19 April 2023

BSA COMMENTS ON THE 2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY DISCUSSION PAPER

Submitted Electronically to the Department of Home Affairs

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the Department of Home Affairs (**DHA**) and the Expert Advisory Board on the 2023-2030 Australian Cyber Security Strategy Discussion Paper (**Discussion Paper**).[2]

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Our members have made significant investments in Australia, and we are proud that many Australian companies and organisations continue to rely on our members' products and services to do business and support Australia's economy.

We welcome the Australian Government's efforts to develop the 2023-2030 Australian Cyber Security Strategy (**Strategy**). While the growth of the Internet, the proliferation of connected devices, and the explosion in cloud-enabled processing capabilities have given rise to new opportunities, the rise of ever-evolving cybersecurity threats, such as large-scale data theft, privacy violations, phishing scams, ransomware, and malicious information operations can result in devastating consequences. As the Discussion Paper notes, uplifting cyber resilience and security to meet these threats must be "an integrated whole of nation endeavour", requiring "coordinated and concerted effort by governments, individuals and businesses of all sizes".[3]

Summary of BSA's Recommendations

BSA proffers the following recommendations in hopes that they will aid the development of a robust and progressive Strategy. They are divided into three categories.

Enhance regulatory coherence

1. Conduct a comprehensive assessment of existing cybersecurity laws and policies to identify and eliminate overlaps and inconsistences and legislate only for identified gaps.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] 2023-2030 Australian Cyber Security Strategy Discussion Paper, February 2023, https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf.

[3] Discussion Paper (2023), p. 7.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

2. Allow relevant ongoing reviews and consultations to run their course before proposing new laws or policies.
3. Vest the Coordinator for Cyber Security and National Office for Cyber Security with the necessary powers to oversee, direct, and harmonise all cybersecurity policies.
4. Include a "harmonisation impact statement" in consultation documents.

Engage with international partners

5. Enshrine key cybersecurity principles and build collaboration mechanisms in international agreements.
6. Refrain from imposing data localisation requirements and data transfer restrictions.
7. Align policies with internationally recognised cybersecurity and data protection standards.

Build robust domestic cybersecurity policies

8. Policies should be risk-based, outcome-focused, and technology-neutral.
9. Rely on market-driven mechanisms where possible.
10. Uphold privacy considerations.
11. Policies should be flexible and adaptable to encourage innovation.
12. Strengthen public-private partnerships.
13. Invest in citizen awareness and workforce development
14. Incorporate appropriate checks and balances.

Enhance regulatory coherence

1. Conduct a comprehensive assessment of existing cybersecurity policies to identify and eliminate regulatory overlaps and inconsistencies and legislate only for identified gaps

The Discussion Paper notes that "[t]here are a range of implicit cybersecurity obligations placed on Australian businesses and non-government entities, including through the corporations, consumer, critical infrastructure, and privacy legislative and regulatory frameworks", leading to cybersecurity obligations which are neither clear nor easy to comply with.[4]

BSA agrees with this observation. There has been a proliferation of cybersecurity laws, policies, and initiatives in recent years. However, due to the increasingly interlinked nature of digital and data related issues, this proliferation has created significant regulatory overlaps in Australia's technology regulatory landscape. For example, while there is currently no universal requirement for Australian businesses to report cybersecurity incidents, there are several mandatory reporting obligations for specific types of businesses that are spread across multiple pieces of legislation.[5] These overlaps

[4] Discussion Paper (2023), p. 17.

[5] Examples of prevailing reporting requirements include:

a) Under the Security of Critical Infrastructure Act 2018, and subsequent amendments, critical infrastructure asset owners and operators must report critical incidents (with a "significant impact" on their asset) within 12 hours of becoming aware of the incident, and other security incidents (with a "relevant impact" on their asset) within 72 hours.

b) The Privacy Amendment (Notifiable Data Breaches) Act 2017 amended the Privacy Act 1988 to require organisations to "notify affected individuals and the [Office of the Australian Information Commissioner] when a data breach is likely to result in serious harm to an individual whose personal information is involved". The scheme applies to all organisations covered by the Privacy Act, which includes Australian Government agencies and businesses with annual turnover of more than $3 million AUD. The Attorney General's Office is currently undertaking a substantial review of the Privacy Act.

