29 August 2025

BSA RESPONSE TO CYBER SECURITY STRATEGY "HORIZON 2" POLICY DISCUSSION PAPER

Submitted Electronically to the Department of Home Affairs (DHA)

The Business Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the DHA on its Policy Discussion Paper on Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy (**Discussion Paper** and **Strategy** respectively).[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, network infrastructure services, cybersecurity solutions, and collaboration systems. 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.

BSA recognises that cyber threats are growing in both frequency and sophistication. We support Australia's efforts to ensure that its cybersecurity laws and policies remain fit-for-purpose and capable of addressing ever-evolving cyber threats. Cybersecurity is a shared responsibility across public and private stakeholders and effective policymaking in this domain requires close coordination between the public and private sectors. We welcome the Australian Government's commitment to co-designing initiatives under Horizon 2 with industry partners.

Summary of BSA's Recommendations

1. Undertake a structured legislative harmonisation review to systematically identify and consolidate overlapping requirements and align definitions and thresholds across different laws.
2. Adopt a risk-based, context-driven framework for identifying and protecting valuable datasets developed in consultation with industry and aligned with internationally recognised standards.
3. Adopt a targeted, risk-based approach to the regulation of emerging technologies such as artificial intelligence (**AI**) to promote their safe and responsible use, strengthen cyber defences, and support innovation.
4. Adopt a clearly defined, government-led approach to active cyber defence.

[1] BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security, July 2025, https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/charting-new-horizons-horizon-2-policy-discussion-paper.pdf

5. Promote voluntary, confidential vulnerability disclosure practices aligned with internationally recognised standards.
6. Avoid imposing prescriptive sovereignty requirements and pursue a risk-based, standards-aligned approach that recognises providers from trusted jurisdictions.
7. Support greater international alignment of cyber security regulations, with a focus on harmonising cyber incident reporting requirements and pursuing mutual recognition of cloud security certifications.

Regulatory Harmonisation and Simplification

The Discussion Paper acknowledged that the existing cyber regulatory framework can be "complex and difficult to navigate", and that more work needs to be done to harmonise and simplify cyber regulations to promote best practices and efficiency.[3]

BSA agrees with this observation. Due to the increasingly interlinked nature of digital and data related issues, this cyber regulatory framework creates significant regulatory overlaps in Australia's technology regulatory landscape. For example, there are several mandatory reporting obligations for specific types of businesses that are spread across multiple pieces of legislation.[4] These overlaps 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. The single reporting portal introduced on cyber.gov.au is a welcome step toward streamlining incident notification processes. However, entities must still navigate distinct thresholds and timelines across different laws and regulations. Without greater harmonisation of the substantive obligations underpinning each reporting regime, businesses, especially those operating across multiple sectors, will continue to face a patchwork of overlapping and often duplicative requirements that drain resources away from actual cyber risk mitigation.

Apart from overlapping requirements, the number and variety of cybersecurity related laws and policies have created a complex regulatory landscape that is difficult for businesses to navigate. The Discussion Paper itself cited various obligations in the Security of Critical Infrastructure Act 2018 (**SOCI Act**), the Australia Privacy Principles (**APPs**) under the Privacy Act 1988 (**Privacy Act**), and the Prudential Standard CPS 234 on Information Security. These form just a small part of the existing corpus of laws and policies related to cybersecurity in Australia, which also include (but are not limited to) the following:

- Cyber Security Act 2024 (**Cyber Security Act**)

[3] Discussion Paper (2025), p. 17

[4] 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.

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.

