COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Department of Home Affairs
in response to the

2023-2030 Australian Cyber Security Strategy Discussion Paper

28 April 2023

CONTENTS

Communications Alliance

Communications Alliance is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

For more details about Communications Alliance, see http://www.commsalliance.com.au.

Introduction

Communications Alliance welcomes the opportunity to provide a submission to the Department of Home Affairs 2023–2030 Australian Cyber Security Strategy Discussion Paper.

Communications Alliance recognises the significance of focusing on and enhancing Australia's cyber security – a reality emphasised by recent and ongoing national cyber incidents. The rapid development in technology and its increased integration into our daily lives has exacerbated the need of effective cybersecurity measures.

A cyber security strategy is, equally, an important tool to foster a whole-of-society and economy-wide approach to cyber security and it ought to form the cornerstone to identify, and subsequently remedy, educational, skills and awareness existing gaps in our security framework. The strategy must be forward-looking and take into consideration the accelerating evolution of technology and the need for agile reaction to the constant change in methods used for cyber-attacks.

Our members take cyber security very seriously, are currently engaging with Government and will continue to engage in the future with cyber security initiatives to seek to counter existing and emerging risks. Industry has also taken proactive steps to develop and apply industry-wide cybersecurity standards and best practices.

We commend Government for the wide and public consultation on this important topic and believe that an open and pragmatic discussion of this matter will assist with the development of a strategy that is effective, efficient, and proportionate, while being sufficiently flexible to accommodate the dynamic environment in which it operates.

1. Ideas

Question 1:

> *"What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?"*

The Strategy includes a variety of different themes, including potential further regulatory reforms, possible strategies to deal with ransomware attacks, international partnerships and standards setting processes and the need for a skilled cyber security workforce for Australia, just to name a few.

However, it is not clear how the strategy builds on or relates to some of the issues raised in the National Data Security Action Plan (NDSAP). It would be useful to understand whether Governments intends for the NDSAP to co-exist in parallel with the 2023-2030 Cyber Security Strategy. In our view, that Government could explore rolling the NDSAP into the 2023-2030 Cyber Security Strategy. In the absence of knowing Government's intentions, we take the opportunity to reiterate some of the feedback in relation to data localisation that we have provided in the context of the Discussion Paper on the NDSAP.

In principle, we advocate for a free flow of information across geographic borders to optimise organisations' participation in the global economy. We are pleased that the Australian Government recognises that digital trade is a key driver of economic growth and has identified data localisation requirements and data flow restrictions as potential risks to digital trade[1].

Indeed, data localisation requirements complicate or impede operations and increase the cost of doing business for organisations that operate across regulatory jurisdictions. The OECD

[1] Refer to p. 86, Department of Foreign affairs and Trade, *Australia's International Cyber and Critical Tech Engagement Strategy:* "Australia seeks to shape an international environment that enables digital trade and reinforces the international rules-based trading system. Essential to this is the reduction of digital trade barriers, such as data localisation requirements and data flow restrictions." as accessed at https://www.internationalcybertech.gov.au/sites/default/files/2021-04/21045%20DFAT%20Cyber%20Affairs%20Strategy%20Internals_Acc_update_1_0.pdf, 13 April 2023

guidelines, that focus on economic benefits derived from a personal data protection framework, support the free movement of personal data. The OECD argues that restrictive personal data localisation requirements affect firms' ability to adopt the most efficient technologies, influence investment and employment decisions, increase the cost of innovation and lead to missed business opportunities. Arguably, similar points can be made for other types of data.

Security, privacy, economic considerations and data efficiency (e.g., latency, proximity to other datasets, etc.) can be optimised when cloud-based services can leverage distributed network infrastructure without geographic restrictions. The physical location of data does not, in itself, make the data secure. Rather, what matters more are technological controls to establish and maintain data security and privacy, along with policies that ensure best practices are adopted.

We recognise some geographic regions are susceptible to potential sovereign risk. We recommend that the Government account for the economic, business and trade implications in its consideration of any regulation, as well as considering whether there are alternate policy tools (such as guidance) that could achieve similar objectives, to enable Australian entities (including Government, businesses and consumers) to effectively manage their data security risk.

Data localisation requirements can also make data more susceptible to attack. Requiring data to be stored or processed in one location can make it an attractive target for bad actors (i.e., a larger 'prize' if the attack is successful) and hence, more likely to attract cyber-attacks.

The global internet infrastructure comprises tens of thousands of independent networks that store and carry data across national borders, typically without the network providers having visibility into the data's contents. Data localisation requirements would, directly or indirectly, impact the flow of data across such networks; affecting the internet's resilience, performance, efficiency and global interoperability.

Consequently, we believe that in developing a data security strategy, Government ought to focus on providing guidance on technical controls to uplift the security of data, rather than imposing data localisation policies which may have significant negative impacts on the adoption of technology in the Australian economy. It is important that cyber security within Australia is upheld by entities, but this also requires a 'two-way street' that includes a focus on the responsibility of individuals to maintain cyber hygiene. In the OAIC's recently-released Notifiable Data Breaches Report, it revealed that 49% of data breaches resulted from cyber security incidents.[2] However, out of those 49% of data breaches, the second highest factor was phishing, accounting for 26%, while only 8% of breaches were a result of hacks.[3] We believe customers should take advantage of information available around scams and how to avoid potential cyber security risks. Individual vigilance – teamed with ongoing extensive cyber safety efforts by industry – is a better formula for ensuring everyone in society is prepared and well-resourced against cyber threats. It is essential that Government invest in and encourage public education on cybersecurity as an integral part of the Strategy, as organisations can only do so much in their policies and management to stop cyber hacks and scams.

