16 September 2020

Department of Home Affairs
6 Chan Street
Belconnen ACT 2617
Email: ci.reforms@homeaffairs.gov.au

To whom it may concern,

Re: Protecting Critical Infrastructure and Systems of National Significance

Salesforce is pleased to provide this submission to this consultation.

About Salesforce

Salesforce is the #1 CRM, and one the fastest growing enterprise software companies. Salesforce is a cloud computing company covering customer relationship management and other business-focused software to businesses, governments, and other organisations around the world. Salesforce is used by over 150,000 companies.

Salesforce relies on four key values: trust, customer success, innovation, and equality. Trust is Salesforce's number one value, and security is the cornerstone of trust. Our comments are appended below.

Introduction

Salesforce recommends that sectoral definitions be narrowed and clarified – particularly as it pertains to "Data and the Cloud." Salesforce encourages an approach which concentrates on regulated entities which control the systems of national significance, not service providers or processors that work across sectors.

Whilst Salesforce welcomes risk-based elements of the proposed framework, we recommend that Australia not pursue compliance-oriented mechanisms. Moreover, Salesforce recommends concentrating oversight and expertise in a single agency and taking into account existing well-developed practices within each vertical.

Who will the enhanced framework apply to? (Questions 1-6)

- **Avoid blanket designation of critical infrastructure.** There are a wide range of systems that underpin modern society, both concentrated within key sectors, as well as spread amongst many sectors. Those who own and operate these systems may also be responsible for a range of systems. Given this Salesforce cautions against overly broad sectoral classifications. Currently, Critical Infrastructure entities cover *"all entities within expanded Security of Critical Infrastructure Act 2018 designated critical infrastructure sectors".* Determinations which treat entities in a blanket manner may unnecessarily force heightened scrutiny of all systems and functions of entities within a sector, rather than focusing on the most critical sources.

- **Designation of "Data and the Cloud" sector is broad.** Salesforce is concerned that the potential designation of "Data and the Cloud" as a critical infrastructure sector is too broad. This designation aims at merely one component of critical systems rather than taking into account a service provider's actual relationship to critical functions of their customer. As mentioned in consultation paper, the *"proposed reforms will be (and should be) focused at the owner and operator level, not at a specific piece of technology."*

- **Protocol of customer engagement.** It should be noted the distinct relationship between cloud service providers and their customers. The responsibility for cloud security is often a shared one between a customer and their provider, imposing security controls and reporting obligations on cloud service provider could undermine the existing contractual arrangements. In the event of an incident detected by the cloud service provider, their obligation is to report to the customer and work with them to resolve the event.

- **Data classification.** Salesforce recommends data and/or system security rules should consider classification, criticality and sensitivity of the asset being protected. The controls to be designed and implemented should be commensurate to the criticality of the asset and the vulnerabilities it is likely to be exposed to.

Government-Critical Infrastructure Collaboration to Support Uplift (Questions 7-9)

- **Information sharing through Trusted Information Sharing Network (TISN) should be aligned with existing groups.** Voluntary information sharing systems are a key element of a robust cybersecurity ecosystem and Salesforce supports improved efforts in this regard. Many regulated entities are already participating in international information sharing systems. At Salesforce, we are a member of FIRST, a peer-to-peer network governance model that helps build trust and create a safer internet. Efforts to improve TISN should seek to improve interoperability.

Initiative 1: Positive Security Obligation (Questions 10-14)

- **Allow industry players to select the best solutions for their systems.** In principle, Salesforce supports frameworks that allow operators the flexibility to choose the technologies and methods that will be most effective to mitigate the particular threats their systems face. In implementing such a model, we strongly encourage close alignment with the United States National Institute of Standards and Technology (NIST) Cybersecurity Framework, a well-established industry standard, fully adopted by some governments, which already guides many major entities relevant to critical infrastructure protection.

- **Assessment Framework.** It is important to specify the framework that would be used by the regulators to assess industry compliance. It is recommended that existing security and audit certifications and frameworks such as the IRAP, ISO 27001, ISO 27017, ISO 27018, SOC should be relied upon, as far as cloud (SaaS/PaaS) deployments are concerned.

Regulators (Questions 15-21)

- **Promote interoperability for the benefit of Australian businesses with global operations:** While Salesforce is encouraged to see collaboration with the industry on standards, Salesforce cautions against imposing Australia-specific or sector specific mandatory standards that may result in excessive fragmentation of the overall framework. Many cloud providers like Salesforce adopt international standards and certifications. Salesforce encourages the Australian government to align its standards and frameworks to the international best practices.

- **A centralised agency with best-in-class talents will help improve oversight.** While leaving well-established vertical oversight and regulation in place, we encourage a model with greater centralisation of expertise and oversight powers, including a single agency able to pool expertise and oversee multiple sectors in concert with vertical regulators.

Initiative 2: Enhanced Cyber Security Obligations (22-28)

- **Provide clearer information on designation of critical infrastructure entities (CIE), regulated CIE, and systems of national significance.** At a high level, a tiered system which establishes heightened obligations and enhanced cooperation for systems of national significance that pose the greatest risk is well conceived and will help to focus attention and resources where they are most needed. However, the criteria and process by which such systems would be designated should be clearer. Salesforce urges greater clarification of these questions, as well as close consultation with industry in determining the designations and categories.

Initiative 3: Cyber assistance for entities (Questions 29-36)

- **Provide industry players with flexibility to address the threat.** Extraordinary circumstances that would require emergency government powers should be carefully defined to establish full clarity and mutual expectations of the standards, liability, and procedures that apply. Any decision should have the ability for judicial redress.

Thank you for the opportunity to provide comment.

Yours sincerely

Sassoon Grigorian
Senior Director, APAC Government Affairs