- Hosting Certification Framework (**HCF**)
- Protective Security Policy Framework (**PSPF**)
- Information Security Manual (**ISM**)
- Information Security Registered Assessors Program (**IRAP**)
- Cloud Controls Matrix (**CCM**)
- State-specific security frameworks, such as the New South Wales (**NSW**) Cyber Security Policy and the Queensland (**QLD**) Government Information Security Policy

This large and complex regulatory framework means that businesses must invest significant resources in compliance mapping and administrative coordination, which not only detracts from actual cyber risk mitigation but also makes it harder for smaller entities to participate confidently in the digital economy. In this regard, the recently enacted Cyber Security Act also represents a missed opportunity, as it could have drawn together various cyber-specific legislative obligations and standards across industry and government into a unified, coherent framework that is simpler for businesses to understand and comply with. Instead, businesses have to cycle through multiple laws, regulations, and rules to grasp the full extent of their cybersecurity obligations.

Recommendation: The Government should **undertake a structured legislative harmonisation review to systematically identify and consolidate overlapping requirements and align definitions and thresholds across different laws**. The Government should also consider how the Cyber Security Act can be updated to serve as an overarching law or framework through which disparate cyber-related obligations and standards can be integrated and administered more cohesively.

Protecting Valuable Data Sets

BSA welcomes the Government's focus on improving the protection of valuable data sets, particularly as the volume, sensitivity, and strategic importance of data continue to grow in an increasingly digital economy. Cyber threats targeting data are evolving rapidly in sophistication, and data sets held by both the public and private sectors have become high-value targets for malicious actors.

Any framework for identifying and securing valuable datasets should be guided by risk. Datasets should not be classified as "valuable" (and therefore subject to more restrictions) based solely on volume or sector, as such an approach tends to oversimplify ways in which data may be sensitive or strategically important. For example, not all data held by entities operating within traditionally "critical" sectors, such as healthcare or finance, should automatically be deemed valuable or likely to cause significant harm if compromised; a substantial portion may be routine and non-sensitive. A more effective approach would involve a contextual assessment that considers factors such as the data's function, sensitivity, interdependence, role in supporting essential services, and potential consequences of compromise. This would enable more targeted and proportionate safeguards, while avoiding unnecessary compliance burdens or unintended restrictions on data-driven innovation.

It is also important to not conflate data security with data localisation. While enhancing the security of valuable data is a legitimate policy objective, measures that mandate data localisation or place blanket restrictions on cross-border data transfers risk undermining Australia's global digital competitiveness and access to best-in-class cybersecurity capabilities. Ultimately, 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 data can undermine cybersecurity by increasing risks and decreasing resilience. For example, under localisation measures, companies in Australia may be prevented from using trusted and leading cloud service providers (**CSPs**) and solutions simply because some of these CSPs do not own or use data centres in-country. Local data storage service providers may not have the same security capabilities as their global counterparts. Furthermore, global CSPs often benefit from collecting worldwide data about real-time threats and comparing malicious actors across regions and customers, which helps identify and prevent potential cyber attacks.

Recommendation: The Government should **adopt a risk-based, context-driven framework for identifying and protecting valuable datasets developed in consultation with industry and aligned with internationally recognised standards**. Data localisation mandates and data transfer restrictions should be avoided as they will restrict Australia's access to cutting-edge cybersecurity solutions and infrastructure without delivering meaningful security benefits, ultimately undermining Australia's cyber resilience.

Promoting Safe Use of Emerging Technologies

The Discussion Paper highlighted the Government's commitment to supporting the safe and responsible use of critical and emerging technologies, such as AI.[5] We agree that these technologies present immense opportunities, not just for economic and societal benefit, but also in strengthening cyber defences. As malicious actors are also increasingly making use of emerging technologies to improve the sophistication and scale of their attacks, both the public and private sectors must build the capabilities to use these technologies for cybersecurity.

Several challenges may limit businesses' ability to access, develop, and deploy AI tools responsibly, including for cybersecurity purposes. Addressing these challenges will be essential to fostering an environment that supports innovation while managing risk. We highlight three potential challenges below:

1. **Overly broad and onerous obligations that do not focus on high-risk use cases.** Australia should adopt a narrow, risk-based approach to AI regulation.[6] An overly broad approach risks capturing a wide range of low-risk, productivity-enhancing tools and imposing disproportionate compliance burdens. Policymakers should focus on identifying specific AI use-cases that present high risks to individuals. For example, we have encouraged policymakers to focus on AI systems specifically developed to make consequential decisions which determine an

[5] Discussion Paper (2025), p. 20. Beyond AI, upgrading to post-quantum cryptography (**PQC**) is critical for safeguarding the digital foundation of modern economies. We note that Australia is already taking steps in this regard, and support prioritising quantum preparedness as a national and economic security imperative. See also: PQC Prepared, June 2025, https://bsa.org/policy-filings/pqc-prepared.

