AmCham

American Chamber of Commerce in Australia
Level 6, 48 Hunter Street | Sydney NSW 2000

(02) 8031 9000 ☎
nsw@amcham.com.au ✉
www.amcham.com.au 🌐

Friday, 17 September 2021

Mr Michael Pezzullo AO
Secretary
Department of Home Affairs
By Email: techpolicy@homeaffairs.gov.au

Dear Mr Pezzullo,

The American Chamber of Commerce in Australia appreciates the opportunity offered by the Department of Home Affairs to make a submission on *Strengthening Australia's Cyber Security Regulations and Incentives* (Discussion Paper).

The Chamber was founded in 1961 by Australian and American businesses to encourage the two-way flow of trade and investment between Australia and the United States, and to assist its members in furthering business contacts with other nations. AmCham is Australia's largest and most active international chamber of commerce, representing some of America's most significant companies operating in the Indo-Pacific region, as well as local start-ups and SMEs. In pursuing its purpose, the Chamber has found itself not only representing the United States' business view, but also speaking increasingly for a broad range of members involved in the Australian business community.

As you may be aware, the bilateral relationship was formed in the trenches during WWI. Over 100 years of mateship, the alliance has grown and diversified to encompass political, diplomatic, economic, and military ties. This year, we will celebrate the 70th anniversary of the ANZUS treaty. The US Australia alliance is underpinned by core common values including the rule of law, transparency, hard work and fair play. The relationship has provided an immense benefit to Australia – including new jobs, higher wages, elevated productivity, market access, capabilities, intelligence, interoperability, research and development, trade and investment, cultural ideas, and exchanges of people.

The current two-way trade and investment relationship between our countries is valued at almost $2 trillion. US trade and investment in Australia in 2019 accounted for $131 billion or 7% of Australia's GDP, roughly equivalent to the mining sector. And over a quarter of all foreign investment in Australia comes from the United States, making it the biggest investor in our country. There are 323,000 Australians working for 1,100 US majority owned companies in Australia on a median salary above $100,000. US companies also spend $1.2 billion a year here on research and development.

Introduction

The Pandemic has accelerated the uptake of ICT and has demonstrated the essential role of digital technology in the country's continued resilience and prosperity. Now more than ever, Australians are empowered by the multitude of benefits afforded by ICT including increased productivity and efficiency, business continuity, and access to global markets. Cyber security will only become increasingly important as digital technologies and services are further entwined with how we govern, do business and live.

We are also experiencing a time of great change in the geostrategic environment. Although this has emphasised the value of developing sovereign capabilities, careful consideration should be afforded to balancing this with outsourcing/collaborating with trusted partners, within the Five Eyes, whose values and security interests are aligned with that of Australia.

Why Should Government Take Action?

AmCham welcomes the endeavour of the Department of Home Affairs to make Australia's Digital economy more resilient to cyber security threats.

First and foremost, education and increased awareness will undoubtedly play an integral role in the adoption of cyber security best practice in Australia. Currently, most organisations do not have the level of internal expertise required to keep across the rapidly changing risk landscape (i.e. human v human threat to human v AI threat) leading to insecure and suboptimal practices, in turn making businesses vulnerable to cyber crime. There is also the widespread misconception that getting cyber insurance will transfer risk.

Furthermore, cyber security threats and intrusions are persistent, evolving, and increasingly severe, creating global challenges to protect sensitive information, critical assets, the environment, and safety of the public. One of the approaches to tackle the threat is to prioritise cyber risk management and the security of information and communication technologies that underpin the digital economy via risk-based, flexible, and balanced approaches.

A multi-stakeholder framework to address cyber threats and risk management activities through a common, transparent, and international approach may be the best way forward. Prescriptive approaches, mandatory or sanction-based security measures degrade ongoing investments in cybersecurity, while divergence in regulatory frameworks shifts limited information security resources from risk management activities to compliance requirements.

The Current Regulatory Framework

Australia's current regulatory environment could evolve to improve clarity, coverage and enforcement of cyber security requirements through:

- **Policies that permit data flows:** Cyber incidents and risk management activities are international in scope and network monitoring, trends, and threat information are shared across borders.

  Information security professionals rely on timely access to cyber threat data (e.g., signatures, indicators of compromise, vulnerabilities) to enhance situational awareness, calibrate defensive measures, and share mitigation strategies with stakeholders. Restrictive localisation regulations artificially create cyber risk by creating blind spots to timely and actionable information exchange. It is recommended that risk-based approaches be adopted, permitting innovation and the free flow of data while meeting the legitimate security needs of law enforcement.

- **A standardised approach:** Businesses are required to comply with the requirements of multiple departments as well as a range of international standards. There is also a lot of cross over among the requirements that, if coordinated properly, would provide efficiencies for both Government and industry.

