13 April 2023

Department of Home Affairs
6 Chan St
Belconnen ACT 2617
Email: auscyberstrategy@homeaffairs.gov.au

Dear Department

Re: 2023-2030 Australian Cyber Security Strategy - Discussion Paper

Salesforce is pleased to provide this submission in response to the discussion paper.

Salesforce and Cyber Security

At Salesforce Trust is our #1 value. The cybersecurity threat is vast, borderless and growing daily. At Salesforce, our customers entrust us with their most sensitive data, and they expect us to protect it using cybersecurity risk management practices and tools that are state-of-the-art. Salesforce strives to ensure that our customers have the functionality to protect their data in line with the existing laws in countries we operate in, such as with our Encryption Key Management Solution (EKMS).

What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

Salesforce response: *Regulatory consistency.* The Strategy notes that there are a range of implicit cyber security obligations placed on Australian businesses, including through the corporations, consumer, critical infrastructure, and privacy legislative and regulatory frameworks, leading to cyber security obligations which are neither clear nor easy to comply with. Salesforce agrees with this assessment.

There are several mandatory reporting obligations for specific types of businesses that are spread across various pieces of legislation. Some of these include: Hosting Certification Framework (HCF); Information Security Registered Assessors Program (IRAP); Security of Critical Infrastructure Act 2018; state specific security frameworks etc.

An example of overlap is the proposed expansion of the HCF to cover Software-as-a-Service (SaaS) providers. However, this expansion is in addition to existing certifications under IRAP. We recommend that these sometimes overalapping regulations be reviewed and clarified to provide regulatory consistency.

How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Salesforce response: *Threat Sharing/Cyber Capabilities.* Now more than ever, threat sharing by governments and private sector is a critical tool to help Salesforce and its ecosystem stay ahead of today's cyber threats. Salesforce supports the establishment and participation of Information Sharing and Analysis Centers, with indemnification of liability when sharing threats. Salesforce has always agrees with the efforts of governments to ensure the timely sharing of cybersecurity information. Salesforce hosts multiple CISOs from across the globe at our annual CISO Forum to facilitate this sharing. We see this as a best-practice for a collaborative approach to achieve better security outcomes across the board.

What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Salesforce response: *International Interoperability of Risk-based Cybersecurity Frameworks*. As a company, we support cybersecurity frameworks that are globally interoperable, and risk-based in their approach. Salesforce supports the comprehensive development of risk management frameworks like the NIST Cybersecurity Framework, and encourage further pursuit of international consensus with similar risk-based models.

We recommend that international standards such as the ISO 27000 series, along with other proven risk frameworks (such as the NIST Cybersecurity Framework), form the baseline for cybersecurity risk management. We note that the combination of ISO27005 and the NIST risk management frameworks is widely considered a best practice by CISOs in Europe. Such an approach would have the added advantages of fostering global harmonisation and encouraging greater consistency among countries in their implementation of existing cybersecurity frameworks. This approach could drive consistency in countries' supervision and enforcement functions, creating frameworks for compliance safe harbors and aiding mutual recognition of cybersecurity risk management measures globally.

Where there are gaps in internationally recognised technical standards, Salesforce recommends the Australian government to work with other government and industry partners to address those gaps, building a basis for policies that can improve security consistently and cooperatively across different markets.

Your sincerely
Sassoon Grigorian
Vice-President, Government Affairs & Public Policy, Asia-Pacific