AIA Australia Limited
(ABN 79 004 837 861 AFSL 230043)

PO Box 6111
Melbourne VIC 3004
Phone : 1800 333 613
Fax : 1800 832 266

AIA.COM.AU

27 August 2021

Cyber, Digital and Technology Policy Division
Department of Home Affairs

Email: techpolicy@homeaffairs.gov.au

SUBMISISON TO DISCUSSION PAPER: STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES

Thank you for the opportunity to share our views on how to strengthen cyber security in Australia. AIA Australia supports the Government's efforts to lift cyber security standards, in particular extending obligations to small and medium businesses and those not covered by existing standards such as Prudential Standard CPS 234 Information Security (CPS 234).

We agree that the best approach is a mix of regulation and incentive, to reward those who actively work to improve and strengthen cyber security in their own organisations while penalising those that don't take appropriate actions for known deficiencies. The hard reality is that until businesses are subjected to legal consequences with associated costs for failing to maintain proper levels of cyber security the standard will remain inadequate. The cost to a business of not setting appropriate cyber security standards should exceed the cost of doing so.

We note the term *"prevent cyber security incidents"* is used several times throughout the discussion paper. Care should be taken in suggesting a view that cyber impacts are fully preventable. This is not the case and any legislation should be created in such a way that penalties for businesses or compensation for consumers is only considered if the issues or practices exploited are known (or should be have been known) and not where the business has done all reasonable things and is still exploited. For example, a business would have no forewarning or awareness of a zero-day attack.

Our response to specific questions is included on the following pages. Should you wish to discuss any aspects of our response, please contact Tom Gordon, Head of Regulatory Affairs in the first instance, on [redacted] or [redacted].

Yours sincerely

[redacted]

Damien Mu
CEO and Managing Director
AIA Australia and New Zealand

Chapter 2: Why should government take action?

A key part of strengthening cyber security in Australia is by lifting the awareness and education of directors, business owners and managers. A core challenge is a fundamental understanding of what cyber risk is and what it is not. This understanding is lacking in many businesses and is likely to see easily preventable cyber security incidents occurring. In developing its response, the Federal Government should enhance partnerships with the private sector, through bodies such as the Australian Cyber Security Centre (ACSC) Partnership Program, to create uplift in awareness and understanding through scalable and low-cost channels. Subsidised or tax-deductible short courses, delivered digitally, would likely assist with this uplift.

1. What are the factors preventing the adoption of cyber security best practice in Australia?	Awareness of what cyber security is and isn't is highly variable within businesses and society more broadly. Good cyber security is often seen as a deep technology skill and the benefits of cyber fundamentals are often overlooked for this reason. The achievement of a common and accurate understanding would go a long way toward supporting a universal level of improvement towards industry best practice. Other factors which prevent the adoption of best practice include: • cost of implementation for businesses, particularly those with legacy IT environments • the inability of small and medium businesses to engage and maintain cyber security skills – both cost and availability • low awareness of the support available, for example organisations such as the ACSC, and what they can provide • capacity of organisations like the ACSC to provide adequate support to support increasing awareness and knowledge uplift • the lack of incentives, similar to those offered for research and development expenditure, that could encourage business to adopt stronger and more responsive cyber security practices.
2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?	As noted, there are significant cyber security skills and knowledge gaps across many businesses. Additionally, many smaller businesses lack the internal resources, or knowledge of where to access external resources to begin the journey to lift their cyber security capability. To help close these skills and knowledge gaps, development of a consistent set of cyber fundamentals for new and established businesses may assist. These cyber fundamentals could be developed by industry groups such as Australian Chamber of Commerce and Industry or the Australian Industry Group. Government action, at least in the early stages, should focus on supportive legislation rather than punitive action for businesses. Deceptive practices or those detrimental to effective adoption of best practice should be penalised either through financial or reputational penalties.

