6 June 2022

BSA COMMENTS ON AUSTRALIA'S NATIONAL DATA SECURITY ACTION PLAN

Submitted Electronically to the Department of Home Affairs

BSA **|** The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Department of Home Affairs (**DHA**) on its Discussion Paper regarding the development of Australia's National Data Security Action Plan (**Discussion Paper** and **Action Plan** respectively).[2]

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members create the technology products and services that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. These products and services require companies to entrust data to our members, and our members work hard to keep that trust. Our members have made significant investments in Australia, and we are proud that many Australian entities and consumers 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 an Action Plan that delivers "whole-of-economy expectations and requirements for data security".[3] Robust, consistent and clear obligations on data security will enhance the businesses' understanding of data risks, facilitate compliance and ultimately promote more responsible uses of data-driven technologies.

BSA has previously provided comments on data-related issues in the context of privacy, critical infrastructure and electronic surveillance,[4] and would like to proffer the following recommendations

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, 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] National Data Security Action Plan Discussion Paper, April 2022, https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf.

[3] Discussion Paper (2022), p. 7.

[4] See:

a) BSA Comments on Review of Australia Privacy Act 1988, January 2022, https://www.bsa.org/files/policy-filings/01212022aupriv1988.pdf;

b) BSA Comments on Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, January 2022, https://www.bsa.org/files/policy-filings/01312022slacip.pdf;

c) BSA Comments on Reform of Australia's Electronic Surveillance Framework, February 2022, https://www.bsa.org/files/policy-filings/02252022auesurveillancefrmk.pdf;

d) BSA Submission to the PJCIS Review of the Security Legislation Amendment (Critical Infrastructure Protection Bill) 2022, February 2022, https://www.bsa.org/policy-filings/australia-bsa-submission-to-the-pjcis-review-of-the-security-legislation-amendment-critical-infrastructure-protection-bill-2022;

under each of the data security pillars underpinning the Action Plan: **Secure, Accountable and Controlled**.[5]

Summary of BSA's Recommendations

- *First*: Align policies with internationally recognised data security standards;
- *Second*: Policies should be risk-based, outcome-focused, and technology-neutral;
- *Third*: Rely on market-driven mechanisms where possible;
- *Fourth*: Ensure that policies uphold privacy considerations;
- *Fifth*: Policies should be flexible and adaptable to encourage innovation;
- *Sixth*: Facilitate public-private collaboration;
- *Seventh*: Refrain from imposing data localisation requirements and data transfer restrictions;
- *Eighth*: Incorporate appropriate checks and balances;
- *Ninth*: Identify a single lead agency to strengthen inter-agency coordination and minimise regulatory overlaps;
- *Tenth*: Incorporate distinction between data controllers and data processors; and
- *Eleventh*: Recognise existing mechanisms governing cross-border data transfers.

Pillar 1: Secure

The goal of the Secure pillar is to "to set consistent and mandatory data security standards and communicate advice, expectations and requirements across the economy".[6] To achieve this goal, we recommend rooting the Secure Pillar in the following guiding principles,[7] which have been derived from BSA's experience working on data and cyber security issues with governments worldwide:

1. Alignment with internationally recognised data security standards

Internationally recognised technical standards provide widely vetted, consensus-based frameworks for defining and implementing effective approaches to data security, 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 provides requirements for an information security management system, can ensure that Australia benefits from proven approaches to data security 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 areas – such as security of Internet of Things technologies and cloud computing services – where gaps in internationally recognised technical standards have sparked the proliferation of different government- and industry-driven approaches. BSA 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,

[5] Discussion Paper (2022), p. 19.

[6] Discussion Paper (2022), p. 19.

[7] BSA International Cybersecurity Policy Framework, April 2018, https://www.bsa.org/reports/bsa-international-cybersecurity-framework.

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 security consistently and cooperatively across different markets.

2. 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 data security and resiliency. The Action Plan 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 they deem best to meet the level of security desired.

3. Rely on market-driven mechanisms where possible

Information technology is constantly evolving, and data security 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 are likely to be most successful in keeping pace with the changing technology and security environment.

