18 December 2020

Digital Transformation Agency

Submitted Electronically

BSA RESPONSE TO DIGITAL TRANSFORMATION STRATEGY 2.0

BSA | The Software Alliance (**BSA**) appreciates the opportunity to provide input to the Digital Transformation Agency (**DTA**) on the proposed Digital Transformation Strategy refresh for the Australian Government (the **Strategy**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[1] are among the world's most innovative companies, creating software solutions that spark the economy. Our members are at the forefront of software-enabled innovation and digital transformation that is fuelling global economic growth, including cloud computing and Artificial Intelligence products and services.

The DTA's discussion paper, *Digital Transformation Strategy 2.0 Discussion Paper*[2] (the **Paper**), notes the progress to date and the importance of accelerating the government transformation and building on the accomplishments so far. It provides the context for the next stage of Australian Government digital transformation and provides several questions to shape input on the strategy going forward.

BSA's foundation, software.org prepared a paper to support governments around the world leverage digital solutions. *The Case for Modernizing IT Now*[3] discusses the importance of digital transformation for governments, particularly post-COVID-19. It highlights the opportunity to make digital investments, including in software and cloud services, to help them accomplish even more in their everyday operations in the face of future challenges. The software.org paper offers 6 high-level steps for governments to modernise its systems:

1. Support and expand remote workforce collaboration.

2. Ensure the security of distance work technology.

3. Improve digital presence and offerings.

[1] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DocuSign, 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] *Digital Transformation Strategy 2.0 Discussion Paper,* Digital Transformation Agency, https://www.dta.gov.au/digital-transformation-strategy/digital-transformation-strategy-refresh

[3] *The Case for Modernizing IT Now,* software.org, *https://software.org/reports/it-modernization/*

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

4. Invest in digital service delivery tools.

5. Modernise citizen support operations.

6. Plan and prepare for future disruptions.

The software.org paper also provides specific considerations for government digital transformation such as the deploying collaboration tools in modern workplaces, the importance of identity management in managing security risk, the value of electronic signatures, the designing and upgrading websites for service delivery, and the value of cloud computing solutions in preparing for future disruptions.

Principles for transformation

The Paper asks about whether the principles in the current Digital Transformation Strategy are still relevant for the next iteration, and whether issues such as privacy, cybersecurity and data retention should be included as additional principles. The five current principles are:[4]

1. People's needs are at the heart of our policy and service design

2. We prove trustworthiness in everything we do

3. We partner and collaborate to deliver value

4. We continuously explore and implement innovation

5. We deliver best value for money for the public

BSA agree that having strong privacy and cybersecurity controls, and being able to demonstrate that, are vital components of a digital transformation strategy. However, in the context of the Strategy they are likely already covered as an aspect of the trustworthiness principle.

Opportunities

The Paper notes that Australia wishes to be a top 3 global digital government by 2025 and asks about some of the opportunities that Digital Transformation could bring and what needs to be achieved across several key domains including technology, policy, people and alliances.

Broadly, digital transformation promises productivity boosts for the Australian Government through the elimination of manual and paper-based processes, and automation.

Digital solutions can also help address business and service agility. This agility can solve challenges like reach and capacity issues through times of crisis or high demand. While the traditional communications channels such as phone or email support are clogged, the government can use more innovative approaches to rethink citizen services. Intuitive artificial intelligence, AI-enabled moderation of online platforms, and other cloud-enabled communication channels can be used together to ensure the Australian Government and citizens are able to offer and benefit from fast access to urgently needed information.

During the pandemic, organisations who were agile and able to adapt to leverage technology responded quickly to the rapidly changing environment. As Australia moves forward, both governments and enterprises need to build agility and resilience to absorb future shocks and to adapt to a distributed or hybrid environment where remote work is a permanent feature.

To continue supporting work flexibility in the future, organisations need to build a resilient distributed infrastructure. This will include putting in place capability and infrastructure to enable working securely from anywhere, collaborating from any device, managing from anywhere, and maximising experience and productivity. The Government can lead by example as it accelerates its digital transformation by

[4] *Digital Transformation Strategy 2.0 Discussion Paper,* Digital Transformation Agency, https://www.dta.gov.au/digital-transformation-strategy/digital-transformation-strategy-refresh, p8

establishing resilient cloud-first infrastructure to support an operating environment with distributed workers and applications.

A common mistake made by organisations is taking a piece-meal approach to digital transformation. Whilst benefits may be gained from individual service digitalisation, without a design thinking or holistic approach to digital strategies, and a focus on building out core platforms and common services, inefficiencies and capability gaps can outweigh benefits.

