20 February 2024

BSA COMMENTS ON SENATE INQURY INTO SOVEREIGN CAPABILITY IN THE AUSTRALIAN TECH SECTOR

Submitted to the Senate Standing Committee on Finance and Public Administration

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the Senate Standing Committee on Finance and Public Administration (**Committee**) on its inquiry into supporting the development of sovereign capability in the Australian tech sector (**Inquiry**).[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, contributing to Australia's socio-economic growth. We are proud that many Australian companies and organisations, including the Australian Public Service (**APS**), continue to rely on our members' products and services to do business and support Australia's economy.

The Inquiry's Terms of Reference[3] raises important considerations, including the need to support Australian tech companies and the consequences of using "non-sovereign" tech in the APS. However, it is just as important to ensure that the public sector has access to cutting-edge products and services from trusted partners to achieve various policy objectives, such as digital transformation and cyber security threat management. BSA advocates for a market-driven and targeted approach, which will enable the APS to keep pace with the ever-changing technology and security environment. This is also not at odds with the policy objective of supporting Australian tech companies.

Summary of BSA's Comments

1. Ensure that the APS can access cutting-edge products and services that best suit their needs.
2. Overly stringent sovereignty requirements in public procurement will disrupt important policy goals, including restricting the growth of Australia's tech sector.
3. Procurement policies should identify trusted partners and be aligned with internationally recognised standards

---

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

[2] Inquiry into supporting the development of sovereign capability in the Australian tech sector, December 2023, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/Supporting_Aust_tech47.

[3] Terms of Reference for inquiry into supporting the development of sovereign capability in the Australian tech sector, December 2023, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/Supporting_Aust_tech47/Terms_of_Reference

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

Ensure that the APS can access cutting-edge tech products and services

With the growth of the digital economy, the needs of the public sector have similarly evolved. In the recent Data and Digital Government Strategy,[4] the Government pledged to "deliver simple, secure and connected public services, for all people and business, through world class data and digital capabilities" as their 2030 vision.[5] Acknowledging that data and digital technologies are critical to the Government's activities, the Strategy committed to, among other things, improving service delivery, replacing outdated technologies, reducing the risks and impacts of data breaches and other cyber security incidents, and encouraging broader adoption of emerging technologies.[6] Similarly, under the APS Reform Agenda, the APS committed to "co-design the best solutions to improve the lives of the Australian community" (Priority Two) and to "create… a robust and trusted institution that delivers modern policy and service solutions for decades to come" (Priority Four).[7]

To meet these commitments, the APS needs access to secure, cutting-edge tech products and services. Procurement policy settings and requirements should therefore prioritise the technical merits, security, quality, functionality, pricing, and efficiency of the tech, so that the APS can procure products and services that best suit their needs. This is especially important in areas such as cyber security, where the threats and challenges are always evolving, and a global perspective of the threat landscape is needed for holistic defence. Cyberattacks by malicious actors can have devastating consequences if they disrupt essential services provided by the public sector or compromise national security. Many global tech companies invest enormous resources in their cyber security 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 help APS defend against the latest attacks. The APS should ensure that they have the best tools at their disposal to face this heightened threat environment.

To further establish confidence in the tech that the APS procures, the Government could also update key procurement policies (e.g., the Commonwealth Procurement Rules[8]) to reference both cyber and supply chain security. This would ensure that the APS considers non-financial benefits when procuring tech, such as a vendor's ability to manage end-to-end risk across its supply chain. More broadly, expressly enshrining such considerations in procurement policies will support the APS in making sound and secure tech procurement decisions on behalf of the Commonwealth and improve Australia's national cyber security posture.

Overly stringent sovereignty requirements will disrupt important policy goals

Relatedly, BSA cautions against imposing overly stringent sovereignty requirements in public procurement, as doing so will disrupt important policy goals. Such policy goals include facilitating the growth and development of Australia's tech sector, which we note is one of the priorities highlighted in the Inquiry's Terms of Reference.