[6] BSA understands that, to the extent that the Government was considering regulating AI, any potential mandatory obligations would be focused on the use of AI in high-risk settings, so that low-risk uses of AI (e.g., in optimising parcel delivery, or monitoring weather patterns, or managing traffic flow) can "flourish unimpeded". BSA supports this approach. See: Introducing Mandatory Guardrails for AI in High-Risk Settings: Proposals Paper, September 2024, https://storage.googleapis.com/converlens-au-industry/industry/p/prj2f6f02ebfe6a8190c7bdc/page/proposals_paper_for_introducing_mandatory_guardrails_for_ai_in_high_risk_settings.pdf, p. 7

individual's eligibility for, and result in the provision or denial of, housing, employment, credit, education, access to physical places of public accommodation, healthcare, or insurance.

2. **Policies which do not account for the different roles of various actors in the AI ecosystem.** AI systems often involve a complex network of actors responsible for different aspects of the system's development and deployment. It is crucial to specify the roles and precise obligations of these different actors across the AI supply chain, particularly in the context of high-risk AI systems. In that context, there are at least two actors which should be distinguished from each other and subject to distinct obligations:
   - **Developers** of high-risk AI systems (1) design AI systems specifically intended to be used as a high-risk system; (2) substantially modify high-risk AI systems, or (3) substantially modify non-high-risk AI systems so that they become high-risk AI systems.
   - **Deployers** of high-risk AI systems use high-risk AI system developed by other entities in providing services and solutions to their customers.

   Policies pertaining to AI should acknowledge and distinguish these different roles, since each type of company has access to different types of information and can take different actions to mitigate risks associated with an AI system.[7]
3. **Policies that limit access to information needed to train AI systems.** Access to large and diverse data sets is critical for developing safe and responsible AI systems. Conversely, a lack of training data sets can degrade model performance, increase the likelihood of biased or unrepresentative outcomes, and exacerbate issues like hallucination and factual inaccuracies. Because much of the content on the Internet is subject to copyright protection (which arises automatically upon the creation of an original work), data used for training may include material protected by copyright. To provide legal certainty and enable responsible AI development, BSA urges the Government to introduce a clear text and data mining (**TDM**) exception to clearly allow AI developers to use publicly available and lawfully accessed information, whether protected by copyright or not, for AI model training and related data analysis, both for commercial and non-commercial uses. This would make clear that copyrighted material can be lawfully used for the purpose of computational analysis in AI training, provided the user has lawful access to the material. Such an exception would bring Australia into closer alignment with jurisdictions like Japan and Singapore, promote AI innovation, and preserve appropriate safeguards for copyright holders.

Recommendation: The Government should **adopt a targeted, risk-based approach to the regulation of emerging technologies such as AI**. This includes (1) clearly identifying high-risk use cases; (2) tailoring responsibilities to the distinct roles of different actors in the AI supply chain; and (3) introducing a TDM exception to support access to large and diverse training sets. These measures will ensure that Australia's regulatory framework promotes safe and responsible use of AI, facilitates the deployment of AI tools for cybersecurity purposes, and enables continued innovation, investment, and international alignment.

