AWS COMMENTS IN RESPONSE TO:
PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE CONSULTATION PAPER

A. INTRODUCTION

Amazon Web Services ("**AWS**") welcomes the opportunity to provide feedback on the *Protecting Critical Infrastructure and Systems of National Significance* Consultation Paper ("**Consultation Paper**").

AWS has made significant investments in cloud related infrastructure in Australia, including the AWS Asia Pacific (Sydney) Region and associated edge locations in Sydney, Melbourne, Brisbane, Perth and Canberra over the last decade. We have over 2,000 direct employees across the country, and provide services to hundreds of thousands of active customers across all areas of economic activity, including the Commonwealth Bank, National Australia Bank, Qantas, Canva, Atlassian, the Australian Bureau of Statistics, and RMIT University. AWS plans to power its global infrastructure, with 100 percent renewable energy by 2025 as part of Amazon's commitment to the Climate Pledge, which aims to reach net zero carbon across all of Amazon's operations by 2040. Amazon has invested in two renewable energy projects in Australia, which will add a combined 165 MWs worth of capacity and are expected to generate 392,000 MWh annually – or enough energy to power 63,000 average Australian homes each year.

Security is AWS's top priority. All AWS infrastructure is built to satisfy the requirements of the most security-sensitive organisations.

AWS supports the Australian Government's objective of improving the security and resilience of critical infrastructure across the nation, and welcomes efforts to enhance the existing regulatory framework for critical infrastructure. AWS looks forward to further assisting the Government develop its enhanced regulatory framework to ensure the framework meets the Government's objectives and is practicable for industry. AWS offers the following observations and recommendations on the Consultation Paper.

B. GENERAL COMMENTS ON THE PROPOSED REGULATORY FRAMEWORK

<u>Consultation Process and Scope of Applicability of the Critical Infrastructure Framework</u> *(addressing Qs 1 – 6 of the Consultation Paper)*:

Recommendation 1: The Government should undertake a robust consultation process, which includes the release of an Exposure Draft Bill and a Regulatory Impact Statement, and commit to a review of the legislation by the Parliamentary Joint Committee on Intelligence and Security. An increased focus on cyber security obligations as part of the critical infrastructure framework is timely, and we welcome the consultation undertaken by the Department of Home Affairs ("**DHA**") and Critical Infrastructure Centre to date. The proposed reforms affect a wide range of industries and potentially hundreds, if not thousands, of companies. They will have economy-wide implications. Given the significant changes to the scope, application and content of the laws, it is important that the Government, and the Parliament, work methodically through the new framework and the regulatory regime. We encourage the Government to take the time required to get this reform right.

While we are broadly supportive of the proposal to expand the enhanced regulatory regime to include the 'Data and the Cloud' sector, this expansion raises many new questions. These include what entities or service providers should be included in the sector; what security standards should apply; and how to avoid regulators of other critical infrastructure verticals creating sector-specific security standards that are inconsistent with internationally recognised standards, are impossible to implement, or that increase the cost of compliance without delivering better security outcomes.

We address some of these threshold questions at a high level in this submission, but it will be important to consult further through the process of an Exposure Draft Bill and Regulatory Impact Statement to understand better the intent and impacts of proposed legislative changes.

Recommendation 2: The concept of a "critical infrastructure asset" in the Security of Critical Infrastructure Act ("SCIA") should be used in the enhanced regulatory framework so that obligations apply to specific critical infrastructure assets of a critical infrastructure entity, and not to all facilities and infrastructure of, or products and services offered by, that entity. We agree with the approach of designating critical infrastructure entities based on their interdependency with other functions and the consequences of compromise. We also support the development of more detailed criteria for this designation based on principles of simplicity, transparency, redundancy, and resilience to hazards.

However, it is unclear from the Consultation Paper whether and how the enhanced regulatory framework will apply at the "owner and operator level, not at [the level of a] specific piece of technology". If the proposal is to regulate *all* of an entity's facilities, infrastructure, products, or services – without considering the level of criticality – it could have unintended consequences and result in over-burdensome regulation. For example, it would be disproportionately costly to require an education entity to secure the facilities where student records are stored at the same level as facilities where sporting equipment is kept. Doing so will raise compliance costs for little security gain, and would ultimately be counterproductive for Australia's security. The Consultation Paper makes the point that focusing only on certain technologies could result in others being ignored, but there is a converse risk that dispersing regulated entities' focus across all of their assets, even those that are less important or sensitive, could undermine the security of truly critical assets.

Therefore, we recommend that the enhanced regulatory framework only apply to specific critical infrastructure assets of a critical infrastructure entity. The Government can do so by adopting the existing approach applying to "critical infrastructure assets" in the SCIA. Namely, critical infrastructure assets in a sector are defined, and obligations then apply to the owners and operators of those defined assets. When defining a "critical infrastructure asset", the definition should not be so broad that it captures all of an entity's facilities, infrastructure, products or services without considering their level of criticality.

