Comments on the Department of Home Affairs Australia Cyber Security Strategy 2023- 2030 Discussion Paper

21 April 2023

Workday appreciates the opportunity to provide comments to the Department of Home Affairs ("DHA") Discussion Paper ("Paper") on Australian Cyber Security Strategy 2023 – 2030. Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics are built with artificial intelligence and machine learning at the core to help organizations around the world embrace the future of work. Workday is used by more than 10,000 organizations around the world and across industries – from medium-sized businesses to more than 50% of the *Fortune* 500. With offices in Brisbane, Melbourne, and North Sydney, two in-country data centres, and a customer support presence, we are proud of our robust offerings in Australia. Workday serves major Australian customers including Atlassian, Canva, the Commonwealth Bank of Australia, Latitude Financial Services, One Rail Australia, QANTAS, Reece Group, Telstra, and St Vincent's Health Australia.

In today's digital age, organisations are increasingly reliant on technology service providers for their operations. In particular, Software-as-a-Service (SaaS) has emerged as a more secure alternative to traditional software given that the viability of the SaaS business model is premised on offering robust security measures to its customers. However, accelerated digitalisation has also led to more large-scale data breaches and cyber incidents, and governments are recognising the need to put in place guardrails that can enhance digital security.

Workday commends the Australian government's efforts to make Australia the most cyber secure nation by 2030. As highlighted in the Paper, uplifting Australia's cyber resilience would provide a significant boost to Australia's digital economy. This is however premised on the ability to secure the personal data, infrastructure, and underlying systems, and addressing these challenges would require innovative cybersecurity practices and tools to defend the integrity, privacy, and utility of the digital ecosystem.

Workday offers our comments and recommendations below to aid the Australian government as it reviews and develops the Australian Cyber Security Strategy 2023 – 2030. Please do not hesitate to contact Eunice Lim, Director Corporate Affairs - APJ, at [redacted] if you have any questions or would like further information.

I. Enhance regulatory coherence and avoid regulatory inconsistencies

The Paper notes that the review of the Cyber Security Strategy could be an opportunity to simplify and streamline existing regulatory frameworks, even as the Australian government looks to enhance its cyber legislation. The Paper lists several ongoing workstreams which complement the work of the Expert Advisory Panel to enhance digital security for Australia such as the Privacy Act Review, the National Plan to Combat Cybercrime, Digital Platform Services Inquiry, etc. There are also other existing legislations such as the Security of Critical Infrastructure (SOCI) Act, the Telecommunications (Interception and Access) Act, that attempt to address security concerns, be it from a sectoral angle or a critical infrastructure protection angle. **Workday welcomes such efforts to streamline the various regulatory frameworks and urges DHA and other relevant agencies to conduct a holistic and robust review of existing cyber related legislation and highlight any potential gaps and overlaps.** As part of the review, the DHA and the Expert Advisory Board should conduct a comprehensive assessment of all existing laws and policies related to cyber security or cyber incident reporting/response. This assessment should include, among other issues, the various objectives behind the laws and policies, the risks they seek to address and whether they remain fit for purpose. Importantly, this exercise will be crucial for identifying overlaps in Australia's complex cyber security ecosystem.

The Paper also includes a proposal to expand the scope of the SOCI Act to include customer data and 'systems' in the definition of critical assets to ensure the powers afforded to the Australian government under the SOCI Act extend to major data breaches. **To avoid complicating the legal landscape, Workday urges caution against expanding the SOCI Act before the overall review is completed and encourages the relevant authorities to conduct further consultations and engagement with the wider industry before embarking on this endeavour.** The full implementation of the amended SOCI Act only began in February 2023 and industry is still adjusting to the new compliance obligations under the SOCI. It may be worthwhile to seek industry feedback on the implementation of SOCI before considering if the SOCI Act requires further reforms. Furthermore, any proposed expansion of the SOCI would have to dovetail with the review which the Parliamentary Joint Committee on Intelligence and Security is required to undertake.