2. Legislative and regulatory reform

The Australian government should ensure, when implementing any new regulation or legislation, that there is a clear articulation for what it is trying to resolve. There is great significance in having clarity of purpose and simplifying the issue to enable entities to properly engage with it on a clearly defined set of definitions and parameters. In our view,

[2] p. 2, Australian Government, Office of the Australian Information Commissioner, Notifiable Data Breaches Report January – June 2022, Nov 2022.
[3] Ibid.

there is still a degree of opacity to exactly what Government wants to achieve with the proposed Cyber Security Act and how successful it would be in enforcing cyber security resilience or harmonising the current extensive and broad mechanisms that already aim to address cyber security in Australia.

We experience some disquiet, for example, when government states that the objective is to make Australia the world's most cyber-secure nation by 2030. To our mind, security is a means of achieving other objectives. It is not the objective in and of itself.

Cyber security is not a 'single-issue' problem, but rather a series of discrete problems with discrete causes and solutions. Therefore, a monothetic solution is not viable, with differing industry and enterprises operating in Australia. In our view, existing industry-specific obligations are effective as they provide the ability to address distinct issues that affect different industries across the sector, that go beyond a minimum baseline standard.

Another strategy Government should pursue is to effectively 'de-value' personal information that criminals are attempting to obtain. We are supportive of Government initiatives in finding better ways for ID verification that reduce the need for individuals to hand over personal data.

Question 2:

> *"What legislative or regulatory reforms should Government pursue to: [sic] enhance cyber resilience across the digital economy?"*
>
> No comment.

Question 2a:

> *"What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance?"*
>
> No comment.

Question 2d:

> *"Should Australia consider a Cyber Security Act, and what should this include?"*

Australian critical infrastructure sectors have recently undergone and are still undergoing regulatory and legislative reform processes as part of the reforms relating to the *Security of Critical Infrastructure Act 2018* (SoCI Act) and/or other sector-specific legislation and regulations.

In our industry, the data storage and processing sector is implementing the asset register, cyber incident notification and risk management program requirements under the SoCI Act.

The telecommunications sector is working through the implementation and fully embedding the requirements of the *Telecommunications (Carrier Licence Conditions—Security Information) Declaration 2022* and the *Telecommunications (Carriage Service Provider—Security Information) Determination 2022*.

In addition, the sector is still awaiting Government's response to the report by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the PJCIS's *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms*. Irrespective of Government's response to the PJCIS report and its recommendations, it would be crucial to avoid duplicative requirements for the industry under the TSSR (*Telecommunications Act 1997*) and the SoCI Act.

Consequently, in our view, it would be appropriate to first allow the respective sectors to fully implement and embed the recent regulatory and legislative changes into systems and processes before considering further changes to the regime. Additionally, the development of reporting and notification protocols could assist with the practical operationalisation of requirements under the current regime.

Where regulatory and legislative reform processes have not been completed as part of an already commenced process, those ought to be given the time to be completed in an orderly manner.

In a second step – and prior to considering further reform mechanisms and processes or even a new Cyber Security Act – we recommend a thorough audit of the existing regulatory and legislative landscape to identify gaps and overlaps. If, upon such analysis, there are overlaps, these should be eliminated; and for any perceived or actual gaps, caution should be exercised as to whether further regulation would indeed be the most appropriate means to achieve the desired outcome. (On a similar point, refer to our response to Question 2b.)

In this context, we note the recent commentary by the Productivity Commission that *"Government initiatives to improve cyber resilience and response should be 'light touch' where the risks are relatively low. This minimises the potential for unnecessary costs to be imposed on businesses while still supporting better security outcomes."*[4]

Importantly, particularly for higher risk situations and associated regulation, the Productivity Commission also makes clear that Government *"should monitor and evaluate the effectiveness and economic impact of implemented policies to improve its understanding of the trade-off between security and growth, and recalibrate the regulations as required."*[5] However, the SoCI Act, in particular, currently does not include an independent review process. Consequently, Finding 4.16 of the Productivity Commission notes *"Cyber security regulation of high-risk sectors needs to manage the risks without unnecessarily deterring businesses' innovation and investment. The impacts of Government's recent critical infrastructure security regulations remain unclear but, while more time and information is required to understand whether these regulations strike an appropriate balance, there is no evaluation or review process included in the legislation."*[6]

We concur with the finding that more time for analysis and evaluation is required, and recommend an independent review of the SoCI Act in 2026, being three years after the risk management program obligations were switched on for some classes.

Question 2b:

> *"Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?"*

The Discussion Paper suggests for consideration the inclusion of 'customer data' and 'systems' into the definition of 'critical asset' in the *Security of Critical Infrastructure Act 2018* (SoCI Act). The Paper appears to suggest that the existing powers under the SoCI Act have not been sufficient to allow Government to adequately deal with recent data breaches, where customer data had been compromised.[7] However, we oppose the inclusion of customer data and systems into the definition of critical asset in the SoCI Act. This inclusion would not address the problem, as remediation of an incident is likely best handled by the affected entity rather than through Government exercising intervention powers.

Rather, we submit that the sharing of information between relevant organisations (e.g., banks) on what data (including personal data) is compromised is a key aspect to managing

[4] Vol. 4, p. 77, Productivity Commission, *5-year Productivity Inquiry: Advancing Prosperity*, Feb 2023
[5] p. 80, ibid
[6] p. 80, ibid
[7] p. 17, Expert Advisory Board, Australian Government, *2023-2030 Australian Cyber Security Strategy Discussion Paper*, Feb 2023

future data breaches. While, in the telecommunications sector, the *Telecommunications Amendment (Disclosure of Information for the Purpose of Cyber Security) Regulations 2022* seeks to address the current legal constraints on such data sharing arrangements (though we note the Regulations automatically sunset in late October 2023), other sectors may not have similar arrangements in place. We submit that this ought to be a focus for Government action.