c) In the financial services sector, the Prudential Standard CPS 234 on Information Security requires entities regulated by the Australian Prudential Regulation Authority (**APRA**) — including banks, insurers, and superannuation funds — to notify the regulator of material information security incidents within 72 hours. Entities must also notify APRA of material information security control weaknesses within 10 business days.

have resulted in unnecessary complexity in the overall cybersecurity regime, making it difficult for businesses of all sizes to understand and meet their compliance obligations. Streamlining and simplifying Australia's cybersecurity regime will improve understanding and compliance with the regime and will boost overall confidence in Australia's business operating environment.

As a starting point, DHA and the Expert Advisory Board should conduct a comprehensive assessment of all existing laws and policies related to cybersecurity or cyber incident reporting/response. These include the following:

- Security of Critical Infrastructure Act 2018 (**SOCI Act**)
- Hosting Certification Framework (**HCF**)
- Protective Security Policy Framework (**PSPF**)
- Information Security Manual (**ISM**)
- Information Security Registered Assessors Program (**IRAP**)
- Cloud Security Controls Matrix (**CSCM**)
- State-specific security frameworks, such as the New South Wales (**NSW**) Cyber Security Policy and the Queensland (**QLD**) Government Information Security Policy
- Privacy Act 1988

This assessment should include, among other issues, a review of the various objectives behind the individual laws and policies, an impact analysis of the costs of complying with them, the risks they seek to address, and whether they remain fit for purpose. Importantly, this exercise will be crucial for identifying and eliminating overlaps, as well as any gaps, in Australia's complex cybersecurity ecosystem.

One example of such an overlap is the expansion of the HCF to cover Software-as-a-Service (**SaaS**) providers. The HCF was originally conceived to address supply chain and foreign ownership risks presented by data hosting providers.[6] However, this expansion adds an unnecessary layer of certification on top of existing guidelines and mechanisms, which are already fit for purpose. For example, assessors certified under the IRAP can provide security assessments of cloud services and information technology (**IT**) systems. To assist with the assessment of cloud services, the CSCM can be used by IRAP assessors to capture the implementation of security controls. Furthermore, following the recent amendments to the SOCI Act, owners, and operators of critical infrastructure assets, including data storage/processing assets, are required to provide owner and operator information to the Register of Critical Infrastructure Assets and to notify the Australian Government whenever cybersecurity incidents occur. They are also required to adopt and maintain a risk management program to identify hazards that present a material risk to the availability of their critical infrastructure assets, and to proactively minimise or eliminate the risk of such hazards occurring. With these laws and policies in place, the application of HCF to SaaS providers further complicates the already complex compliance landscape for cybersecurity.

Beyond identifying overlaps, the assessment will assist in determining if a new Cyber Security Act is viable, or whether it is sufficient simply to remove overlapping requirements. The assessment will also assist in determining if any of the perceived gaps in the current regime have already been addressed through other legislation or whether there are indeed gaps that need to be addressed through a new Cyber Security Act. To the extent that such a Cyber Security Act will "draw together cyber-specific legislative obligations and standards across industry and government"[7] and addresses only actual gaps in the cybersecurity regime, BSA supports creating a new Cyber Security Act or framework. In the meantime, DHA and the

[6] Release of the Hosting Certification Framework, March 2021, https://www.dta.gov.au/news/release-hosting-certification-framework.

[7] Discussion Paper (2023), p. 17.

Expert Advisory Board should also publish the assessment, which can serve as guidance material for the industry on their cybersecurity obligations and will provide a clearer picture of the overall costs imposed on businesses by multiple regulations.

2. Allow relevant ongoing reviews and consultations to run their course before proposing additional changes

The Discussion Paper noted that "[t]here are a range of other important Government priorities which will significantly enhance Australia's digital security, and which will progress in parallel with the Strategy".[8] Indeed, there are various initiatives and efforts that seek to address issues such as data privacy and consumer data protection, most notably the ongoing Review of the Privacy Act 1988 (**Privacy Act Review**).