Technology

Cloud services

One of the most powerful technologies for governments' digital transformation remains cloud services. Cloud services enable governments to access, process, and transmit data across diverse geographies and work environments at the push of a button, building in speed, scalability, flexibility, and mobility. Cloud technologies are critical to creating agile governments that can accelerate and scale to keep pace with advances in technology, changes in policies, and growing public expectations.

To take full advantage of this technology, the Government needs to remove barriers to the adoption of cloud services, and develop policies that prioritise a risk-based, technology adaptable approach in the systems and services that store, process and transfer data. Barriers such as security policies and data localisation requirements are noted below.

Artificial intelligence

Another key technology for digital transformation in governments is Artificial Intelligence (**AI**).

BSA provided comments to the Department of Industry, Science, Energy and Resources in response to the consultation on the draft Australian AI Action Plan[5] which addresses another key technology for digital transformation.

As AI is integrated into Government processes that have consequential impacts on people — such as their ability to obtain access to payments, housing, or employment — the public must be confident that such technologies are being designed and deployed responsibly.

To foster such trust, the Government should focus on ensuring that existing laws, administrative processes, and regulations are keeping pace with the evolution of technology. The public should be assured that the strength of these protections will apply irrespective of whether a decision is made by a person or an automated system. In this regard, we note that existing regulatory regimes are often sufficient for addressing concerns with the adoption and use of AI. To the extent that new regulations are necessary, those should be focused on specific applications of AI that pose high risks to the public, and should account for the unique roles and responsibilities of the range of actors involved in an AI system's supply chain.

Given the global nature of AI development, we recommend that DTA ensure that Australia's approach to AI governance is aligned nationally with widely adopted, international approaches. In addition to promoting trust, confidence, and marketplace efficiencies, international standards have the added benefit of mitigating the market distorting risks that can accompany country-specific standards. Consistent with this, the Government should prioritise Australian participation with the range of international standards development organisations that are currently developing AI standards. Australia should likewise continue to influence the development of global norms for AI governance through multilateral engagement with the OECD and the Global Partnership in AI.[6]

Policy

Cybersecurity

Australia's compliance approach to cloud security continues to be a barrier to the adoption of cloud services. Compliance frameworks that rely on bespoke local standards, such as Australia's

[5] BSA Comments on the Draft Australian AI Action Plan, BSA | The Software Alliance, https://www.bsa.org/policy-filings/australia-bsa-comments-on-the-draft-australian-ai-action-plan

[6] The Global Partnership on AI takes off – at the OECD, https://oecd.ai/wonk/oecd-and-g7-artificial-intelligence-initiatives-side-by-side-for-responsible-ai

Information Security Manual, are expensive to maintain and require an inordinately high amount of resources from the Government to maintain and to train staff in its use without improving security outcomes beyond that provided by international security frameworks. Similarly, the revised Government Cloud Security Guidance, released in 2020, is yet to prove whether it will improve the assessment process and make a wider range of cloud services available to the government.

Cybersecurity policies should instead recognise widely adopted international security standards, such as ISO/IEC27001 and SOCII, to effectively demonstrate the robustness of security controls and organisational security practices. Such certifications allow for the evaluation of providers according to consensus criteria based on well-established industry best practices. They provide strong security outcomes without requiring service providers to undertake duplicative and expensive processes locally in Australia.

The draft Critical Infrastructure Bill inserts more uncertainty and complexity to securing cloud services in Australia by adding another layer of regulation on top of the existing burdensome approach.[7]

Best security practices have shifted from compliance-based approaches to more risk-based, security outcome-oriented practices based on widely adopted, international standards. We encourage the Government to take this opportunity to adopt security solutions better tailored to current technologies and best practices based on "defence in depth" to more effectively advance government operations through the acquisition and use of secure cloud computing services.

Cloud security policies should prioritise the assessment, management, and reduction of risk in cloud infrastructure. The policies should be flexible and allow entities to select the most suitable cloud products for delivering government services in a secure and resilient manner, and thereby also promoting a diverse marketplace of solution providers. Security policies should also be adaptable enough to allow all entities to take forward-looking approaches to security by leveraging innovative security approaches to security as technologies change and threats evolve.

Better security policies help ensure that the Government maintains security and has fast access to the new and innovative technologies needed to effectively provide agile, flexible, and scalable services to support citizens.

Another potential barrier is the increasing interest in data localisation policies in Australia. The security and sovereignty of data is less dependent on its location, and more on what controls are applied to securing the data. Policies that recognise this and avoid data localisation mandates allow service providers and manufacturers that rely on data analysis, AI and cloud computing services to grow into international markets.