Further, given that data breaches can and do originate in many different sectors, to the extent that the protection and sharing of personal information is concerned, this is more appropriately dealt with through mechanisms in the (to-be revised) *Privacy Act 1988*.

It is also worth noting that the definition of 'asset' under the SoCI Act is already broad and includes 'a system', 'a device', 'a computer program', 'data' and 'any other thing', which raises the question what effect the proposed expansion of 'critical asset' practically would have.

Question 2c:

> *"Should the obligations of company directors specifically address cyber security risks and consequences?"*

We do not believe that this is required, given that company directors and senior executives already have obligations to manage cyber security risks and consequences. The two duties most relevant in this context are:

- the duty to exercise their powers with due care and diligence; and
- the duty to exercise their powers in good faith in the best interest of the corporation/organisation.

In addition, the company regulator's willingness to enforce relevant security regulations and requirements is demonstrated in the recent decision in *ASIC vs RI Advice Group Pty Ltd*, where an Australian financial services (AFS) licensee was found to have breached its licence obligations after failing to adequately manage its cybersecurity risks and ensure the financial services covered by its licence were provided fairly and efficiently.

On its website, the regulator notes:

> *"ASIC expects directors to ensure their organisation's risk management framework adequately addresses cyber security risk, and that controls are implemented to protect key assets and enhance cyber resilience. Failing to do so could cause you to fall foul of your regulatory obligations."*[8]

Inclusively, the Critical Infrastructure Risk Management Program (CIRMP) requires entities to provide an annual report to the relevant Commonwealth regulator. This new board attestation in the CIRMP provides ASIC a reference point to take further action, to enforce any breach of directors' duties.

We acknowledge that cyber security is important, however this would need to be considered in conjunction with other material risks that may occur. It would, therefore, not be ideal to distinguish cyber risks from other potential risks to entities, and it is suggested that an all-hazards risk-based approach should be encouraged.

The Australian Institute of Company Directors has also published *A Director's Guide to Governing Information Technology and Cybersecurity*. The guide emphasises that in

[8] Australian Securities & Investments Commission, as accessed at https://asic.gov.au/about-asic/news-centre/articles/cyber-risk-be-prepared/ on 12 April 2023

exercising these duties organisations should, where possible, acquire expertise in IT and have policies in place to deal with breaches and cybersecurity.[9]

Question 2e

> *"How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?*

Harmonisation of frameworks/strategies/requirements

We recommend that Government consolidate Federal and State cyber security strategies and requirements into a single Australian cyber security framework. Currently, businesses are faced with multiple overlapping, inconsistent and at time redundant security requirements spread across several Federal and State Government frameworks sitting in different Departments and agencies, thereby further complicating compliance for entities. The frameworks and requirements include the:

- Hosting Certification Framework (HCF) under the Digital Transformation Agency (DTA);
- Protective Security Policy Framework (PSPF) under the Attorney-General's Department (AGD);
- Information Security Manual (ISM), and the Information Security Registered Assessors Program (IRAP) assessment of services under the Australian Cyber Security Centre (ACSC) in the Australian Signals Directorate (ASD);
- Essential 8 (E8) under the ACSC (ASD);
- State-specific security frameworks, such as the New South Wales Cyber Security Strategy 2021, the Victorian Cyber Security Strategy with its recently announced Mission Delivery Plan 2022-23 (and Cyber Security Hubs), and the Queensland Government Information Security Policy; and
- Sector-specific legislation/regulation (e.g., for the financial services sector).

In addition, the Department of Defence released the Defence Cyber Security Strategy (DCCS) in August 2022. The DCCS explains that it "should further enable strategic partnerships with industry, acknowledging industry partners' critical role in Defence's overall cyber security posture."[10] However, we are unclear about industry's exact role in the DCCS or how it interacts with the National Strategy or any of the State Strategies.

Mapping and managing these various security compliance requirements is particularly difficult for entities that operate globally, as Australian domestic standards either only partly overlap and/or veer from global security standards. This burden is also particularly acute for small and medium enterprises (SMEs) that lack the internal capacity to manage compliance with multiple standards. Where compliance to domestic standards is made a prerequisite to public sector procurement opportunities, Government is not only limiting its ability to adopt world's best security technologies and services, but also precluding domestic players from participating in such opportunities.

We recommend lessening industry's administrative and financial burden for meeting Australian-specific cyber security controls and standards – and thus increasing the availability of security services available to the Australian Government – by focusing on harmonisation, both internationally and domestically (between Federal and State security requirements) and increasing international interoperability with major global security frameworks. Specific recommendations include:

[9] Dr Nicholas J A Tate, Alexander J G Tate, Australian Institute of Company Directors, *A Director's Guide to Governing Information Technology and Cybersecurity*, 2016
[10] p. 13 Australian Government, Defence, *Defence Cyber Security Strategy*, Aug 2022