Chapter 3: The current regulatory framework

3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?	The current Australian Privacy Principles (APPs) are generally clear and easily understood and provide beneficial guidance to businesses of all sizes and industries. CPS 234 has the fundamentals of a similar model. There are benefits to having something similar to the APPs for businesses where cyber compliance and controls are involved but should be designed in a way that avoids a 'tick the box' approach rather than an understanding of threats and controls. One of the limitations of Australia's current regulatory framework for cyber security is inconsistencies, and sometimes competing obligations, which exist between legislation across Federal and State jurisdictions. For multinationals, this can extend to inconsistencies with overseas jurisdictions. Where supply chains cross industries, there is often a lack of cohesion which adds further complexity to managing cyber security risk. To illustrate these inconsistencies, financial service providers must comply with CPS 234, but also need to comply with regulation like the General Data Protection Regulation in the EU, Personal Data (Privacy) Ordinance in Hong Kong and AB 375 in the United States. Telecommunications and energy companies must also comply with the Critical Infrastructure obligations In seeking to address inconsistencies and competing obligations, businesses can often divert funding or organisational effort towards addressing those issues and away from actual compliance. Any changes to obligations should look to minimise overlap and inconsistencies between jurisdictions and between industries.
4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?	The focus should be on ensuring that different pieces of legislation are aligned and complement each other, where possible, to improve clarity of cyber security requirements. The other advantage of aligning and complementing different pieces of legislation is minimising the need for expensive court proceedings to determine which act prevails when misaligned. Proposals to extend obligations to small businesses, who are largely unregulated in this regard, would address coverage and enforcement concerns. Establishing trust in the supply chain has created unsustainable burdens on small business and small security teams due to the highly variable nature and methods to establish that trust. The current regulatory environment supports stronger trust between suppliers and business but doesn't contribute toward a common standard which would improve clarity.

Chapter 4: Governance standards for large businesses

5. What is the best approach to strengthening corporate governance of cyber security risk? Why?	Option 1, voluntary governance standards for larger business, is the most appropriate at this time. This option will ensure industry buy-in, will discourage a 'tick the box' approach, will provide better ability to align with international standards and should not significantly increase the business cost of compliance. Applying mandatory governance standards should only be considered, and limited to critical industries only, should there not be widespread adoption of the voluntary governance standards. Mandatory standards are more likely to drive a ‘tick the box’ approach where businesses become focused on reporting compliance (and showing Green) against each clause. This shifts the focus from assessing the level of threat and quality of protective controls to providing reports which can drive a result counter to the intended outcomes. Industry buy-in of best practice is critical to focus businesses on defining the risks, threats and impacts themselves.
6. What cyber security support, if any, should be provided to directors of small and medium companies?	Small and medium businesses do not usually have the size and scale to fund specialist cyber resourcing. Support for cyber awareness, education and assessment could be provided by specialist agencies such as ACSC, or businesses could be provided tax incentives for uplifting cyber capabilities. In some small businesses e.g. member-based companies, the pool from which directors can be sourced is often restricted by company constitutions which may make including cyber skills on a board impossible without some level of change in governing legislation. Therefore, it is critical business have access to scalable and cost-effective support. Across all businesses, responsibilities for directors and boards are an important element of appropriate governance and management ‘challenge’. However, in developing or refining obligations for directors and boards, care needs to be taken to avoid lifting accountability in any area to the point where the distinction between management and the board is compromised.
7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?	A level of consistency in base-level education would be beneficial. Particularly ensuring the focus of cyber security operation, management and governance is directed to information protection, threat analysis and response and not on "what is the minimum I have to do to tick the box?". The current inability of unpaid directors to claim education expenses discourages improvement of knowledge and capability. Given a large percentage of boards are voluntary, this represents a challenge to improving capability. Some level of funding or deductibility being made available for self-education of small business owners/directors would reduce these barriers.