- **Alignment with global standards:** Businesses are facing an increasingly fragmented global regulatory landscape. Companies that want to invest and participate in the market often confront legal challenges, lessening their ability to comply with multiple, overlapping, and duplicative security measures. Where possible, cyber security policies should rely on existing standards. For example, the US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Framework), which was developed through an international multi-stakeholder process could be one approach. We encourage the Government to avoid national approaches that create patchworks that are not cohesive, which increase the likelihood that country-level regimes conflict with one another. Instead, we recommend efforts be made to align Australia's approach with international standards and best practices. Cyber security requirements and notification obligations that are globally aligned minimise complexities, reduce administrative burdens and the risk of error, improve system security and incentivise businesses to make the right investments.

- **Periodic Audits / Briefings:** The ICT environment is rapidly evolving, constantly revealing new threats and making it difficult for the regulatory environment to keep pace. It is recommended Australia's overall cyber posture be independently audited at regular intervals. Further, it is recommended the ACSC hold bi-annual briefings with industry to help ground threat and risk assessments, review the regulatory framework, and develop deeper trusted relationships.

  It should be noted that ICT cuts across multiple sectors – it has a horizontal structure as opposed to a discrete vertical structure like the health, transport and logistics or energy sectors. We encourage the Government to consider a different approach to its traditional consultation. The IT sector – whose clients cut across multiple industry sectors - is uniquely placed to truly partner with the Government on this agenda.

Part 1: Setting Clear Expectations

Governance Standards for Large Businesses

Generally large businesses are equally incentivised to have appropriate risk management practices in place. Cyber issues have long been high on the list for risk in corporate boardrooms, particularly at larger institutions. Many institutions that are publicly traded list cyber risk as a key risk area and promise shareholders that the company has sufficient practices to manage that risk. Therefore, adding requirements only for large businesses is unlikely to move the needle on preventing cyber issues.

If standards are being considered, AmCham would support the development of voluntary governance standards for larger businesses. It is recommended that any voluntary governance standards:

- Outline a set of minimum (baseline) guidelines describing the responsibilities and processes for managing cyber security risk that businesses (and cloud providers) should conform to;
- Support the role of company boards overseeing cyber security risk. One way to get board and senior level oversight on cyber would be to encourage boards to voluntarily diversify to include technology and cyber experts or ensure boards have access to cyber experts, as needed, to assess management's representations regarding the overall security posture of the firm;
- Encourage organisations above a certain size, as a best practice, but not mandatory, to employ a cyber security officer (i.e. similar to a health, safety and environment officer which is mandated for organisations above a certain size in many jurisdictions);
- Not require specific technical controls to be implemented; and

AmCham National Partners
KPMG NORTON ROSE FULBRIGHT
AmCham Premium Members
3M THE ADECCO GROUP AIG AMERICAN EXPRESS AT&T BHP BOEING citi Coca-Cola BRICKWORKS ConocoPhillips Brookfield CSIRO CAT CBRE DXC.technology
GE Google Incitec Pivot Limited INPEX NORTHROP GRUMMAN Johnson&Johnson J.P.Morgan JONES DAY K&L GATES Kellogg's lendlease LOCKHEED MARTIN
McKinsey&Company ORD MINNETT MetLife Pfizer pwc Raytheon Australia sky news stryker THE UNIVERSITY OF SYDNEY STRATEGIC EDUCATION INC TORRENS UNIVERSITY AUSTRALIA verizon

- Be co-designed through the multi stakeholder model.

As mentioned in the Discussion Paper, there is currently a shortage of cyber security experts in Australia. Any efforts to strengthen Australia's cyber resilience will require the development of talent through educational programs and the creation of a better pipeline of cyber security experts.

Access to a pool of skilled resources such as a centre of excellence may assist in incident response.

The US Department of Commerce's National Institute of Standards and Technologies' Cyber Security Framework[i] (NIST Framework) is just one example of a construct helping businesses to better understand and improve their management of cybersecurity risk. The NIST Framework comprises a set of actions (see below) a business can take to achieve specific cyber security outcomes:

- **Identify**: Develop/enhance organisational understanding to comprehend and manage cybersecurity risk (For example through a series of structured programs/certifications/skill development courses in the various areas pertaining to cyber security);
- **Protect**: Develop and implement appropriate safeguards against threats (this could be grounded on the voluntary guidelines to be implemented by Government);
- **Detect**: Develop and implement appropriate activities to identify the occurrence of a cyber security event. (the abovementioned Centre of Excellence could play a key role here);
- **Respond**: Take appropriate action on a detected cyber security event. (As this action needs to be swift and decisive, an appropriate incident response mechanism needs to be in place. Again, the Centre of Excellence could assist with this); and
- **Recover**: Appropriate activities for resilience and recovery from any cyber security event. (This will need to be organisation specific due to the different business models and systems adopted by organisations).