4. Uphold privacy considerations

The Discussion Paper observed that "[p]rivacy settings ensure the protection and security of personal and sensitive information including from unauthorised access", whereas "[d]ata security seeks to address unauthorised access to all data types".[8] Consequently, the Discussion Paper noted that "privacy and data security combine to ensure the protection and security of data".[9] Given the importance of personal and sensitive information, data security policies should be carefully attuned to privacy considerations. Key considerations include ensuring civilian leadership and avoiding policies that undermine the use of privacy-enhancing technologies.

Relatedly, BSA strongly encourages Australia to align its privacy policies with leading global privacy laws, such as by incorporating the data controller/processor distinction in its review of the *Privacy Act 1988* (**Privacy Act**).[10] Alignment would 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.

5. 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, data security requires constant innovation to keep pace with changing threats. Policies must be flexible and adaptable to enable businesses to develop new approaches to new challenges and to deliver innovative products to the customers that depend on them.

6. Facilitate public-private collaboration

Data security is a shared responsibility across government and private stakeholders. Although governments often hold critical security tools and information, the private sector is responsible for significant elements of the critical infrastructure and the technology platforms that are targeted by

[8] Discussion Paper (2022), p. 2.

[9] Discussion Paper (2022), p. 2.

[10] This distinction is necessary in today's digital economy, where an individual may use a service from one consumer-facing entity, but that entity may rely on numerous other enterprise service providers to store, analyse, and process the data in connection with that service. Each entity that processes an individual's personal information should be subject to strong obligations to safeguard that information, but those obligations should vary according to the different roles these entities play. Other privacy regimes that have adopted this distinction include the European Union's General Data Protection Regulation, California's Consumer Privacy Act, Japan's Act on the Protection of Personal Information, and Singapore's Personal Data Protection Act.

malicious cyber activity, as well as many of the cyber security tools and services necessary to defend against such threats. Only by working in close collaboration with the private sector can governments truly combat cyber security threats while sustaining the vitality of the digital economy.

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 *Security of Critical Infrastructure Act 2018* (**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.[11] We also note that CISC, in collaboration with the relevant industries, will be developing further guidance material to support implementation of the critical infrastructure security reforms, which will include a legislative handbook on the Serious Cyber Security Response Measures (also known as government assistance measures) and a supporting playbook that steps through how the government assistance measures will work in practice.[12] Such guidance material are essential for helping businesses understand their obligations. BSA strongly recommends that DHA continues with this collaborative approach to policymaking and implementation.

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

A growing trend of data localisation requirements present serious challenges for business of all kinds. Governments often impose these requirements under the belief that the best way to protect data is to store it within a country's borders.

However, the security of data does not depend on where it is stored. Rather, data security is improved by adopting risk-based policies that ensure data remains protected regardless of its physical location. 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. For example, under localisation measures companies may be unable to use their business's own globally-centralised data storage center and unable to use service providers without data centers in country. But 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 identify 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.

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 their data.

In this regard, we are encouraged that Australia's Digital Trade Strategy[13] expressly acknowledges the importance of facilitating cross-border data transfers and prohibiting data localisation

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

[12] Department of Home Affairs submission into the Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, February 2022, https://www.aph.gov.au/DocumentStore.ashx?id=7725468b-8682-4573-b698-018c6dc4373c&subId=720229

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

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 approach taken in Australia's Digital Economy Agreement with Singapore, which sets out binding rules prohibiting unwarranted restrictions on cross-border data transfers and requirements to localise computing facilities. BSA urges DHA to keep these policy positions in mind when assessing whether localisation is necessary in the context of data security.

Pillar 2: Accountable

The goal of the Accountable Pillar is to ensure that custodians of data, which includes both the Government and commercial data centres, are "held accountable through clear and concise guidance, policy and legislative mechanisms".[15] BSA recognises that data should be securely stored, and that rigorous mechanisms are oftentimes necessary to ensure that a high standard of data security is maintained. However, it is equally important to make sure that such mechanisms do not take precedence over other key considerations, such as the right to privacy. In this regard, BSA proffers the following recommendations:

8. Incorporate appropriate checks and balances

The Government is vested with significant powers to uphold data and cyber security. However, policies that introduce intrusive powers, even for the purposes of upholding data security, 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 mandatory review process through which panel of independent technical experts assesses the security, technical feasibility, and reasonableness of exercising said powers.