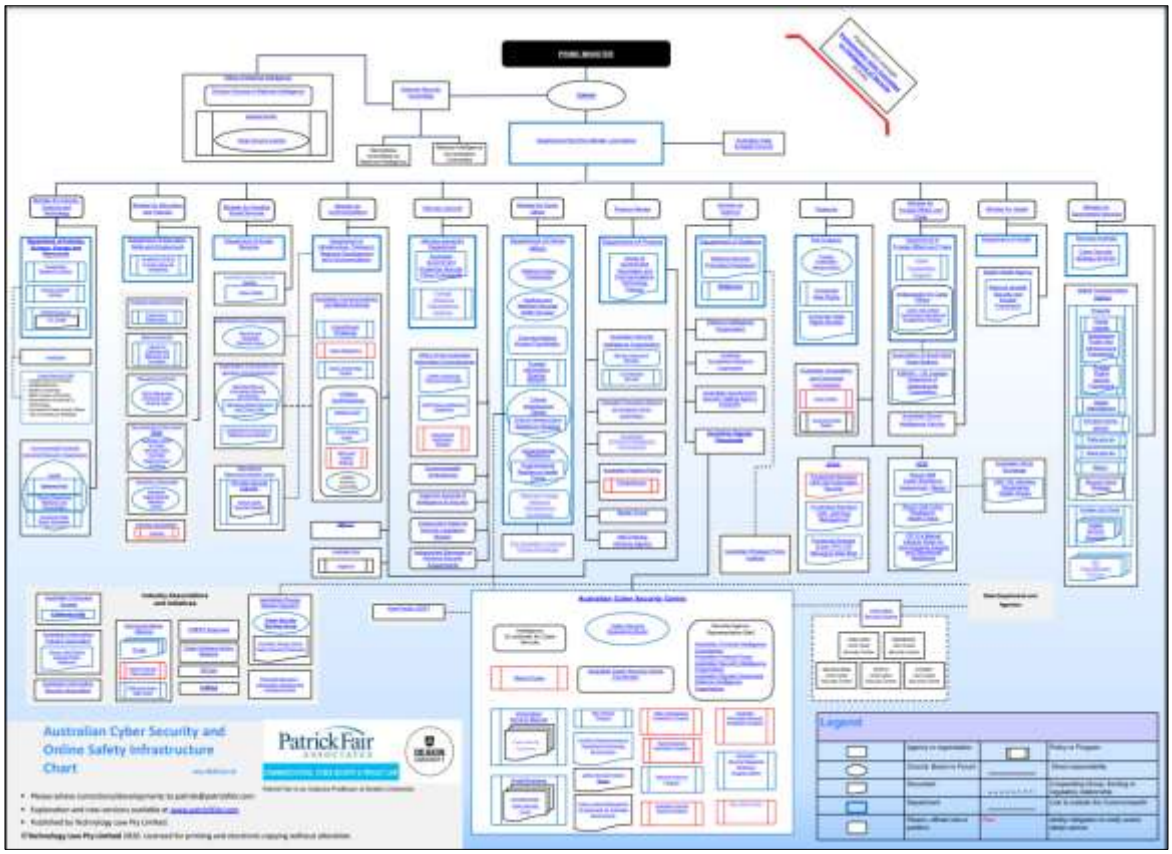
- Seeking a single, overarching cyber security framework that harmonises Federal and State security requirements;
- Removing overlapping requirements between leading global cyber security frameworks and the Australian Government ISM. For example, cryptographic standards are broadly standardised among like-minded countries. However, companies that have already demonstrated compliance with US FedRAMP encryption standards must also demonstrate compliance with Australia's ISM;
- Relying on businesses demonstrating compliance to well-established internationally recognised security standards (e.g., the ISO 27000 series) instead of domestic standards; and
- When there are clear gaps between Australian security requirements and global frameworks, the Australian government should collaborate with partner nations to ensure that these Australian-specific requirements are addressed in the larger globally-recognised cyber security frameworks, particularly the US' FedRAMP and National Institute of Standards and Technology (NIST) / Federal Information Processing Standards (FIPS).

Finally, a major aspect of regulatory burden is the effort to interpret vaguely-worded legislative requirements. For example, the definitions of 'critical infrastructure' and 'asset' in the SoCI Act leave much room for interpretation and give rise to uncertainty. This interpretational burden is particularly acute for SMEs that typically lack the legal and technical resources and capacity to make such interpretative analysis and judgement calls. We urge Government to provide significantly more explicit guidance for industry that can be easily understood and accessed by a wide range of businesses. Such guidance ought to specifically address the uncertainty caused by vague definitions, e.g., with illustrative case studies. While not perfect in all respects, the Data Retention Frequently Ask Questions for Industry manual issued by the Office of the Communications Access Co-ordinator may serve as an example as to how more specific, meaningful guidance can be given to industry.

Streamlining of organisational, functional and process-related resources

As noted in previous submissions, as a matter of principle, Government's strategy on cyber security ought to focus on coordination, optimisation and efficiency in the use of Government resources to fight cybercrime and to protect critical infrastructure from unauthorised access and interference.

Unfortunately, the Australian cyber security landscape is characterised by an almost bewildering matrix of Government departments and agencies with an interest in, or portfolio responsibilities relating to, cyber security. These departments/agencies cover a large array of security-related issues and address a multitude of different stakeholders, e.g., telecommunications network operators, businesses across all sectors, the general public, etc. The below diagram illustrates this point. In fact, the landscape is so complex that it is difficult to depict it in a legible format in this submission. For an (expandable) online version of the diagram, see here. (Please note that since drafting this diagram, further changes have occurred which are not yet included, e.g., the Communication Access Co-ordinator is now under the Attorney-General's Department and the Cyber & Infrastructure Security Centre now sits under the Department of Home Affairs, and ACORN has been replaced by new reporting processes at the Australian Cyber Security Centre etc.)



https://www.patrickfair.com/_files/ugd/ce391e_546b5b105fe64af79037d0d2fe70d329.pdf as accessed on 12 April 2023

As noted in our previous submissions on this issue, it would be important to gain a better understanding of the precise roles and responsibilities of each of the involved departments/agencies, and where their responsibilities intersect and overlap. We strongly recommend a streamlining of organisations, functions and processes to allow industry, especially smaller businesses and those not intimately involved with the Australian market, to more effectively and efficiently access relevant documentation and engage with the relevant frameworks and requirements. (Also refer to our feedback at Question 13.)A better coordination of the current spread of agencies and programs and more focussed spending on a single national point of access would result in a more effective approach to cyber security, for members of the public, industry and Government agencies alike.