The Discussion Paper sought feedback on whether "further developments to the SOCI Act are warranted, such as including customer data and "systems" in the definition of critical assets".[9] However, the Privacy Act Review will also deal with issues relating to the protection of customer data. The Attorney-General's Department's (**AGD**) Privacy Act Review Report 2022 (**Privacy Act Review Report**)[10] contained various proposals designed to give individuals more transparency and control over how their personal information is handled and impose greater obligations on businesses to protect personal information, including minimising the amount of personal information businesses collect and retain.

To avoid duplicating efforts and further complicating the legal landscape, BSA recommends that DHA and the Expert Advisory Board allow ongoing reviews and consultations related to cybersecurity, such as the Privacy Act Review, to run their course before proposing or introducing additional legislative changes, such as a new Cyber Security Act or an amendment of the SOCI Act. Relatedly, if a new, consolidated Cyber Security Act is to be enacted, we recommend *not* amending the SOCI Act, thus allowing it to be superseded by the new Cyber Security Act.

3. Vest the Coordinator for Cyber Security and National Office for Cyber Security with necessary powers to oversee and direct all cyber security policies

Due to the proliferation of piecemeal cyber-specific policies, multiple Government agencies — including DHA, the AGD, Digital Transformation Agency, and the Office of the National Data Commissioner — oversee different legal and policy initiatives related to cyber security.

BSA notes the Government's recent announcement that it will "will establish a Coordinator for Cyber Security, supported by a National Office for Cyber Security within the Department of Home Affairs, to ensure a centrally coordinated approach to deliver Government's cybersecurity responsibilities".[11] We applaud the Government's commitment to strengthen coordination and harmonisation among the different agencies, and ensure consistency and coherence across various cybersecurity laws and policies. However, the precise remit and responsibilities of the Coordinator for Cyber Security (**Coordinator**) and the National Office for Cyber Security (**Cyber Security Office**) are not yet clear or disclosed.

---

[8] Discussion Paper (2023), p. 14.

[9] Discussion Paper (2023), p. 17.

[10] Privacy Act Review Report 2022, February 2023, https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf (Report 2022).

[11] Prime Minister's Cyber Security Roundtable Media Release, February 2023, https://www.pm.gov.au/media/prime-ministers-cyber-security-roundtable

In this regard, the Coordinator and Cyber Security Office should be granted powers to oversee and direct the cybersecurity policies of *all* Government agencies. For example, all government agencies should be required to seek the endorsement of the Coordinator before implementing any new cybersecurity policies or adjusting existing ones, thereby reducing instances of agencies imposing obligations without regard or consideration for the wider cybersecurity landscape. In addition, the Coordinator and Cyber Security Office should be responsible for maintaining a single reporting portal for all cyber incidents and harmonising existing and new requirements to report separately to multiple regulators.

4. Include a "harmonisation impact statement" in consultation documents

As structural changes will take significant time to implement, BSA suggests that, in the meantime, agencies include a "harmonisation impact statement" in cybersecurity consultation documents. Similar to a regulatory impact statement, a harmonisation impact statement should list the government agencies that have been engaged in internal consultations and their perspectives, as well as the implications of any policy overlaps, if any. It should also take into consideration relevant State-based laws and policies, especially when the consultation relates to proposing new national policies. While this may lengthen the consultation process, this would compel agencies to harmonise their positions internally before proceeding with public consultations. It would ultimately result in better laws and policies that do not divert resources to compliance functions but instead incentivise better security.

Engage with international partners

5. Enshrine key cybersecurity principles and build collaboration mechanisms in international agreements

Digital Economy Agreements (DEAs) and international agreements with digital trade chapters provide opportunities for Australia to enshrine key cybersecurity principles and build collaboration mechanisms with international partners.