The Paper also did not detail the concerns and policy objectives of the government for proposing the expansion in scope of the SOCI Act. It would greatly benefit the industry to understand the rationale of the government and to work with the government to consider if there are other viable alternatives to better protect the data of Australians and enhance the cyber resilience of Australia. For example, more resources could be channelled into helping organisations manage cyber risks, or regulatory guidance could be provided to help organisations shore up their cyber defences through internal security controls or security programmes. While remediation and notification obligations in the event of a breach are no doubt important, especially for consumers, a narrow focus on these aspects could divert valuable resources away from core cybersecurity activities, which may not enhance the overall cybersecurity posture of Australian organisations.

II. Risk-based, outcome focused and technology-neutral policy and regulatory approach

It is imperative that when policymakers are developing new or reviewing existing policies, that different actors are accorded obligations which are proportionate to the roles and responsibilities that each actor plays. Indeed, malicious cyber security activities carry different risks for different actors within the technology ecosystem. For example, the cyber risks faced by an Infrastructure-as-a-Service provider (IaaS) could be different from that of a Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) provider. Further, technology service providers and their enterprise customers both maintain important yet distinct security responsibilities.

Laws and policies should support the cloud services shared responsibility security model, which clarifies that the responsibility of security in the cloud depends on the services procured by the customer and the extent the customer has migrated its data to the cloud. Effective security programs assign appropriate responsibilities to providers and customers relative to their role in, and level of control over, the cloud environment. This model of shared responsibility can be tailored to best benefit customers and providers needs and has been successfully implemented in the financial services and other sectors.

Workday recommends that the 2023-2030 Strategy prioritise approaches and policies 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, and that reflect their particular role in the market.

III. Alignment with internationally recognised standards

Internationally recognised technical standards provide widely vetted, consensus-based frameworks for defining and implementing effective approaches to cyber security. Alignment with internationally recognised technical standards and guidance, such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, 27017, and 27018 standards allows Australia to benefit from proven approaches to common cyber challenges, thus enabling international collaboration. Furthermore, given that the technology supply chain is global in nature, with products containing components from different jurisdictions, building laws and policies based on internationally recognised standards can support interoperability, enhance overall supply chain resilience, and strengthen the security posture of multinational organizations.

In this regard, **Workday strongly encourages the Australian government to embrace such internationally recognised standards when developing its domestic policies and regulations. For example, rather than developing a new domestic cybersecurity certification or domestic standards,** Australia can leverage internationally recognised standards and accepted certifications from internationally accredited bodies as demonstration that a vendor has implemented appropriate security controls. Where there are gaps in internationally recognised technical standards, Workday urges the Australian government to work with other like-minded governments and industry partners to address

those gaps, building a basis for policies that can improve security consistently and cooperatively across different markets.

IV. Cybersecurity in Commonwealth Government departments and agencies

The Paper called out the need for more education and training in cyber security to help improve cyber literacy to address evolving cyber security challenges. **Workday supports this and believes that further investments in cyber security training is an area which the Australian public service would greatly benefit from.** The evolving nature of the cyber security field requires all professionals, not just the cybersecurity professionals, to stay up to date with the latest trends and best practices, to maintain a security baseline. Continuing education and training is necessary to ensure that professionals have the skills and knowledge they need to do their jobs effectively.

Accelerating the adoption of cloud services in the Australian public service would also be important in improving the overall cybersecurity posture of the Australian government. As noted in a 2020 publication by the Australian Cyber Security Centre (ACSC)[1], when properly managed through a thorough understanding of the shared responsibility between the cloud end-user and service provider, *cloud computing service can offer a range of potential cyber security benefits such as, providing access to advanced security technologies, fine-grained access management, comprehensive monitoring, and highly redundant geographically dispersed cloud services*. In contrast, an organisation that owns and manage its own IT infrastructure is responsible for securing all aspects of it, including achieving the desired security baseline, maintaining it and updating it as adversary tradecraft evolves. This would often require the organisation to dedicate significant effort and resources to achieve this. In a highly competitive global cloud services market, cloud service providers use security to differentiate themselves from competitors, hiring the best talent in this space and dedicating significant resources to its development, accomplishing the necessary security improvements while also enabling improved functionality for customers. In this regard, **Workday strongly encourages the Australia Government to invest in modern IT infrastructure and cybersecurity by accelerating the migration to cloud services.**

[1] Anatomy of a Cloud Assessment and Authorisation, ACSC, first published June 2020, last updated October 2021.