9. Identify a single lead agency to strengthen inter-agency coordination and minimise regulatory overlaps

As noted in the Discussion Paper, multiple Government agencies – including DHA, the Attorney General's Department (**AGD**), Digital Transformation Agency, and the Office of National Data Commissioner – oversee different legislative and policy initiatives related to data security, which "creates a congested environment".[16] To mitigate this congestion, the Action Plan should consider identifying a single lead agency to oversee and direct the data security initiatives of *all* Government agencies. Designating a single lead agency will strengthen coordination between the different agencies and ensure consistency and coherence across all policy initiatives.

It is also vital for the lead agency to ensure that regulations/initiatives do not overlap and create unnecessary layers for businesses while also driving up costs. One example of such an overlap is the upcoming expansion of the Hosting Certification Framework (**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.[17] 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 Infosec Registered Assessor Program (**IRAP**) can provide security assessments of cloud services and ICT systems. To assist with the assessment of cloud services, the Cloud Security Controls Matrix (**CSCM**) can be used by IRAP assessors to capture the

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

[15] Discussion Paper (2022), p. 19.

[16] Discussion Paper (2022), p. 14.

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

implementation of security controls. The CSCM also provides indicative guidance on the scoping of cloud security assessments, and inheritance for systems under a shared responsibility model. With these guidelines and mechanisms already in place, the application of HCF to SaaS providers is unnecessary and might further complicate the regulatory and compliance landscape for data security.

Pillar 3: Controlled

The goal of the Controlled Pillar is to enhance and promote "mechanisms that allow individuals to control the use and collection of their data", including the ability to "freely remove, transfer and destroy the data".[18] To achieve this goal, individuals must be made aware of the responsibilities and obligations of key stakeholders in the data security ecosystem, so that they can effectively control the use and collection of their data. Given that the focus of this pillar is on the individual's control of their data, we proffer the following privacy-related recommendations for DHA's consideration:

10. Incorporate distinction between data controllers and data processors

At present, the Privacy Act does not expressly distinguish between controllers and processors; instead, it regulates all Australian Privacy Principles (**APP**) entities[19] and imposes on them a common set of obligations.

BSA strongly recommends that the Government implement a clear distinction between the roles and obligations of entities that decide how and why to collect personal information (**controllers**) and those that instead process personal information on behalf of other entities (**processors**). This approach creates laws that better protect privacy and data security, 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 data security risks and undermine consumer privacy.

11. Recognise existing mechanisms governing cross-border data transfers

BSA encourages the Government to recognise different data transfer mechanisms which can meet the requirements imposed by the Privacy Act and support the accountability model for international data transfers. These include the APEC/Global Cross-Border Privacy Rules (**CBPR**) and Privacy Rules for Processors (**PRP**),[20] as well as mutual recognition arrangements, such as adequacy with the European Union's General Data Protection Regulation (**GDPR**). Recognising these mechanisms would align Australia's international data transfer regime with global best practices and give entities the flexibility to determine which mechanisms will be better suited for each situation. These mechanisms are also incorporated in other data protection frameworks to promote cross-border data transfers.

We also urge the Government to refrain from creating new data transfer mechanisms solely for use by entities transferring data to and from Australia as such measures would not encourage the widespread use of interoperable mechanisms to facilitate responsible data transfers. For example, the AGD's Discussion Paper on the Privacy Act Review proposed introducing standard contractual

[18] Discussion Paper (2022), p. 19.

[19] Defined as agencies or organisations subject to the APP, per the Australian Privacy Principles Guidelines, Chapter B: Key Concepts, July 2019, https://www.oaic.gov.au/__data/assets/pdf_file/0003/1200/app-guidelines-chapter-b-v1.3.pdf.

[20] See http://cbprs.org/ and http://cbprs.org/business/.

clauses (**SCCs**) to regulate cross-border transfers of personal information.[21] However, if the proposed SCCs are not interoperable with other similar standard contractual clauses, they would impose operational and compliance challenges for entities operating in multiple jurisdictions. As such, BSA recommends that any new Australian-specific data transfer mechanisms should remain voluntary and be interoperable with other global schemes to help further industry participation and ensure meaningful protections for consumers.

Conclusion

We hope that our comments will assist the Government as it moves forward with the Action Plan. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong

Tham Shen Hong

Manager, Policy – APAC

[21] Discussion Paper, Review of the Privacy Act 1988, October 2021, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf, p. 161-162.