The movement of data is critical for the services that sustain global commerce, protect consumers from fraud and counterfeit products, improve health and safety, and promote social good. The ability to move data across borders responsibly also contributes to the workforce's ability to remain productive through teleworking, virtual collaboration, and online training, as well as remotely delivered health care and other services.[8]

Privacy

The Australian privacy regime is not optimised for the current realities of cloud computing. The *Privacy Act 1988* lacks some of the provisions of other modern privacy laws. In particular, it is lacking the distinction between data controllers and data processors.[9] This distinction is important to ensure strong privacy controls are maintained in cloud services, while recognising the variety in cloud deployment scenarios and applications, and the unique roles and responsibilities of the different actors who collect, use or process the personal information of individuals.

---

[7] Protecting Critical Infrastructure and Systems of National Significance, Australian Department of Home Affairs, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

[8] *Cross-border data transfers and data localization*, Global Data Alliance, https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf

[9] *The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation*, BSA | The Software Alliance, https://www.bsa.org/policy-filings/the-global-standard-distinguishing-between-controllers-and-processors-in-privacy-legislation

BSA provided this input as part of comments on the current review of the Privacy Act being conducted by the Attorney-General's Department.[10] With the privacy regime currently being reviewed, it is an opportune time to update the law to include this important distinction.

Data

The Office of the National Data Commissioner recently conducted a consultation on a draft *Data Availability and Transparency Bill 2020* (**DAT Bill**).[11] BSA provided comments as part of that consultation.[12]

Data is the lifeblood of the modern digital economy — powering innovation, spurring economic growth, and enabling organisations to create new jobs, boost efficiency, drive quality, and improve output. Data is also an important component of efficient and effective government services. The ability to combine different data sets, conduct analysis and share data drives more effective government programs, policies and service delivery.

BSA strongly supports initiatives like the DAT Bill for the Australian Government to better use data and build a culture of data sharing and accessibility within the Government for the benefit of Australia.

The DTA should support the development, availability and adoption of tools and best practices that make it easier and less expensive to share data in ways that are consistent with rigorous privacy expectations. Technical tools, such as application programming interfaces or APIs, can facilitate data exchanges that are faster and more secure than traditional transfers.

In addition, the Australian Government should embrace privacy-enhancing technologies. A range of privacy-enhancing technologies and data governance structures can enable value-added uses of data without compromising the confidentiality or security of the underlying data. DTA should promote the use of privacy enhancing technologies — such as differential privacy, homomorphic encryption, and federated machine learning — to create opportunities for sharing data while preserving individual privacy.

People

The increasing use of and demand for technology through digital technology created new demand for jobs in every part of the Government that require an evolving set of skills. The Paper asks how Government can collaborate better with industry and academia to better develop the digital profession in the Australian Public Service (**APS**) of the future.

The Government needs to support new approaches to workforce training, re-training and upskilling the current APS. These education pathways need to be short, flexible, and inclusive so that staff can navigate to the changed skills needed in a modern digital government. Shorter education programs should be supported that provide relevant certifications and other stackable credentials.

An example of this is the Skill Finder website.[13] BSA members Adobe, Atlassian, AWS, IBM, Microsoft, and Salesforce, along with Google have joined with Australian company //balance internet to develop the Skill Finder website. Skill Finder aims to create a marketplace to help the Australian workforce engage with the digital economy by providing access to technology, training courses, and learning opportunities.

Data skills should be part of the broader response to the Government's approach to digital transformation. As part of this, there should be a focus on leadership and culture. Data skills are required at all levels of government, including in senior executive teams. Senior leaders do not always have the experience of using data and should receive appropriate training to experiment with data and find new ways to use data to make decisions.

---

[10] *BSA Comments on the Australian Privacy Act Review*, BSA | The Software Alliance, https://www.bsa.org/policy-filings/australia-bsa-comments-on-australian-privacy-act-review

[11] Consultation on the Data Availability and Transparency Bill 2020, Office of the Data Commissioner, https://www.datacommissioner.gov.au/exposure-draft/dat

[12] *BSA Comments on the Data Accessibility and Transparency Bill*, BSA | The Software Alliance, https://www.bsa.org/policy-filings/australia-bsa-comments-on-the-data-accessibility-and-transparency-bill

[13] Skill Finder website, https://www.skillfinder.com.au/

* * *

BSA looks forward to the opportunity to have wide range of conversation on how BSA and our members can work together with the DTA to develop the next Digital Transformation Strategy for the Australian Government. Please let us know if you have any questions or would like to discuss these comments in more detail.

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