[7] BSA AI Developers and Deployers: An Important Distinction, March 2023, https://www.bsa.org/policy-filings/ai-developers-and-deployers-an-important-distinction

Active Cyber Defence

The Discussion Paper notes that Australia "must adopt a proactive cyber posture to create a hostile environment for our cyber adversaries" and asks if there is a need to "provide clarity on permissible and non-permissible active cyber defence in the Australian context".[8]

BSA supports adopting a proactive cyber posture to promote resilience and preparedness, but the Government must clearly define "active cyber defence", the scope of permissible activities, and the entities which may be subject to obligations in this context. The Government should not frame the concept of active cyber defence too broadly as this may blur the roles and responsibilities of the public and private sector. Permissible activities should be limited and government-led. We urge the Government to consider the following:

1. **Strictly limited permissible activities.** Active cyber defence could encompass a wide range of activities, from intelligence gathering to more assertive or offensive actions (sometimes referred to as "hack back"). It is critical that the Government limit the scope of permissible activities to clearly defined defensive measures, taking into account both the proportionality of any actions and the potential for anticipated and unanticipated consequential damage. BSA objects to requiring or empowering private entities to engage in retaliatory actions as this may expose companies to criminal or civil liability in some jurisdictions and escalate hostilities with malicious actors. It is also unlikely to be effective in fulfilling its objectives of disrupting or deterring cyber criminals and aiding data recovery. BSA also objects to any measures that would require private entities to weaken the security features of their products and services (e.g., by breaking encryption or creating backdoors). More broadly, in the context of any permissible activities, the relevant regulations must enshrine clear and adequate legal protections for private entities to ensure they are not subject to undue risk when cooperating with government-led cyber defence efforts.
2. **Government-led public-private coordination.** BSA supports a model where active cyber defence capabilities are led by the government and implemented in close collaboration with trusted industry partners through voluntary information-sharing mechanisms. Existing mechanisms such as the National Cyber Intelligence Partnership (**NCIP**) and the Trusted Information Sharing Network (**TISN**) should continue to evolve as trusted, well-governed forums to exchange timely and actionable intelligence.
3. **Consultations, oversight, and accountability.** To the extent that any new powers are vested in government entities in furtherance of active cyber defence, BSA urges the Government to engage in a robust public dialogue with industry stakeholders on how such powers should be scoped and applied. Importantly, creating or expanding new legal authorities, especially where it may permit intrusive measures (e.g., remote access to private sectors systems or devices to neutralise threats), must be robustly debated and, even if implemented, should be subject to independent oversight. Transparent governance mechanisms and regular review processes will be essential for maintaining public trust, ensuring proportionality, and safeguarding civil liberties.

[8] Discussion Paper (2025), p. 21

Recommendation: The Government should **adopt a clearly defined, government-led approach to active cyber defence**, with permissible activities limited to narrowly scoped, defensive measures and excluding any retaliatory actions by private entities. Any new powers should be developed through coordination and consultation with industry, and must be subject to independent oversight, particularly where they may involve intrusive measures.

Managing Vulnerability Disclosures

The Discussion Paper asks if more can be done to "incentivise businesses to adopt vulnerability disclosure policies".[9] BSA supports responsible and voluntary disclosures of vulnerabilities that will enhance the long-term security and resilience of the digital ecosystem. In that context, we recommend that the Government maintain a voluntary approach and encourage businesses to align with internationally recognised standards such as ISO/IEC 29147:2018 (Vulnerability disclosure) and ISO/IEC 301111:2019 (Vulnerability handling processes).

Australia should avoid implementing mandatory disclosure requirements. Such requirements, if implemented without necessary safeguards, may inadvertently introduce new risks, such as the disclosure of sensitive information that alerts malicious actors about the existence of a vulnerability and creates security risks, legal liability for entities that disclose vulnerabilities, or operational inefficiencies without commensurate security benefit. Modern software, and in particular cloud-based software delivered as a service, is much more likely to use a dynamic list of components. As such, disclosed vulnerabilities can become outdated rapidly, limiting their effectiveness. Prescriptive requirements may also inadvertently create compliance burdens and further disincentivise disclosure. In any case, existing coordinated vulnerability disclosure (**CVD**) practices already allow businesses to issue security advisories to customers as appropriate.