The Digital Trade Chapter in the Australia-United Kingdom Free Trade Agreement (**AUKFTA**) contains a detailed Article on cybersecurity.[12] Article 14.20 calls on parties to build the capabilities of their respective national entities responsible for cybersecurity incident response, strengthen existing collaboration mechanisms to identify and mitigate cyber threats, and to maintain a dialogue on cybersecurity issues. Notably, Article 14.20 also recognises that, given the evolving nature of cybersecurity threats, risk-based approaches may be more effective than prescriptive laws. To that end, both Australia and the UK will endeavour to employ, and encourage enterprises within their jurisdictions to use, risk-based approaches that rely on open and transparent cybersecurity standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

The ongoing negotiations at the Indo-Pacific Economic Framework (IPEF) is a good opportunity for Australia to further exhibit thought leadership on cybersecurity. We urge Australia to enshrine the same forward-leaning language used in the AUKFTA's Article 14.20 in the IPEF's digital trade text. There is also potential for Australia to push for more ambitious language. For example, given that cybersecurity certification requirements and other measures may increase risk when they contain elements that impair cross-border coordination or access to cybersecurity technologies, Australia and its international partners can commit to ensuring that governments embrace and engage in the development and adoption of internationally recognised

[12] Australia-United Kingdom Free Trade Agreement, https://www.dfat.gov.au/trade/agreements/not-yet-in-force/aukfta/official-text.

standards rather than adopting domestic standards that could result in unintended trade barriers. (Please also see our comments in section 7 below on aligning policies with internationally recognised security standards.)

6. Refrain from imposing data localisation requirements and data transfer restrictions

A growing trend of data localisation requirements presents serious challenges for business of all kinds. Governments often impose these requirements under the belief that storing data within a country's borders would enhance cybersecurity. **However, the security of data does not depend on where it is stored. In fact, requiring businesses to localise their computing facilities and data can actually undermine security by increasing risks and decreasing resilience.** This can happen when localisation measures compel businesses to use local data storage providers, which limits options for businesses deciding which entities they will entrust their data to and mechanisms for ensuring redundancy and resiliency of the data.

For example, under localisation measures, companies may be unable to use their business's own globally centralised data storage centers that may be situated in other countries, nor use service providers without data centres in-country. However, local data storage service providers may not have the same security capabilities as global counterparts, which benefit from collecting data worldwide about real-time threats and comparing malicious actors across regions and customers, which helps detect and prevent potential cyber threats. Fragmented cybersecurity systems could also expose customers in a region that relies on localised networks to new threats from other parts of the world, reducing information privacy and security for those customers. Further, requiring data to stay within a country does not allow for a company to create backups that will not be susceptible to physical or natural disaster related risks, thus adversely impacting resiliency.

Localisation measures are not necessary for regulatory oversight, even in heavily regulated sectors such as the financial services sector. As a general principle, there is no reason to impose localisation requirements on businesses if regulatory authorities have immediate and ongoing access to data.

In this regard, we also note that Australia's Digital Trade Strategy[13] expressly acknowledges the importance of facilitating cross-border data transfers and prohibiting data localisation requirements. As the Digital Trade Strategy notes, "[u]nnecessary restriction on the flow of data, or requirements to store data locally raises costs for businesses and significantly reduces efficiencies, impacts the ability to make decisions on business development, marketing, innovation and development of comparative advantage, and makes it difficult for businesses to enter new markets".[14] We are also fully supportive of the approaches taken in Australia's DEA with Singapore and the AUKFTA, both of which set out binding rules prohibiting unwarranted restrictions on cross-border data transfers and requirements to localise computing facilities. **BSA urges DHA and the Expert Advisory Board to keep these policy positions in mind when assessing whether localisation is necessary in the context of cybersecurity.**

7. Align policies with internationally recognised cybersecurity and data protection standards

Internationally recognised technical standards provide widely vetted, consensus-based frameworks for defining and implementing effective approaches to cybersecurity, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability. Alignment with internationally recognised technical standards and guidance, such as the International Organization for Standardization (**ISO**)/International Electrotechnical Commission (**IEC**) 27001 Standards, which

[13] Digital Trade Strategy, April 2022, https://www.dfat.gov.au/sites/default/files/digital-trade-strategy.pdf.

[14] Digital Trade Strategy (2022), p. 10.

provide requirements for an information security management system, can ensure that Australia benefits from proven approaches to cybersecurity and is even better-positioned to cooperate inter-operably with the international community in confronting transnational threats, especially with respect to essential services systems protection.