However, this is not to say that all cyber-related functions ought to come under a 'single roof' as it will be important to retain appropriate checks and balances the regime (e.g., by building in mechanisms for judicial oversight and/or review by independent agencies), especially with respect to the exercise of any Government powers.

It should also be noted that the chart above lists only cyber security-related organisations and initiatives and some online safety related activities, and does not include any other cyber-related Government organisations. While we do not have access to a similar chart regarding the overall cyber-related activities by Government agencies, it seems likely that a similarly complex picture exists.

Question 2f:

> *"Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by cyber criminals by:*
>
> *(a) Victims of cybercrime*
> *(b) And/or insurers? If so, under what circumstances?*

(i) What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?"

No comment.

Question 2g:

"Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?"

No comment.

3. Building our regional cyber resilience and response

Question 3:

"How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents."

No comment.

4. International Alignment

Question 4:

"What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Our industry supports all efforts to further foster greater digital regulatory alignment and certainty through digital trade rules in bilateral agreements such as the Australia-Singapore Digital Economy Agreement, and via Australia's role as a co-convenor of the digital trade negotiations at the World Trade Organisation.

Alignment with international standards, especially the ISO 27000 series or ETSI EN 303 645, helps ensure that best practices are utilised, promotes interoperability and avoids introducing unnecessary and burdensome complexity. Wherever possible, Australia ought rely to the greatest extent possible on international standards and best practices, rather than seek to develop new national standards or create diverging versions of existing international standards.

As the Productivity Commission commented in its recent Inquiry Report *5-year Productivity Inquiry: Advancing Prosperity*:

> *"There can be cross-country differences in digital and data regulations and policy frameworks. While this often justifiably reflects different countries' priorities and constituents, it can create additional burdens for businesses that operate in multiple jurisdictions. They may face extra costs in meeting inconsistent requirements, and potentially withdraw from smaller markets where regulations differ from those in larger markets because the costs outweigh the benefits of conforming to an additional set of rules. Greater international engagement between policymakers and regulators would support the development of 'interoperable policy frameworks that can streamline requirements across borders and create mechanisms to reduce regulatory overload' (WEF 2020a, p. 5)."*[11]

We urge Government to consider the costs of diverging national standards and regulation and the potential consequences for the Australian economy more broadly.

[11] Vol. 4, pp. 91/92, Productivity Commission, *5-year Productivity Inquiry: Advancing Prosperity*, Feb 2023

Question 5:

> *"How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?"*

We identified a number of regional and global fora that engage with cyber security and that, we believe, are relevant to Australia's strategic interests. However, it is not always clear to us whether Australia engages in all of those fora, and if so, through which organisation/means of representation it participates, whether this engagement is effective and whether additional or different efforts would be required, particularly also in areas that do not specifically relate to security.

The following are some of the many global and regional fora but is not exhaustive.

Global fora:

- Organisation for Economic Co-operation and Development's (OECD) Working Party on Security and Privacy in the Digital Economy
- Internet Governance Forum
- United Nations (UN) Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
- International Telecommunication Union
- Global Forum on Cyber Expertise
- Global Conference on Cyberspace
- Commonwealth Telecommunications Organisation
- National Institute of Standards and Technology (NIST)

Regional fora:

- Asia Pacific regional Internet Governance Forum (APrIGF)[12]
- Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group
- Association of Southeast Asian Nations (ASEAN) Cyber security Cooperation Strategy
- East Asia Summit

An analysis of Australian businesses' data sharing arrangements as set out in privacy policies may reveal further fora and countries of interest, and Australia's ability to demonstrate thought leadership and drive alignment in international approaches to cyber security. Australian businesses, like those of most other nations, make use of commercial advantages outside Australia and outsource some of the strategic and/or operational functions to other countries, e.g., European Union, India, Philippines, US, UK, Singapore and Japan. China plays an important role independent of any potential outsourcing arrangements due to the large quantity of devices that originate from there and the potential to greatly impact any nation's cyber space.

We would also like to see Government adopting a comprehensive and structured consultation process to assist the preparation of positions to be put forward at bilateral, regional or global fora. We are not aware of such a structured approach but note that industry does receive occasional ad-hoc requests for input.

[12] In August 2023, auDA will host the Asia Pacific regional Internet Governance Forum (APrIGF) in Brisbane. Emerging technologies are the main theme.

5. Government Best Practice

Question 6:

> *"How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other agencies?"*

Please refer to our comments at Question 2e).

We also note that the role that Commonwealth Government departments and agencies play in cyber security is important to developing best practice to ensure cyber security and resilience across the economy. Building accountability and responsibility within these departments and agencies would serve as a model for other agencies to follow and be guided by. Initiatives such as the Essential Eight developed by the Australian Cyber Security Centre (ACSC) could therefore be re-examined and adjusted to serve as such a model.

In this regard, the Essential Eight was a result of the ACSC developing prioritised mitigation strategies. However, while this initiative was mandated for all entities, there is no timeline for implementation, and the Commonwealth Cyber Posture for 2022 revealed that maturity levels remained low across the Commonwealth.[13] Notably, the number of entities that had used their Incident Response Plans, and those reporting incidents to the ACSC, was also low.[14] We believe that having clearer requirements around the timeline of when entities should implement this would bolster their uptake. This would also provide a consistent level of vigilance and preparation throughout government to effectively respond to cyber security issues.

