16 June 2020

Ambassador Tobias Feakin

R.G. Casey Building

John McEwen Crescent

Barton ACT 0221 Australia

Submitted electronically via cyberaffairs@dfat.gov.au

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE CYBER AND CRITICAL TECHNOLOGY INTERNATIONAL ENGAGEMENT STRATEGY

Dear Ambassador

BSA | The Software Alliance[1] welcomes the opportunity to provide comments for the Department of Foreign Affairs and Trade Cyber and Critical Technology International Engagement Strategy consultation. We welcome the contribution already made by the Government of Australia and by Ambassador Feakin as part of the previous Critical Technology International Engagement Strategy.

The economic and societal effects of the COVID-19 pandemic will likely last much longer than the immediate public health crisis. As governments around the world work to recover their economies from the economic impact of the crisis and build digital resilience into their businesses, this is an opportunity for the Australian Government to advocate for a strong digital economy that opens up new markets for Australian businesses and builds a stronger and more resilient regional economy.[2]

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] See more information on BSA's policy recommendations for recovery from COVID-19 at https://www.bsa.org/policy-filings/bsa-response-recovery-agenda.

300 Beach Road
#25-08 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

What should Australia's key international cyber and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology?

Promote the free flow of data transfers across borders

The rapid and seamless movement of data across borders is essential to the 21st century global economy. Cross-border data transfers allow software companies to provide new and innovative services to every sector of national economies — driving growth, enabling the technologies of the future, improving health and safety, and promoting social good.

Some countries are considering, or have implemented, measures that mandate data localization. Laws that require data to be stored locally, or that restrict the movement of data across borders, not only impede innovation in the development of cutting-edge technology, but also put every local business at a competitive disadvantage by limiting the services available to them, and the markets they can access.

Australia has been a strong advocate for promoting cross border data flows and antilocalization policies and should continue to do so. BSA advocates the adoption of trade norms to prevent data localization requirements and opposes new localization proposals and requirements in markets around the world.[3]

Strong Global Cybersecurity Environment

Cybersecurity is a vital component of a vibrant global digital economy. BSA supports efforts to improve government and industry capabilities and readiness to address cybersecurity threats. These include promoting a secure software ecosystem, strengthening cybersecurity workforce capabilities, supporting policies that enable the development of cutting-edge cybersecurity technologies, and other steps to secure and defend information infrastructure.

Australia should continue to be a strong advocate for a safe and secure Internet.

Malicious cybersecurity activity carries different risks for different systems. There are generally multiple approaches to defending against the same type of cyber-attack, and multiple approaches to improving system security and resiliency in general. Policies should reflect these variables, prioritizing approaches that address different levels of risk and enable owners and operators of networks and systems to defend their infrastructure with the technologies and approaches they deem best to meet the level of security desired.

National information technology ecosystems and the digital economies they support depend on the ability to innovate new solutions. Cybersecurity 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.

The strategy should encourage the mutual adoption of a voluntary, standards-based, outcome-focused cyber risk management frameworks to drive the adoption of stronger cybersecurity measures by both government and industry stakeholders.[4]

Strong and Interoperable Data Privacy

Privacy frameworks should enable and encourage global data flows, which underpin the global economy. Where differences exist among varying privacy regimes, governments should create tools to bridge those gaps in ways that both protect privacy and facilitate the free flow of data. BSA promotes a user-centric approach to privacy that provides consumers with control over their personal data while ensuring industry can continue delivering value to consumers by providing innovative products and services.

Privacy systems must support the free flow of data across international borders so cloud computing and other valuable data services can flourish. BSA also supports efforts to ensure that law

---

[3] See more information on the BSA position on cross border data flows at https://www.bsa.org/policy-issues/cross-border-data.

[4] See more information on the BSA position on cybersecurity at https://www.bsa.org/policy-issues/cybersecurity.

enforcement authorities can access stored content, but only pursuant to a process that has sufficient privacy and due process protections.[5]

Australia should advocate for strong internationally interoperability privacy regimes globally.

We would welcome the opportunity to discuss this further. If you require any clarification or further information in respect of this submission, please contact the undersigned at brianf@bsa.org or +65 8328 0140.

Yours faithfully,

Brian Fletcher

Director, Policy – APAC

BSA | The Software Alliance

[5] See more information on the BSA position on privacy, including the BSA Privacy Framework and Global Privacy Principles at https://www.bsa.org/policy-issues/privacy .