Interoperability is a particular concern in important areas like Internet of Things technologies and cloud computing services. BSA again strongly urges the Australian government to embrace multilateral, interoperable initiatives to address security in these areas rather than to seek to develop national standards that could duplicate and potentially conflict with existing efforts. Where there are gaps in internationally recognised technical standards, **BSA calls upon the Australian government to work with other government and industry partners to address those gaps, building a basis for policies that can improve cybersecurity consistently and cooperatively across different markets.**

Relatedly, the Strategy should also establish mechanisms to give companies more opportunities to demonstrate their security measures and processes by showing compliance with other certification mechanisms based on equivalent internationally recognised standards (e.g., US FedRAMP[15]). The focus of Australian cloud security certification processes should be to identify and address gaps between such certifications and Australian requirements, especially where there are significant overlaps between the Australian requirements and internationally recognised standards, and mitigate any resultant residual risks.[16] This will significantly reduce the complexity, cost, resourcing, and timeframes for assessing cloud services and other IT systems.

Build robust domestic cybersecurity policies

8. Policies should be risk-based, outcome-focused and technology-neutral

Malicious cyber activity carries different risks for different systems and types of data. There are generally multiple approaches to defending against the same type of cyber-attack, and multiple approaches to improving cybersecurity and resiliency. The Strategy should prioritise approaches and policies that address different levels of risk and enable owners and operators of networks and systems to defend their data with the technologies and approaches that are best to meet priorities and the level of security required.

9. Rely on market-driven mechanisms where possible

Information technology is constantly evolving, and cybersecurity threats evolve with it. Neither technologies nor threats are bound by national borders, meaning that overreliance on national government structures or regulatory enforcement is unlikely to achieve desired results with threats beyond borders. Policies that leverage market forces to drive cybersecurity will be most successful in keeping pace with the changing technology and security environment.

10. Uphold privacy considerations

Given the importance of personal and sensitive information, cybersecurity policies should be carefully attuned to privacy considerations.

---

[15] The US's Federal Risk and Authorization Management Program (**FedRAMP**) provides a standardised approach to security authorisations for cloud service offerings. See: https://www.fedramp.gov/.

[16] For example, the risk management framework used by Australia's ISM draws from the National Institute of Standards and Technology (**NIST**) Special Publication (SP) 800-37 Rev. 2, which is also used by FedRAMP. As such there are significant overlaps between the ISM and FedRAMP. See the Australia Information Manual (updated March 2023), p.2, https://www.cyber.gov.au/sites/default/files/2023-03/Information%20Security%20Manual%20-%20%28March%202023%29.pdf.

In this regard, BSA supports many of the AGD's proposals in the Privacy Act Review Report,[17] particularly the proposal to implement a clear distinction between the roles and obligations of entities that decide how and why to collect personal information (controllers) and those that process personal information on behalf of other entities (processors).[18] This approach creates laws that better protect privacy and cybersecurity, because it creates clarity for individuals about the obligations of different companies that handle their information and helps them identify which entity to contact to exercise their rights under the Privacy Act. Assigning distinct obligations to both controllers and processors will also help to ensure that individuals do not receive duplicative consent requests from different entities, where a controller and a processor may both be inadvertently required to seek consent for the same processing activities. Indeed, in many cases, failing to distinguish between these different types of companies can confuse consumers and, more importantly, create cybersecurity risks and undermine consumer privacy.

Alignment would also substantially streamline obligations for Australian entities required to comply with the privacy laws of other jurisdictions, which facilitates compliance while also enhancing participation in the global digital economy.

11. Policies should be flexible and adaptable to encourage innovation

Information technology and the millions of jobs technology supports depend on the ability to innovate new solutions. Likewise, policy approaches to cybersecurity require constant innovation to keep pace with changing threats. Policies must be adaptable to enable businesses to develop new approaches to new challenges and to deliver innovative products to the customers that depend on them.

12. Strengthen public-private partnerships

Cybersecurity is a shared responsibility across government and private stakeholders. Although governments often hold critical security tools and information, the private sector owns and operates significant elements of the critical infrastructure and the technology platforms that are targeted by malicious cyber activity, as well as many of the cybersecurity tools and services necessary to defend against such threats. Only by working in close collaboration with the private sector can governments truly combat cybersecurity threats while sustaining the vitality of the digital economy. Relatedly, under the shared responsibility model, security is also a shared responsibility between the end user and the service provider – while the service provider is responsible for monitoring and responding to security threats related to the service itself and its underlying infrastructure, end users, including individuals and companies, are responsible for protecting data and other assets they store in any cloud environment.