The Government could also consider establishing safe harbours or legal protections for good faith security research, which would provide assurances to ethical hackers who report vulnerabilities. Clear guidelines should be established o support responsible disclosure, so that sensitive information remains confidential and public harm can be avoided.

Recommendation: The Government should **promote voluntary, confidential vulnerability disclosure practices aligned with internationally recognised standards** such as ISO/IEC 29147 and ISO/IEC 30111. Any future policy measures should avoid prescriptive mandates and instead focus on incentivising industry adoption through guidance, awareness, and legal protections for good-faith actors. This will encourage broader uptake while preserving operational flexibility and reducing unintended risks.

Sovereignty Capabilities and Requirements

BSA notes the Government's commitment to growing and developing robust sovereign capabilities.[10] However, the Government should not introduce prescriptive sovereignty requirements, such as obligating critical infrastructure entities to use only domestically owned or

[9] Discussion Paper (2025), p. 22-23

[10] Discussion Paper (2025), p. 27

hosted services. BSA advocates for a market-driven and targeted approach which will enable Australia to keep pace with the ever-changing technology and security environment.

As noted in BSA's comments to the Senate Standing Committee on Finance and Public Administration in response to its inquiry on developing sovereign capability in the Australian tech sector,[11] access to secure, cutting-edge technology products and services is especially important in the context of cybersecurity, where the threats and challenges are always evolving and a global perspective of the threat landscape is needed for holistic defence. Many global technology companies invest enormous resources in their cybersecurity capabilities and constantly upgrade the security programs and controls in their systems and services to deal with the latest cyber threats. They also have a wide perspective of emerging threats around the world and are thus in a position to best defend against the latest attacks. The Government should ensure that both the public and private sectors have the best tools at their disposal to face this heightened threat environment.

Relatedly, sovereignty requirements may also restrict the growth of Australia's domestic tech sector. Technology solution delivery requires an array of roles, such as system integrators, developers, trainers, infrastructure managers, and solution support managers. For example, in the Software-as-a-Service (**SaaS**) space, many domestic SaaS providers build their products and services on cloud infrastructure provided by global CSPs. In so doing, these domestic SaaS providers benefit from the innovative solutions, substantial expertise, and reliable infrastructure provided by their global partners. The imposition of sovereignty requirements may limit these SaaS providers' choices to a restricted pool of CSPs, which will not only deprive SaaS providers from using services that best suit their needs, but will also lead to reduced competition and innovation in Australia's information and technology (**IT**) sector. Furthermore, many global technology companies are significant employers of Australian talent and responsible for developing valuable, experienced workers in the IT sector. Experienced workers cultivated by global technology companies are a key source of value across the Australian IT ecosystem, as many of them will take up roles in Australian technology companies, the public sector, and other industries, bringing with them specialised knowledge and skills. Some of these experienced workers also go on to found or help scale Australian startups, creating new jobs in the economy and supporting the development of the Australian startup ecosystem.[12]

As such, instead of imposing blanket sovereignty requirements, procurement policies should consider if the technology is developed and sold by a company based in a country that is one of Australia's trusted partners. Australia should prioritise procuring and deploying technology from trusted vendors and supply chains, while avoiding restrictions based on country of origin to maintain supply chain resiliency. This approach considers the security and operational needs of government entities while still allowing both the public and private sectors to access best-in-class technology, thus building greater resilience without sacrificing competitiveness. This approach can be further supplemented by adopting and referencing internationally recognised

[11] BSA Comments on Senate Inquiry Into Sovereign Capability in the Australian Tech Sector, February 2024, https://www.bsa.org/policy-filings/australia-bsa-comments-on-senate-inquiry-into-sovereign-capability-in-the-australian-tech-sector

[12] Harnessing the hidden value: How US tech workers boost the growth of Australia's tech ecosystem, August 2023, https://techcouncil.com.au/wp-content/uploads/2023/08/20230807-Harnessing-the-hidden-value-vfff-portrait891.pdf

standards in procurement policies, which ensure that the procured technology is aligned with international best practices.