Chapter 5: Minimum standards for personal information

8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?	Yes. If the initiatives in Chapter 4 are adopted, then we would expect the Privacy Act would only require minor amendments to ensure protection of sensitive information includes protection from cyber threats. The prescribing of relevant protections should be within the cyber security code.
9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?	The Privacy Act already has good control principles, but it could be stronger on preventing access to unauthorised people/organisations. The basic premise should be that businesses prevent access to all information unless there is a genuine need, including any B2B sharing. Expanding APP2, the Anonymity Principle, to be stronger about obfuscation or the use of encryption by default would be important inclusions to achieve the objectives.
10. What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?	Provided the requirements are reasonable and not overly costly to adopt, manage and monitor then all sectors should be covered by a code. Since small and medium businesses do not have funding or resourcing available to operate a dedicated cyber security function, responsibilities may fall to unskilled personnel. Providing direction within the code on basic security practices or tools, such as anti-virus, limiting access to any electronic information storage, the use of encryption by default and other basic and easily understood best practices would be beneficial in achieving the best cyber security outcomes.

Chapter 6: Standards for smart devices

Much of the discussion on consumer devices is focused on this as a consumer / household cyber threat. However, with a large percentage of employees working from home and unlikely to operate any network security, the indirect threats to business from poor security remains a concern. Evolving, conflicting and unclear standards in the consumer product market as well as interoperability from this is creating significant risk of successful cyber compromise of consumer devices. Most companies do not have systems in place to prevent low-security devices being brought into their environments.

11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why?	AIA Australia supports Option 1 - Mandatory standards for smart devices. This standard should include the requirement of devices delivered by telecommunication providers to detect and isolate incompatible devices. This would be mandated by firmware updates within a certain timeframe for existing devices and included as standard with any new devices issued after certain date. Labelling of compliance would assist consumer purchasing decisions. Most consumers have limited cyber skills and would be heavily reliant on the level of trust of the labelling standards applied. Therefore, standards should include controls which prevent providers from using sales and marketing activities which could result in false sense of security for consumers, such as misleading labelling.

12. Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices? a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate? b. If not, what standard should be considered?	Yes, ESTI EN 303 645 is an appropriate standard for Australia to adopt. We recommend adoption of more than just the top three requirements. While 5.1 to 5.3 are important, most of the other requirements, for example 5.12 – Easy setup with security on by default, are equally important to improve the cyber security of smart devices.

Chapter 8: Responsible disclosure policies

22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?	Manufacturers should be mandated to disclose serious vulnerabilities if not remediated in a reasonable period. This would force manufacturers to rectify material issues. Currently, the threat of publication by 'white hat' hackers tends to force manufacturers to fix vulnerabilities, but this is not always timely. Mandating responsible disclosure obligations would encourage manufacturers to act quicker and would allow consumers to select products or manufacturers which have a better reputation for providing high quality products.

Chapter 9: Health checks for small businesses

23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses? businesses to participate in a health check program?	AIA Australia strongly supports a health check program as it will lift the capability of small businesses. The inter-connected nature of supply chains mean that security is only as strong as its weakest link; therefore, a cyber security health check program for small businesses would reduce the points of greatest weakness and result in a strengthening of the entire supply chain.
24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?	Yes, there would appear to be commercial benefits to small businesses from a health check program. Promotion by Government of the 'health check trust mark' indicating a favourable assessment would be an easy way to reward businesses who participate and allow them to be easily identifiable by either consumers or other businesses in their supply chain. Businesses that display this trust mark, provided the bar is set sufficiently high, would be more likely to enter into supply arrangements with larger businesses, where vendor screening is well entrenched. This could benefit businesses in the same way those who undertake ISO certification are seen as preferred vendors. Similarly, the trust mark would help savvy consumers make choices about providers where they are concerned about issues such as data privacy.

25. If there anything else we should consider in the design of a health check program?	Having a standardised security assessment or an accredited health check, similar to the Cyber Health Check used in the UK, would provide much needed consistency for all parts of the supply chain. In practice we see multiple templates used to assess cyber security, many running to hundreds of questions. These templates are generally bespoke, required significant time and investment in completing. A standardised approach would improve the value of the health check program across the entire supply chain.