended CPS 220. "~~An APRA-regulated entity must annually confirm that its information security response plans are effective.~~"
Paragraph 26 "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: (a) the rate at which the vulnerabilities and threats change; (b) the criticality and sensitivity of the information asset;	While paragraph 26 offers some helpful criteria for scaling the testing program that assist in determining the risk of material incidents, we do note an issue with (a) in that some types of vulnerabilities and threats such as viruses, malware, spyware, and the like change on an daily or even hourly basis. As such this criteria in some circumstances will fail as a scaling criteria, and requiring that testing the frequency be 'commensurate' with	Proposed amended drafting: "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 **appropriate given** ~~commensurate with~~: (a) the rate at which the vulnerabilities and threats change**, where these change**

(c) the consequences of an information security incident; and (d) the risks associated with exposure to untrusted environments, where an entity's ability to enforce its information security policy is impeded."	these changes could imply that the testing happen just as frequently (e.g. daily / hourly). Potential overlaps with testing and control requirements in CPS 220 should be removed or cross-referenced in this paragraph. AFMA suggests that CPG 234 be updated to provide guidance on whether this testing should be of the risk management and control self-assessment testing; technical testing through vulnerability scanning and penetration testing or a combination of both of the above.	**frequently this may suggest periodic testing with ongoing monitoring**; (b) the criticality and sensitivity of the information asset; (c) the consequences of an information security incident; ~~and~~ (d) the risks associated with exposure to untrusted environments, where an entity's ability to enforce its information security policy is impeded~~.~~**; and** **(e) the materiality of the information assets.**"
Paragraph 27 "Where information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, an entity must assess whether that testing is commensurate with paragraph 26 (a)-(d)."	Consistent with the responses for CPS-15 and CPS-19 above, in the absence of a materiality threshold, the operation of CPS- 27 is expected to be a substantial burden on AFMA members and reporting entities generally. The requirement could potentially apply to a large number of related or third party entities. Our proposed drafting alters the requirement to allow for the standard independent assessments that are available from leading cloud providers. We have also altered the drafting to clarify that supplier security assessments can be performed at the entity level (rather than the service level) in order to comply with this requirement.	Proposed amended drafting: "Where information assets are managed by a related party or a third party, **there is an assessment of material risk,** and the APRA-regulated entity is reliant on that party's information security control testing, an entity must **either itself or through an independent third party, at the entity level** assess whether that testing is commensurate with paragraph 26 (a)-(d)."
Paragraph 28 "An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner, to enable an assessment and potential response by the Board or senior management to mitigate the exposure, as appropriate."	AFMA suggests the inclusion of some materiality threshold on this escalation and reporting obligation. AFMA also notes that a multiyear program to resolve a control deficiency may not be considered 'timely' in the operation of this paragraph, we suggest the wording 'an appropriate timeframe' to allow customisation of remedies to the criticality and scale of the deficiency.	Proposed amended drafting: "An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify **material** information security control deficiencies that cannot be remediated in ~~a timely manner~~ a**n appropriate timeframe**, to enable an assessment and potential response by the Board or senior management to mitigate the exposure, as appropriate."
Paragraph 29 "Testing must be conducted by appropriately skilled and functionally independent specialists."	AFMA queries the use of the qualifier "functionally". Given the sophistication of the systems it is often appropriate to use staff from the same function to undertake testing. This requirement as drafted may operate to exclude skilled internal resources from testing in areas such as penetration testing. Under the APRA CPS 220 standard firms will already have a designated risk management function that is operationally independent and can provide appropriate oversight on a risk-adjusted basis.	Proposed amended drafting: "Testing must be conducted by appropriately skilled ~~and functionally independent~~ specialists."
Paragraph 30 "An APRA-regulated entity must review the sufficiency of the testing program at least annually or on material change to	While annual reviews are appropriate, to review the program following every material change could be a substantial task.	Proposed amended drafting: "An APRA-regulated entity must review the sufficiency of the testing program at least annually or **relevant portions of it** on