It should be noted that adding additional governance requirements will only increase compliance costs to the company without providing additional protection. Consequently, this has the potential to negatively impact a company's budget for improving the actual technical controls. For example, it's a much better cyber defence to spend resources ensuring appropriate vulnerability patches than hiring a person to monitor whether the risk management program is consistent with regulatory guidance.

Compliance-focused regulatory models also do not create the flexibility for the businesses and Government to protect them. It is important for Government cyber security policies to recognise that cyber security threats are ever evolving and that the tools needed to confront them must also evolve. Intelligence sharing and international best practices enable organisations to adopt cyber security practices and procedures in a manner that is consistent with their respective business models and relevant risks.

It is recommended the Government carefully balance legitimate public policy needs to improve resistance to cyber attacks while creating a framework that is flexible, adaptable and scalable to work for both small and large organisations and everyone in between.

Minimum Standards for Personal Information

The Privacy Act in Australia requires organisations to take reasonable steps to protect personal information, which includes actively monitoring the cyber risk environment for emerging threats and taking reasonable actions to mitigate those risks.

Given existing incentives to maintain rigorous risk management practices, our preference would be to maintain the status quo. However, if standards are being considered, AmCham would support the development of voluntary governance standards. Once again, consultation with industry will be critical in this process.

It is recommended that any voluntary governance standards:

- Be tailored to be commensurate with the size of the organisation and the risk associated with the company's activities and data collection practices;
- Be risk-based (as opposed to static technical controls) to ensure the requirements keep up with emerging technology in cyber and can be designed in a manner that is appropriate for the organisation; and
- Adopt safe harbors for compliance with industry standards (ISO, NIST) and other laws (both in Australia or globally) to ensure harmonisation of cybersecurity requirements rather than adding compliance complexity for organisations that already comply with commensurate cyber legal requirements or industry standards globally.

As outlined above, ICT cuts across multiple sectors. Therefore, any standards should apply both vertically and horizontally.

Part 2: Increasing Transparency and Disclosure

Responsible Disclosure Policies

Cyber breaches have the potential to impact the supply chain and multiple organisations across industries. The Chamber supports the responsible disclosure of cyber events as we seek to warn others of risks more broadly. However, it is important to balance disclosure with the importance of protecting victim organisations from further adversity. Not all organisations will respond to cyber attacks in the same way and no regulation should seek to penalise an individual company's approach. It is recommended the Government consult widely with industry on appropriate responsible disclosure policies before any regulation is considered. Again, AmCham encourages the pursuit of greater global consistency of approach, especially amongst Five Eyes nations.

Health Checks for Small Businesses

AmCham would welcome a cyber security health check program for small businesses. Whilst this is a great initiative for business owners, it should be noted that the ability to implement corrective actions is commonly constrained by cost and specialist cyber security knowledge.

Measures to increase cyber security awareness and knowledge amongst business owners may include enhanced promotion of 'User Guides' to assist small business on preventative and corrective actions with regards to their cyber security posture. While User Guides are available on the Australian Cyber Security Centre (ACSC) website (www.cyber.gov.au/acsc/small-and-medium-businesses), this is generally not the first place to look for SME business support. It is recommended that User Guides or web links be included on the following websites forwarding business owners to the ACSC website:

- www.business.gov.au/new-to-business-essentials
- www.asic.gov.au/forbusiness/small-business/starting-a-company
- www.ato.gov.au/Business/Starting-your-own-business/Before-you-get-started

Further, the Australian Government's New to Business Essential website is a primary support portal for business owners, providing a range of workshops and webinars for SMEs. We also recommend the website be updated to include cyber security workshops for increased awareness and education.

Garner Learnings through Simulation

ICT systems can be quite complex – layered with client requirements, legal obligations and procedures. Australia's critical infrastructure reforms are aimed at rapid response. The nation's cyber preparedness is best understood through simulations which can help to identify issues, gaps and learnings.

Accordingly, it is recommended the Government run simulations with industry of possible cyber attacks as a means of testing the procedures articulated by the critical infrastructure legislation.

Thank you for your consideration, and for this opportunity to submit AmCham's views to this Discussion Paper. We welcome any queries you have regarding our submission and any opportunities to further engage in the consultation process.

Kind regards,

April Palmerlee
Chief Executive Officer

AP: ao

[i] *Cybersecurity Framework* (2021) National Institute of Standards and Technology, https://www.nist.gov/cyberframework