AUSTRALIAN INSTITUTE of SUPERANNUATION TRUSTEES

8 June 2018

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

Email: PolicyDevelopment@apra.gov.au

Dear Sir/Madam,

Re: Draft APRA Prudential Standard CPS 234 Information Security

In brief:
AIST supports CPS 234 as a useful mechanism to promote increased focus on information security and to promote continuous improvement. AIST believes that the requirement to notify incidents to APRA within 24 hours should be clarified with respect to levels of seriousness, with less material breaches set to 5 working days. Clarification of notification of control weaknesses should also be clarified.

AIST is pleased to be able to provide this submission on the proposals set out in the discussion paper on draft CPS 234. Please note that we do not plan to provide specific comments on all proposals contained in the discussion paper.

1. CPS 234 is a useful mechanism to promote increased focus on information security and to promote continuous improvement.
2. The requirements in paragraph 34 for notification of incidents to APRA within 24 hours should be clarified and recognise two levels of materiality:
    a. information security incident is defined as a confirmed or potential compromise of information security. This could mean that a potential compromise of information security would also need to be reported within 24 hours. The standard should define what potential compromise means.
    b. the obligation to notify no later than 24 hours of an information security incident. commences from the time a fund experiences an information security incident. This may not be detected after the incident and means the fund could have breached the standard before it is aware of the incident. The standard should further clarify a fund's obligations in such circumstances.
    c. the obligation to notify within 24 hours should be specific to more serious incidents, such as hostage or ransomware attacks, or other malicious software

Level 23, 150 Lonsdale Street
Melbourne VIC 3000

T +61 3 8677 3800
F +61 3 8677 3801

info@aist.asn.au
www.aist.asn.au

that result in damaging, blocking or publishing data. The requirement to notify other incidents should be extended to 5 business days.

d. while attacks of this nature are likely to trigger incident management processes (and potentially crisis management processes), we are unaware of any other legal requirement to respond to a government body within 24 hours.

3. The requirements in paragraph 35 for notification of control weaknesses to APRA within 5 business days should also be clarified:
    a. based on the current draft and the complexities of the cyber-security landscape this is uninterpretable.
    b. some clarification or a definition of "material" plus guidance on the subjective parts of CPS (eg, material, weakness, timely).
    c. the most effective way of providing this guidance would be to publish a small number of "hypothetical" scenarios. This would assist in providing clearer operating parameters.

Yours sincerely,

Eva Scheerlinck
Chief Executive Officer

The Australian Institute of Superannuation Trustees is a national not-for-profit organisation whose membership consists of the trustee directors and staff of industry, corporate and public-sector funds.

As the principal advocate and peak representative body for the $1.2 trillion profit-to-members superannuation sector, AIST plays a key role in policy development and is a leading provider of research.

AIST provides professional training and support for trustees and fund staff to help them meet the challenges of managing superannuation funds and advancing the interests of their fund members. Each year, AIST hosts the Conference of Major Superannuation Funds (CMSF), in addition to numerous other industry conferences and events.