27 August 2021

First Assistant Secretary,
Cyber, Digital and Technology Policy Division,
Department of Home Affairs
4 National Circuit
Barton ACT 2600

Email: techpolicy@homeaffairs.gov.au

Dear Sir/Madam,

STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES

Insurance Australia Group (IAG) welcomes the opportunity to comment on the Department of Home Affairs *Strengthening Australia's cyber security regulations and incentives: An initiative of Australia's Cyber Security Strategy 2020* document (Cyber Security Consultation).

IAG is the parent company of a general insurance group with controlled operations in Australia and New Zealand. Our businesses underwrite almost $12 billion of premium per annum, selling insurance under many leading brands, including: NRMA Insurance, CGU, SGIO, SGIC and WFI (in Australia); and NZI, State, AMI, and Lumley Insurance (in New Zealand). With more than 8.5 million customers and information on the majority of domestic residences in our markets, we use our leadership position to understand and provide world-leading customer experiences, making communities safer and more resilient for the future.

Our purpose is to make your world a safer place and we recognise that our role extends beyond transferring risk and paying claims. Our purpose drives our business to work collaboratively with the community to understand, reduce and avoid risk, and to build resilience and preparedness. This results in better outcomes for the community and means fewer claims and lower costs for our business.

We work collaboratively with government, industry bodies and Australian and international organisations on a range of topics and issues that relate to our customers, our people and the community including safety on the road.

In responding to the Department of Home Affairs Strengthening Australia's cyber security regulations and incentives consultation, IAG have considered all questions but have only responded where we have specific feedback.

IAG's Role in enhancing the Cyber Resilience of Australian businesses

IAG develops and delivers insurance products that align to our purpose to 'make your world a safe place'.

In recent years this has extended to offering Cyber Insurance products specifically tailored to the needs of small to medium enterprises (SMEs). These products address the growing need to provide the expertise and to quickly respond to cyber incidents and cover the costs of recovery.

IAG's own experience in the sales and service of cyber insurance products also reveals that a significant portion of the economy is not well prepared for the increasing cyber threat landscape. IAG has been investing in awareness campaigns and proactive cyber risk assurance services (such as its investment in UpGuard) to educate Insurance Brokers and SMEs on the threats and the risk mitigation options.

IAG, as a regulated financial services provider, also has made significant investments to uplift its own security capabilities and demonstrate its commitment to meet its obligations defined in APRA's Standard for Information Security (CPS-234).

Through its experience with providing Cyber Insurance and proactive risk management services to SMEs and its experience as a regulated financial services provider, IAG is well placed to offer its view on a number of topics that the government is seeking feedback on.

Q1. What are the factors preventing the adoption of cyber security best practice in Australia?

IAG's view is that there are many competing sources of best practice for cyber risk management and security management that are available internationally and domestically. This presents a challenge to many businesses to determine which practice is the most suitable for their size and nature of business and level of maturity.

IAG's view is that the Government has the opportunity to simplify this complex landscape of various competing and overlapping standards of good practice. This could be achieved by developing a more uniform set of security best practices that Australian businesses can leverage as a common reference.

Furthermore, this could be used as a basis for the development of National "Code of Practice" that Australian businesses could adopt to demonstrate that they are addressing their cyber risks in a consistent way. Further, sector specific "Codes of Practice" could be developed and tailored to the cyber threat landscape for each industry sector.

Q3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?

IAG agrees with the Government's view that establishing a common set of principles-based requirements is an appropriate approach to provide clearer direction. Adopting this approach recognises that businesses need to be permitted to take a proportionate approach based on the nature of their business, the environment in which they operate, their level of maturity and the scope of operations.

IAG recommends that Government consider extending the principles-based approach adopted by APRA (defined in CPS-234) and extending this to other sectors as a basis for requirements that can be applied consistently across all Australian businesses.

Similarly, the Standards defined by APRA are supported by a set of guidelines published as "Prudential Practice Guide CPS234 Information Security". This could also be adopted by other industry sectors as a good foundation for medium-to-large enterprises seeking advice on generally accepted best practices.

Q4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

Some key sectors of the economy already have regulations in place that support the objective of ensuring sound cyber security management practices are in place.

Where this is the case, IAG believes the Dept of Home Affairs should collaborate with the current regulators to review the current regulations and make any vital amendments; instead of introducing a new set of regulations. This will avoid unnecessary overlapping and/or conflicting requirements. Furthermore, this will avoid the burden of additional costs of managing and reporting compliance to multiple regulators.

Q8. 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?

IAG's view that underpinning the Privacy Act with a supplementary cyber security code is not the optimal method for setting guidance or prescriptive requirements to manage cyber risks.

The Privacy Act's design and scope is to ensure the protection of personal information. It is not designed to address other cyber risks such as threats to availability of critical business systems, threats to the integrity of information, or threats to physical safety of people and assets.

Furthermore, the Privacy Act only applies to organisations with an annual turnover that exceeds $3 million (with some exceptions). Therefore, many small businesses will not be motivated to uplift their cyber risk management practices if additional requirements are included in this legislation.

IAG's view is that the Government should consider associating a cyber security code with the Corporations Act so security practices can be uniformly applied to address the broader range of cyber risks.

Q22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

IAG supports the view that the Government should establish general guidelines that Australian businesses can use to implement voluntary disclosure policies. More specific guidelines could be provided for classes of business such as technology companies that develop software.

Q23. 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?

IAG has had first-hand experience with the operation of a cyber health check program designed for small businesses. This has been conducted in conjunction with our cyber security startup investment partner, UpGuard.

IAG's view is that these cyber security health checks which provide an assessment and benchmark of a SMEs cyber security posture, have proven to be an excellent approach to educating SMEs about their cyber risks and how to proactively mitigate their exposures.

Q24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

General Insurers that offer Cyber Insurance already undertake health checks as part of the process of collecting information to rate the risks and to determine appropriate pricing and terms as part of the underwriting processes.

As the market for Cyber Insurance matures, small businesses with good practices may benefit from lower insurance premiums for continually maintaining healthy proactive cyber security practices

The Government could consider developing a self-assessment health check program that small businesses could use to identify and assess their risks. Alternatively, the Government could partner with specialist industry partners that can provide assistance to businesses that may need a benefit from more in-depth cyber health checks, and ongoing cyber risk monitoring and assurance services.

Q25. If there is anything else we should consider in the design of a health check program?

IAG believes that a health check program provides a basis that businesses can use to measure improvement in cyber risk practices. Generally, a Health Check program will produce a set of recommendations that can be then used by a business to take action.

However, a health check program invariably leads SMEs to seek further guidance because they may lack the expertise to know how to implement the recommendations.

A Health Check program needs to be underpinned by an easy-to-understand and easy-to-apply set of resources that SMEs can use as guidance so they can take the right course of action.

If you have any questions or require any further information, please do not hesitate to contact Ian Cameron at [redacted].

Yours sincerely,

[redacted]

Jeff Jacobs
Executive General Manager
Cyber & Protective Services