6. Information and threat sharing / incident reporting

Question 7:

> *"What can government do to improve information sharing with industry on cyber threats?"*

Naturally, the sharing of threat information ought to be optimised, i.e., the right amount of information (i.e., only important information) ought to be shared as rapidly as quickly as securely as possible. Unfortunately, this is currently not yet the case and further improvements can be made. Overall, we believe that the current information sharing is still lacking in scope, detail and speed, i.e., our sector has, in recent years, not experienced substantial information flows coming from Government agencies that would provide its participants with detailed threat information that they did not already gather through other sources.

In this context we highlight that the PJCIS recommended in its 2022 Report on the *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms:*

"Recommendation 5

3.121 The Committee recommends that the Australian Government give consideration to establishing a dedicated telecommunications security threat sharing forum, to enable the Australian Security Intelligence Organisation and Australian Signal Directorate to brief telecommunications stakeholders about ongoing and emerging threats to the maximum classified level possible.

This forum could be a new group established under the Trusted Information Sharing Network or could be an adjunct group to the existing Communications Sector Group already established under that network, or the working group created as a result of Recommendation 3 of this report."

[13] p.3 Australian Government, Australian Signals Directorate, The Commonwealth Cyber Security Posture in 2022, Dec 2022
[14] p. 4, Ibid

We encourage Government to implement this Recommendation.

We also note that the Australian Cyber Security Centre (ACSC) has established the Cyber Threat Intelligence Sharing (CTIS) program and encourage Government to roll this program out with a broad scope and thorough implementation.

We also submit that the Joint Cyber Security Centres (JCSCs) are only sub-optimally fulfilling their intended role. To remediate the situation and instil a greater cyber uplift through each JCSC, one could consider providing each JCSC with a sectoral subject matter expert, e.g., a mining expert for the WA JCSC, whereas the Sydney and Melbourne JCSC might host experts on communications and finance etc. This would enable the respective JCSCs to better customise their threat sharing and disseminate information within their respective sectors.

To further quickly disseminate intelligence, consideration ought to be given to developing a trusted information sharing network (we note the already existing TISN) which includes private organisations that are already screening security threats at a large scale and in real-time. This network can then work with the ACSC so that Government can produce non-classified briefs to share with the wider industry community.

Question 8:

> *"During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?"*

We are aware that some confusion exists as to the role of the ACSC and its delineation from the CISC. At times there is a perception that the ACSC is the regulator for the SoCI Act or that information reported to the ACSC may shared with the (actual) regulator, the CISC. To the extent that explicit confidentiality obligations upon the ASD/ACSC can contribute to remediate this situation, we encourage such steps be taken. We also recommend further educational work be done to clarify the roles of the two agencies/centres.

7. Mandatory Reporting of Ransomware or Extortion

Question 9:

> *"Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?"*

We are not convinced that expanding the current incident notification regime would provide additional benefits to the public on the issue of ransomware and extortion.

Prior to turning to the merits of an improved public understanding of ransomware and extortion demands, we note that the *Privacy Act 1988* prescribes notification of eligible data breaches for personal information; and the *Security of Critical Infrastructure Act 2018* (including its recent amendments) and sector specific legislation and regulations set standards for the notification of cyber incidents to authorities where those meet the requisite thresholds. We suggest that Government provide more detailed guidance (including examples) when it expects a ransomware attack and/or extortion demands to fall within the definitions of a reportable 'critical' or 'other cyber security incident'. For example, it is well conceivable that extortion demands on individuals may not meet the threshold of a reportable incident.

With regard to an improved public understanding of such types of cybercrimes, it is unclear why Government is considering mandatory reporting as the vector for achieving this.

Incident reporting ought to focus on security-related goals (i.e., remediation etc.) rather than public education. What matters for the Australian public is that their personal information is not compromised in a cybercrime incident and that critical infrastructure is not compromised to an extent that essential functionalities of the economy are compromised.

We also have doubts about how effective a mandatory reporting regime for ransomware and extortion would be. There is also a real concern that public notification of ransomware attacks and extorsion attempts may lead to public concerns/panic and unhelpful media speculations without associated benefits of transparency as (1) the notifying entity will not be in a position to divulge many details given the circumstances of a potentially still ongoing criminal attack or a crime that is still under investigation; and there is also likely to be confidential and highly sensitive information involved in most ransomware or extortion cases (possibly even rising to the level of national security) and even if the information were to be released to the public, it would have to be highly redacted.

If a public reporting requirement was contemplated, it ought to be limited to incidents where the public disclosure of a ransomware and/or extortion demand clearly outweighs any potential negative consequences that may arise from doing so. Careful consideration would need to be given to the criteria used to determine the circumstances of when the threshold for a mandatory public disclosure has been reached.

If ASD is able to attribute attacks, there may be merit in publicly providing this information to allow the public to gain an understanding of the origin of the threat and, where ransoms are being paid, to form an opinion as to whether individuals would have preferred alternative pathways to resolving the issue.

To the extent that Government is seeking to sensitise the public to the issue of ransomware and extortion, we are of the view that a public education programme undertaken by Government would ultimately be more effective at achieving this aim. This could involve Government creating public education campaigns around the odious recipients of cyber crime proceeds, such funding terrorism or child exploitation.

8. Automated threat-blocking

Question 10:

> *"What best practice models are available for automated threat-blocking at scale?"*
>
> No comment.

9. Cyber Security Workforce/Skills

Question 11:

> *"Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?"*
>
> No comment.