Recommendation: The Government should **avoid imposing prescriptive sovereignty requirements, which would restrict access to best-in-class cybersecurity tools and harm the competitiveness of Australia's IT sector.** Instead, Australia should pursue a risk-based, standards-aligned approach that recognises providers from trusted jurisdictions and prioritises security, capability, and interoperability over nationality.

Global Engagement to Shape Norms and Promote Regulatory Alignment

BSA strongly supports the Government's efforts to engage internationally to shape cyber norms and promote regulatory alignment.[13] Alignment across jurisdictions is critical to reducing international regulatory fragmentation, lowering compliance burdens, and enhancing collective cyber resilience.

Two areas of international cooperation merit particular focus.

Harmonisation of cyber incident reporting requirements across different markets

BSA urges the Government to work with international partners to harmonise cyber incident reporting obligations, including what constitutes a "reportable cyber incident," the timeframes for notification, and the type of information that must be submitted to authorities. As highlighted in BSA's 10 Principles for Cyber Incident Reporting Harmonization Around the Globe,[14] harmonised requirements create a set of consistent data points from which stakeholders can efficiently and effectively share information, enhance threat intelligence, improve vulnerability management, adjust security controls, and expedite incident responses.

BSA's 10 principles are as follows:

1. **Align domestic reporting requirements.** National governments should ensure the cyber incident reporting requirements of their states, provinces, prefectures, municipalities, and territories as well as each of their agencies are harmonised.
2. **Define "reportable cyber incident" consistently.** The Government should collaborate with private sector partners and academia to create a shared definition of what types of cyber incident are reportable cyber incidents. Reportable cyber incident should be narrowly defined so that they include only actual cyber incidents that are significant and compromise a business's ability to deliver critical functions, and not suspected activities or those that only risk or jeopardize such functions or otherwise make a cyber incident more likely.
3. **Apply reporting obligations only to the business that is the victim of a reportable cyber incident.** Governments should not require a business's third-party service provider to report incidents on behalf of the business. Such requirements result in duplicative, conflicting, and inefficient reporting. If a third-party service provider is the victim of a reportable cyber incident itself, then it should be required to report as any other business

[13] Discussion Paper (2025), p. 29

[14] BSA's 10 Principles for Cyber Incident Reporting Harmonization Around the Globe, February 2025, https://www.bsa.org/files/policy-filings/02182025bsacyberincidreporting.pdf

would be required. To support greater consistency in reporting obligations, BSA also encourages the Government to adopt a clear distinction between data controllers and data processors in the Privacy Act.[15] Importantly, this distinction ensures that obligations are clearly and appropriately allocated among different business entities in the data privacy context.

4. **Commence reporting requirements based on the same knowledge threshold.** The timeframe governments establish in which in incidents must be initially reported should begin when a business knows it has suffered a reportable cyber incident and not when a business only suspects or reasonably believes it has suffered a reportable cyber incident.

5. **Standardise timeframes.** Governments should align deadlines for providing "reports" (i.e., businesses privately providing information about and analysis of known cyber incidents). Governments should provide at least 72 hours for an initial report — this timeline is aligned with the reporting frameworks of key jurisdictions, notably the European Union's NIS 2 Directive and the US's Cyber Incident Reporting for Critical Infrastructure Act (**CIRCIA**).

6. **Collect the same information.** Governments should require the same, targeted information in notifications and reports, which should be limited to information an affected business knows about 1) the malicious actor including its tactics, techniques, and procedures; 2) the vulnerability, including how it was exploited; and 3) the impacted information and information systems. If timeframes for reports are not the same, then the information required in a report should be commensurate with the time allotted for reporting.

7. **Designate a single government agency responsible for receiving all cyber incident reports.** Governments should ensure that, particularly during cyber incident response and recovery, businesses do not have to navigate a bureaucratic labyrinth or provide the same reports to multiple agencies to meet various requirements. Instead, governments should establish a single point of contact to which the report is required to be sent.