information assets or the business environment."		material change to information assets or the business environment."
Paragraph 31 "An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance)."	AFMA notes again the difficulty in reviewing the design and operating effectiveness of information security controls of 3rd party providers. As a matter of good general business practice the responsibility for the review of controls of third parties sits outside of the scope of internal audit function. Independent external auditors are generally used to audit material third parties in line with internal third party risk management and governance processes. As drafted the requirement may result in a scenario where a reporting entity as an outsourced third-party for other reporting entities (clients), could be subject to coverage by the client's internal audit function, in addition to existing third party external audit obligations. (GS007/SOC1/SSAE18 etc.)	Proposed amended drafting: "**The scope of a**n APRA-regulated entity's internal audit activities must include ~~a review of~~ the design and operating effectiveness of information security controls, including those **procedures used by the APRA regulated entity to monitor information security controls** maintained by related parties and third parties (information security control assurance)."
Paragraph 33 "Where information assets are managed by a related party or third party, internal audit must assess the information security control assurance provided by that party, where an information security incident affecting those information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers."	Paragraph 33 appears to again suggest that an entity's internal audit functions should audit the third party's second line of defence and internal audit functions. Audit should be limited to reviewing an entity's oversight and monitoring controls over external information assets in the same manner as presently performed over outsourcing.	Proposed amended drafting: "~~Where information assets are managed by a related party or third party, internal audit must assess the information security control assurance provided by that party, where an information security incident affecting those information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.~~ "
Paragraph 34 "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."	The paragraphs on APRA Notification (34 and 35) have raised the most concerns amongst AFMA members. The appropriate order of priorities in regard to information security incident management, consistent with the framework set out in the Government's suggested framework for data breach management[3], should be to (1) Contain the breach/incident (2) Assess and if possible take remedial action (3) Notify regulators and review. The "as soon as possible" and 24 hour requirements suggest reversing this priority and introducing a regulatory engagement which are inherently high overhead while working to contain the incident. We suggest the interests of depositors, policyholders, beneficiaries and other customers would be better served by focusing key resources on containment and remedial action in the first instance. We suggest a "practicable" qualifier and a change to 3 days. We note that GDPR and the Australian data breach	Proposed amended drafting: "An APRA-regulated entity must notify APRA as soon as **practicable** ~~possible~~, and no later than ~~24 hours~~ **3 days**, after **becoming aware of** ~~experiencing~~ an information security incident **and forms the view** that the incident has~~:~~ ~~(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.~~"

[3] See https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#the-notifiable-data-breaches-ndb-scheme

	timings are 72 hours and the requirement to report to APRA in CPS 220 is 10 business days after the entity becomes aware. We also note difficulties in the use of the word "experiencing" as the timeframe should start from when the entity becomes properly aware there is an incident and not from when the incident itself starts. We suggest change this word to "becoming aware of" (as with CPS 220) and "forms a view it is material". This is consistent with recent changes proposed (and agreed in principle) to ASIC's reporting requirements.[4] In terms of the materiality threshold we suggest aligning with the NDBS standard: "a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates." In relation to 'near misses' as there is by definition no harm and there is not the same need for urgent reporting. Reporting of 'near misses', especially without clear definition, risks an increase on non-actionable reports which could potentially distract from relevant reporting within Australia. Consequently, A period of time should be permitted for entities to make an internal assessment of whether there is an information security incident which is eligible for reporting. The requirement to duplicate the reporting to other Australian regulators is an inefficient burden on industry that should be avoided by better coordination between the various regulators. APRA has received submissions previously in a range of areas critical of the requirements to duplicate reporting to APRA (see for example APRA's Update on regulatory cost savings 2016 [5]). APRA should take this opportunity to increase data sharing with other arms of government or arrange a common portal for reporting incidents of this type. As to the requirement to duplicate reports to foreign regulators this is not an appropriate way to select matters for reporting. APRA should set objective criteria to report against and not set itself to receive reports from the lowest common reporting threshold. Further the drafting does not make clear that these matters are limited to those that directly affect the local entity.	

[4] See page 9 of https://treasury.gov.au/review/asic-enforcement-review/r2018-282438/

[5] http://www.apra.gov.au/CrossIndustry/Consultations/Documents/Update%20on%20Cost%20Savings%20August,2016.pdf

	AFMA has privacy concerns on reporting non-Australia ("other jurisdiction") related incidents to APRA. In addition, there are specific protocols on reporting such incidents outside respective jurisdictions for which 24 hours may not be adequate. Mandatory notification should only relate to material incidents impacting the reporting entity and/or Australia legal entity's clients. As noted clearer definition of materiality and what constitutes an information security incident is required, as at present it could include a wide range of data breaches that may not be related to information security.	
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."	The appropriate role for a regulator does not extend to detailed management of security control weaknesses. As part of any firm's information security program control weakness should be identified and remediated internally. There should not be a need to report every control weakness to APRA. In the event APRA decides to proceed with a requirement to report control weaknesses the timeframe should be extended match the OAIC data breach notification timeframe of 30 days and the wording adjusted to make the timing relevant to the particular control.	Proposed amended drafting: "~~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.~~" "An APRA-regulated entity must notify APRA as soon as possible and no later than ~~five~~ **thirty** ~~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~~ **within an appropriate timeframe, given the nature of the control weakness**."