Question 12:

> *"What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?"*

It is widely reported that Australia is already experiencing and will certainly experience a shortfall of appropriately skilled cyber security workers in the near future. For, example, the AustCyber *Australia's Cyber Security Sector Competitiveness Plan 2022* highlighted that:

> "***Australia's cyber security sector is expected to have 3,000 fewer workers than required by 2026, despite projected growth of 1,200 workers over the period***. *Demand for cyber security workers will increase to 51,100 workers by 2026. However, based on projected inflows and outflows from the cyber security workforce, by 2026 there will be a shortage of 3,000 workers. Only 48,100 of the demanded roles will be filled."*[15]

We recommend that, in addition to 'freshly' training a (graduate) workforce with the requisite skills for cyber security, it will be also useful to consider whether the existing workforce could be re-trained – and, if so, which specific parts – to fill the skills gap. Such training and re-training of workers becomes even more relevant with an increasing prevalence of artificial intelligence and the potential for it to reduce, or even eliminate, the need for certain parts of the workforce, necessitating that affected workers be equipped with new and/or additional skills to remain relevant and employable.

For example, research found that professions that typically require numerical and pattern recognition, such as accounting, and strong governance-related roles are closely aligned to the skill set required for many roles in the cyber security arena. At the same time, one could argue that accounting roles may soon at least partly be replaced by AI.

The above argument of training and re-training can equally be made in relation to the granting of visas for the purpose of skilled immigration, i.e., fast-tracking visa applications could be considered with a view to enhancing the workforce to meet Australia's demand for cyber security skills. We, therefore, recommend that Government should reconsider its decision to remove 'ICT security specialists' from the skilled visa processing priorities list, previously known as the Priority Migration Skilled Occupation List (PMSOL It is important that re-skilling Australia it would be beneficial to explore the potential of including international talent in cyber security workforce. Members also report that another area of concern is the difficulty of employing sufficiently security-cleared staff, or to obtain such clearances within appropriate timeframes. Members report that clearing timeframes with the Australian Government Security Vetting Agency (AGSVA) often exceed six months. Such timeframes render business processes for most of our members difficult, if not sometimes impossible, to handle.

Therefore, we welcome the decision to move responsibility for Top-Secret level security clearances over to the Australian Intelligence and Security Organisation (ASIO). However, we urge Government to also adequately resource the ASIO without loss of resources to AGSVA to approve applications by both organisations so that the desired shorter clearance timeframes will eventuate.

We also suggest a process that would, in appropriate circumstances, fast-track a clearance request.

10. Post-incident response

Question 13

> *"How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?"*
>
> No comment.

Question 13a:

> *Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?*

[15] AustCyber, Australia's Cyber Security Sector Competitiveness Plan 2022, as accessed at https://www.austcyber.com/resources/scp-2022/chapter-2 on 14 April 2023

Principally, we support considerations in relation to creating one point of entry for reporting incidents. However, the discussions and logic of the argument ought to be much broader than the above question suggests.

While it is desirable to have a single reporting portal for cyber incidents, other forms of incident reporting also ought to be eligible for the single-entry portal. A single portal ought to include reporting capability for not only cyber incidents, but also eligible data breaches and any other State and/or Federal reporting obligations for all sectors.

Moreover, any discussions in relation to harmonisation of existing requirements in relation to cyber incidents to different regulators also ought to target a simplification and reduction in reporting requirements, trigger points, harmonisation of timelines for reporting, data requirements etc. The below figure provides an indication of some of the current reporting requirements.

CPS 230 – op risk incident	CPS 234 – info security incident	CSP 234 – security control weakness	SOCI – critical incidents	SOCI – other incidents	Privacy Act – eligible data breach	ASX Rules – continuous disclosure
Operational risk incident that is determined to be **likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations**.	An **information security incident** that: a) materially affected, 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.	Material information security control weakness which the entity expects it will not be able to remediate in a timely manner.	**Critical** cyber incidents: a) a cyber security incident has occurred or is occurring; and b) the incident has had, or is having, a **significant** impact on the **availability of the asset**...	Other cyber incidents: a) a cyber security incident has occurred, is occurring **or is imminent**, and b) the incident has had, is having, or is likely to have, **a relevant impact on the asset**. • An incident will be considered to have a "relevant impact" if it impacts on the availability, integrity, reliability or confidentiality of the asset.	'Eligible data beach': a) unauthorised access or disclosure of personal information, or loss of personal information; and b) reasonably likely to result in serious harm to any of the individuals to whom the information relates.	Once an entity becomes aware of **any information** concerning it that a reasonable person would expect to have a **material effect on the price or value of the entity's securities**, it must tell ASX that information.
72 hours	72 hours	10 business days	12 hours (oral report) 84 hours (written report)	72 hours (oral) 48 hours (written report)	As soon as practicable from awareness 30 day-assessment period from suspicion	Immediately

Figure 1 – Current Cyber Incident Reporting Requirements

Gilbert and Tobin, as accessed at: https://www.lexology.com/library/detail.aspx?g=6b2f9aa5-e5c1-4f5e-a067-72c0e8b73286 on 13 April 2023

A simplification of requirements and a reduction of reporting points would allow affected entities to focus valuable resources on security-enhancing activities rather than compliance-related activities.