8. **Use information obtained in cyber incident reports only for cybersecurity purposes.** Governments should only use the information provided by a business in a cyber incident report, most of which will be sensitive information, for cybersecurity purposes.

9. **Protect information from public disclosure and share only anonymized analysis.** Governments should protect information obtained in cyber incident reports from laws and policies that provide the public access to information and share only the anonymized analysis gathered from the cyber incident reports with other cybersecurity stakeholders to reduce barriers to businesses sharing information, reduce the likelihood of further harms to a business victim, and improve the cybersecurity of other businesses.

10. **Create a reciprocity mechanism so a business's cyber incident report to one government satisfies its reporting requirements to other governments.** Notifications

[15] In brief, "data controllers" refer to entities which determine the purposes and means of processing personal data, whereas "data processors" are entities that handle personal data on behalf of controllers pursuant to their instructions. In its Response to the Privacy Act Review Report, the Government agreed-in-principle to the proposal to implement a clear distinction between controllers and processors in the Privacy Act (see Government Response to the Privacy Act Review Report, September 2023, https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report).

and reports provided to like-minded governments should be accepted as sufficient to meet a government's own cyber incident reporting requirements.

Mutual recognition of cloud security certifications

Cloud computing is foundational to digital transformation, public sector service delivery, and cybersecurity itself. Governments around the world are increasingly adopting cloud security certification schemes to verify the trustworthiness of CSPs before allowing them to serve government or critical infrastructure sectors. While this intent is sound, the emergence of diverging national schemes risks creating a complex, duplicative, and fragmented ecosystem that deters investment and slows adoption.

As outlined in BSA's paper "Projecting Cyber Strength Through Improved Cloud Security",[16] like-minded governments should pursue mutual recognition of cloud certification frameworks, particularly where national schemes share common reference points such as ISO/IEC 27001 (Information Security Management Systems). In practice, each government's existing or contemplated cloud certification programs can have hundreds of requirements and associated controls. Requiring a CSP to demonstrate conformance numerous times for the same or similar set of controls does not improve security. In addition, it limits the ability of government agencies and local businesses to use their preferred, secure cloud service; it drives up costs; and it rewards businesses for their ability to navigate unique, complex certification procedures rather than for providing better security and functionality.

Mutual recognition would not impede a country's ability to set its own cloud security requirements — the recognition would only apply to those controls that are mapped as functionally equivalent. For example, governments might require different certifications for businesses in different sectors. However, mutual recognition would improve cybersecurity and resilience broadly and strengthen the foundation from which partners can collaborate and address large and novel challenges. Mutual recognition would directly help partner countries by providing government agencies and local businesses access to their preferred cloud services, enhancing the incentives for CSPs to invest in and deliver more secure services, and helping improve citizen and customer experience by using the most secure and functional cloud services.

Recommendation: The Government should prioritise international engagement in two key areas: (1) **harmonising cyber incident reporting requirements** by aligning definitions, timelines, and thresholds with trusted partners; and (2) **pursuing mutual recognition of cloud security certifications** by mapping functionally equivalent controls across international frameworks. These steps will promote interoperability, strengthen cyber resilience, and ensure Australia remains a leading voice in shaping trusted, globally integrated digital ecosystems.

Conclusion

We thank DHA for the opportunity to provide our recommendations in response to the Discussion Paper. We hope our comments are useful as you continue to advance Australia's Cyber Security Strategy and the Horizon 2 Action Plan. We welcome DHA's consistent commitment to engaging

[16] Projecting Cyber Strength Through Improved Cloud Security: How to Improve Cybersecurity through Mutual Recognition of Cloud Certifications, March 2025, https://www.bsa.org/files/policy-filings/03272025bsacyberstrengthcloudsec.pdf

with industry stakeholders, including BSA and our members and we look forward to continued dialogue in support of your important mission to protect Australian citizens and assets and to achieve your goal of becoming a world leader in cybersecurity by 2030.

Yours sincerely,

[redacted]