In this respect, BSA would like to commend DHA and the Cyber and Infrastructure Security Centre (**CISC**) on the collaborative approach taken when seeking stakeholder inputs on amending the SOCI Act. The several townhalls organised by DHA and CISC on specific measures proposed in the amendments were helpful platforms for business and industry to provide immediate feedback and field questions. CISC also provided factsheets on many key issues and obligations, such as the Register of Critical Infrastructure Assets, Cyber Incident Response Government Assistance Measures, and Cyber Security Incident Reporting.[19]

Another recent initiative by the DHA — the Trusted Information Sharing Network (**TISN**) — serves as a positive example of an effective and innovative public-private partnership mechanism. The TISN

---

[17] Privacy Act Review Report 2022, February 2023, https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf (Report 2023).

[18] Report (2023), Proposal 22.1.

[19] See: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018

provides a platform for critical infrastructure owners and operators to share information on threats and vulnerabilities and collaborate on appropriate measures to mitigate risk and boost resilience. The TISN comprises representatives from different critical infrastructure sectors, and each sector is supported by an Australian Government agency — usually the agency that has regulatory responsibility for that sector. Under the TISN Data Sector Group, data storage and processing service providers, which include cloud service providers, work together with government agencies to: (a) identify and manage risks to critical infrastructure; (b) address security gaps within sectors and implement mitigation strategies; (c) inform future policy and programs to further support critical infrastructure resilience; and (d) achieve the objectives of the Critical Infrastructure Resilience Strategy.[20]

The DHA and Expert Advisory Board should leverage on these collaborative mechanisms to enhance trust and facilitate communication between the public and private sectors, ultimately building an ecosystem that is more resilient and responsive to cyber threats.

13. Invest in citizen awareness and workforce development

In addition to strengthening public-private partnerships, the DHA and Expert Advisory Board should also invest in increasing public awareness that citizens also play an outsized role in cybersecurity. In this regard, it should be noted that vast majority of cyber breaches and attacks are attributable to poor individual cyber hygiene. There are many ways governments can invest in public awareness; successful efforts have included national awareness events (such as dedicating a national cybersecurity awareness week or month), public service advertising campaigns, dedicated websites and online guidance, social media campaigns, and school events. Another important way the government can promote cybersecurity awareness is by making available aggregate and publicly disclosed data about cybersecurity incidents to enable researchers, policymakers, and average citizens better understand the scope and contours of cybersecurity challenges. These efforts should be supplemented by adopting measures at the organisational level to mitigate personnel risks. One example is to implement access controls – both physical and digital – so that only authorised individuals can access critical assets.

Entrenching cybersecurity awareness among citizens begins with ensuring that cybersecurity education at every level of the education system is available, accessible, and aligned to emerging cybersecurity challenges. Through such education efforts, the government can also build a cybersecurity workforce to meet the current and future needs of Australia. In this regard, the DHA and the Expert Advisory Board should also consider programs to:

- Expose young people to cybersecurity concepts, including basic cyber hygiene, through primary school curricula;
- Increase interest in and access to cybersecurity education among youth through scholarships and research competitions; and
- Incentivize the development, accreditation, and promotion of cybersecurity-focused education programs through universities, community colleges, and other educational venues.

14. Incorporate appropriate checks and balances

The Government is vested with significant powers to uphold cybersecurity. However, policies that introduce intrusive powers, even for the purposes of upholding cybersecurity, can compromise user confidence in the integrity and trustworthiness of a service provider's products and services, and should therefore be subject to appropriate checks and balances, such as independent authorisation and reviews on the exercise of such intrusive powers. One possible check is the implementation of a

[20] Trusted Information Sharing Network – Overview, accessed February 2023, https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/tisn-overview.pdf.

mandatory review process through which panel of independent technical experts assesses the security, technical feasibility, and reasonableness of exercising said powers.

Conclusion

We hope that our comments will assist DHA and the Expert Advisory Panel as it moves forward with the Cyber Security Strategy. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

[redacted]

Tham Shen Hong
Manager, Policy – APAC