The Productivity Commission provided similar commentary in their recent Inquiry Report noting that:

> *"The numerous requirements can complicate compliance for businesses, particularly those operating in multiple states.*
>
> *The proliferation of reporting requirements and the need to report to different agencies could place unnecessary burdens on businesses at an already challenging time, when they are focusing on recovering from the security breach. A more unified approach to reporting requirements would assist — the Australian Institute of Company Directors (sub. 44, p. 8) notes that 'the example of cyber incident reporting… reflects a tendency for governments and individual regulators to "go it alone" to respond to an emerging risk. … Without coordination across government, organisations and boards risk being swamped by complex, inconsistent and duplicative obligations'. The Australian Information Industry Association has also observed that disparate but overlapping cyber security reporting regimes place unnecessary red tape burdens on regulated companies (Smith 2022). The Insurance*

> *Council of Australia noted that overlapping cyber incident reporting requirements from the ACSC and APRA are 'compounding resource pressures for insurers, in a historically tight market' (ICA, sub. 203, p. 5)."*[16]

In the context of reporting, we would like to stimulate discussion in relation to enhancing the functionality of the Document Verification System (DVS) to act as a central depository or 'single point of truth' with respect to information for compromised identity documentation. Once an identity document has been compromised, this ought to be flagged within the DVS so that any further verification against this document is not possible or, at least, raises awareness that further investigation may be required.

We also welcome steps to advance a consistent national approach to greater use of digital identity documents by Australians and will continue to engage with Government and all relevant stakeholders on processes that are designed to further develop and refine existing efforts.

Question 14:

> *"What would an effective post-incident review and consequence management model with industry involve?"*

We note that the Office of the Information Commissioner is currently reviewing some of the recent data breaches and will provide a report with insights in due course.

Without prejudice to the findings of the report, we believe that the following merits consideration:

- Organisations that experience a cyber incident must be enabled to place all immediate focus on incident management and law enforcement responses. Compliance management and regulatory investigations ought to follow as appropriate once resources are no longer required to deal with the immediate incident management;
- Regulatory investigations should be better coordinated and not duplicate information requests. (Also refer to our commentary in relation to a single reporting portal and reduced/simplified reporting obligations at Question 13a);
- Governments' (Federal and State) incident response architectures ought to be highly adaptive and flexible; and
- Industry would benefit from clear guidance and best practice examples of incidence management to better inform internal preparations and processes.

We recommend that a post-incident review and consequence management model could be structured based on, and take guidance and inspiration from, the US Cyber Safety Review Board (CSRB). This would ensure that both an effective post-incident review is undertaken, and a consequence management model is implemented. We suggest that if a similar CSRB model is implemented in Australia it would sit under the Office of Cyber Security within the Department of Home Affairs.

11. Improvement of best practice to protect victims / ecosystem / future-proofing etc.

Question 15:

> *"How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?"*

[16] Vol. 4, pp. 81, Productivity Commission, *5-year Productivity Inquiry: Advancing Prosperity*, Feb 2023

We support the effort to help promote data security awareness and/or resources amongst all organisations, particularly small and medium enterprises (SMEs) that may not have the resources to devote to data security. We note that a better general understanding of data risk and governance might, in many organisations, initially yield greater returns in terms of managing risks associated with data. In order to be able to adequately address data security, organisations must have an understanding of data governance (i.e., the architecture, compliance requirements, processes, technologies and of data management techniques that surround the data) before they can apply detailed data security technologies and policies.

Importantly, SMEs will see greatest benefits with an improved security-by-design approach to product and service development. These businesses typically do not have the resources or capabilities to engage deeply with cyber security issues and, consequently, will be best served with solutions that incorporate security considerations into their architecture.

Question 15a:

What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

No comment.

Question 16:

"What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?"

No comment.

Question 17:

"How should we approach future proofing for cyber security technologies out to 2030?"

No comment.

Question 18:

"Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?"

No comment.

Question 19:

"How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?"

As previously highlighted, supporting security-by-design initiatives will be critical to lifting Australia's overall cyber security posture. This also includes the promotion of end-user trust in the security of devices, including and especially in the many IoT-related devices that end-users increasingly incorporate in their daily lives.

As one example of such an initiative we commend the completely Australian-developed IoT/OT Security Trust Mark™ Certification and Cybersecurity Labelling Scheme (CLS) to Government for support through the Department of Home Affairs. Producing measurable outcomes based on globally recognised standards and best practice, as done by the Trust

Mark™ Certification and CLS, will be critical to the success of such initiatives. (For further information, refer to http://www.iotsecuritytrustmark.org.)

More generally, to 'future-proof' the Strategy, it should adopt risk- and principles-based approaches to regulatory measures and policies, to avoid unnecessary and prescriptive requirements that may be tied to specific technologies, or the state of technology at the time those measures and policies are developed.

12. Evaluation and assessment

Question 20:

> *"How should government measure its impact in uplifting national cyber resilience?"*
>
> No comment.

Question 21:

> *"What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?"*

Irrespective of the details of the final Strategy, we encourage Government to give sufficient consideration to devising clear accountability and success measurement structures that require all relevant Departments and Government agencies to report against clearly stated objectives and outcomes (i.e., the Strategy ought to formulate those) in a timely and public manner.

We note that the Strategy horizon is set at 8 years (2023 to 2030) – a rather long timeframe in a very dynamic and fast-paced environment. It will, therefore, be key to create milestones and associate clearly measurable goals with such milestones in order to determine the success (or otherwise) of the Strategy and, if required, correct course.

13. Conclusion

Communications Alliance and our members look forward to continued engagement with the Department and other relevant stakeholders on developing the Strategy. Communications Alliance supports the Department of Home Affairs Cyber Security Strategy and believe harmonisation of standards and regulations create the biggest opportunities for government to achieve these outcomes provided these policy objectives do not create further complex legislation for industry to digest. We welcome any opportunity to engage further on the Strategy development to ensure effective uptake of any initiatives.

We share Government's desire to create a robust, effective and efficient cyber-security framework that appropriately allocates responsibilities across all actors involved, and that enables all Australians to adequately protect themselves against the risks that come with it while enjoying the enormous benefits that it affords to all of us.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E
info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507