Sovereignty requirements may 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 the cloud infrastructure provided by global cloud service providers. In so doing, these domestic SaaS providers benefit from the innovative solutions, substantial expertise and reliable infrastructure provided by their

---

[4] Australian Government Data and Digital Government Strategy, December 2023, https://www.dataanddigital.gov.au/sites/default/files/2023-12/Data%20and%20Digital%20Government%20Strategy%20v1.0.pdf

[5] Data and Digital Government Strategy (2023), p. 5.

[6] Data and Digital Government Strategy (2023), p. 9.

[7] Australia Public Service Reform Outcomes and Initiatives, October 2022, https://www.apsreform.gov.au/about-aps-reform/our-focus-areas, accessed February 2024.

[8] Commonwealth Procurement Rules, June 2023, https://www.finance.gov.au/sites/default/files/2023-06/Commonwealth%20Procurement%20Rules%20-%2013%20June%202023.pdf.

global partners. The imposition of sovereignty requirements may require these SaaS providers to select from a restricted pool of cloud service providers, which will not only deprive SaaS providers from using services that best suit their needs, but also lead to reduced competition and innovation in Australia's tech sector. In turn, the APS will be forced to procure tech from an increasingly limited roster of companies which may not be able to offer the best-in-class tools and services.

Relatedly, many of these global tech companies are leading employers of Australian talent and responsible for developing valuable, experienced workers in the tech sector. Experienced workers cultivated by global tech companies are a key source of value across the Australian tech ecosystem, as many of them will take up roles in Australian tech 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.[9]

In an increasingly competitive digital global marketplace, the transmission of knowledge, ideas and innovation is critical. Sovereign requirements will stifle this diffusion, preventing the Australian tech sector from scaling through the services and talent that global tech companies provide.

Identify trusted partners and align with internationally recognised standards

BSA recognises that the origin of tech products and services used by governments are important from a national security perspective. However, as highlighted above, exclusively relying on home-grown technologies will not be as effective as identifying vendors and technologies built upon the highest standards of product integrity and supply chain best practices. In this regard, instead of imposing blanket requirements that apply to all non-Australian tech, procurement policies should consider if the tech is developed and sold by a company based in a country that is one of Australia's trusted partners, such as the US, Japan, Singapore, and the EU. This approach considers the security and operational needs of government entities while still allowing the APS to access best-in-class tech.

This approach can be further supplemented by adopting and referencing internationally recognised standards in procurement policies, which ensures that any tech procured by the APS are aligned with international best practices. For example, alignment with the International Organization for Standardization (**ISO**)/International Electrotechnical Commission (**IEC**) 27001 Standards, which provide requirements for an information security management system, can ensure that Australia benefits from proven approaches to cyber 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. BSA notes that, particularly in the context of cyber security, Australia's Department of Home Affairs collaborates closely with their international counterparts, including the US's Cybersecurity and Infrastructure Security Agency, Japan's National Center of Incident Readiness and Strategy for Cybersecurity, and Singapore's Cyber Security Agency, in publishing principles and approaches for "Secure-by-Design" software.[10] This is preferable to developing national standards that could duplicate and potentially conflict with existing efforts.

The above suggestions are also in line with the Quad Principles on Critical and Emerging Technology Standards (**Quad Principles**),[11] where the Quad members affirmed their support for "private sector-led, consensus-based, and multi-stakeholder approaches to international standards development that foster interoperability, compatibility, and inclusiveness." Specifically, the Quad Principles stated that technology standards "should promote interoperability, innovation, trust, transparency, diverse

---

[9] 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

[10] Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design software, October 2023, https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf. Initially published in April 2023, this joint guidance urges software manufacturers to take urgent steps necessary to ship products that are secure by design and revamp their design and development programs to permit only secure by design products to be shipped to customers.

[11] Quad Principles on Critical and Emerging Technology Standards, May 2023, https://www.pmc.gov.au/sites/default/files/resource/download/quad-principles-critical-emerging-technology-standards.pdf.

markets, security-by-design, compatibility, inclusiveness and free and fair market competition" and that the members "[s]upport technology standards that promote interoperability, competition, inclusiveness and innovation." We urge the Committee to bear the Quad Principles in mind as it moves forward with this Inquiry.

Conclusion

We hope that our comments will assist the Committee with this Inquiry. 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
Senior Manager, Policy – APAC