<u>Information Sharing, Education and Engagement Frameworks</u> *(addressing Qs 7-9 of the Consultation Paper)*

Recommendation 3: Include the Data and the Cloud sector in the expanded Trusted Information Sharing Network (TISN). We recommend that the expanded set of critical infrastructure sectors should be included in the TISN Sector Groups to enhance and integrate with the Government's existing critical infrastructure education, communication, and engagement activities. We would welcome being involved in the TISN and look forward to working with the Government to build deeper understanding of cybersecurity amongst all critical infrastructure entities.

Positive Security Obligation ("PSO") *(addressing Qs 10-21 of the Consultation Paper)*

Recommendation 4: PSOs should be based on actual threat assessments, allow for compensating controls, and cross-sectoral coordination at the outset. We agree with the Government's proposal that principles-based outcomes should form the basis of the PSO. We think that the Government should apply consistent principles to PSOs in both the SCIA and any sector-specific standards, as this will encourage critical infrastructure entities to continue innovating and improving their security posture and practices, while remaining true to the overall principle, or desired outcome, identified by the regulator. On the other hand, adopting a prescriptive approach would require regulated entities to meet an inflexible bar that may not be appropriate for their specific offering. This could stifle innovation and may not lead to the bar not developing over time to adjust to new security threats. This will likely be counterproductive to achieving intended security outcomes.

In addition to those suggested in the Consultation Paper, we also recommend reflecting the following principles in the Exposure Draft Bill and any sector-specific standards:

(i) **The PSO regulatory model should avoid placing duplicative or unnecessary requirements on regulated critical infrastructure entities.** We agree with the Consultation Paper that PSOs should build on rather than duplicate existing regimes that apply to a regulated critical infrastructure entity's use of technology. We think that this can be achieved in several ways. Firstly, a technology service provider, that is also a regulated critical infrastructure entity complying with its own sector PSO, should not have to comply with additional security obligations imposed by another regulator (either directly or via the service provider's regulated customers) that duplicate or build upon that entity's PSO. The government and sector regulators must ensure that existing laws and regulations requiring regulated customers of critical infrastructure entities to perform diligence or security reviews of their service providers, or imposing security obligations on those service providers, state that a service provider's compliance with its own sector PSO is sufficient to meet those requirements without review or additional obligations. The Government should therefore avoid having sector vertical regulators impose separate requirements on regulated technology service providers.

Secondly, the Government should also clarify that entities will not be inspected, examined or audited against the same requirements by multiple regulators. For example, if the Data and the Cloud sector regulator requires a data centre to be audited against a specified standard (e.g. SOC), then it should not be the case that another sector specific regulator, like the financial sector's Australian Prudential Regulation Authority, would need to separately require an audit against the same standard.

If the Government imposes duplicative requirements or audits across different sector verticals, it would increase complexity and overhead costs for regulators. Furthermore, it would be unnecessarily onerous for regulated critical infrastructure entities that offer services to multiple sectors in the Australian economy, creating operational costs without improving overall security outcomes. To this end, we recommend allowing regulated entities and their technology service providers to provide third party audit reports or attestations in lieu of additional "independent audit or regulatory review." Recognising this principle in the legislation will make the administration of government more effective, reduce red tape for regulated entities and improve the overall security posture.

(ii) **PSOs should be based on international security standards and best practices.** Basing the PSOs on accepted international standards such as the ISO 27000 series, SOC, and PCI[1] will ensure that there is international consistency, and ongoing independent review of the standards. This would ensure that Australia's critical infrastructure is offered state-of-the-art protection and reduces the burden on regulators to independently develop compliance standards or to carry out separate audits. Many additional or divergent standards will also increase the cost of compliance and confusion among regulated entities.

(iii) **The PSOs for one sector should not contradict or conflict with those in another sector**. We understand and support the need for sector-by-sector analysis and sector-specific standards, but are concerned that this could lead to a fragmented set of security requirements across different sectors. This increases the risk that technology service providers offering services to customers in multiple critical infrastructure sectors are unable to provide services in one sector because of a competing or contradictory PSO in another sector. Such an outcome is undesirable as it will limit the choice of service providers available for each sector, and increase the cost of compliance for critical infrastructure entities. We believe that the Government should create a forum and process for coordination between the critical infrastructure sector regulators to ensure that sector-specific PSOs are consistent with each other.

Assistance Provisions *(addressing Qs 29-36 of the Consultation Paper)*

Recommendation 5: Do not introduce enhanced Government assistance/intervention powers until there has been further consultation with regulated critical infrastructure sectors, a practical regulatory regime with liability limitation and safe harbours is agreed, and a significantly narrowed set of powers is defined. We recognise and acknowledge the Government's need to protect critical infrastructure from immediate and serious cyber threats. However, we are concerned that the proposal for Government 'assistance' or 'intervention' powers may give government overly broad powers to issue directions or act autonomously. While we have not seen the draft law, the high level summary of these powers suggest they could be significant and exercisable across a broad swath of society, with unclear limitations or guardrails.

The breadth of the newly regulated critical infrastructure sectors, coupled with seemingly broad powers described in the Consultation Paper, raise many issues and unknowns. For example, we are concerned that the Government's power to take direct action in the event of an emergency is vague and undefined. A plain reading of the Consultation Paper suggests that the Government could use these new powers to either issue directions or take autonomous action to do virtually anything in response to cybersecurity threats. It is unclear whether: the triggers for exercising such powers are objective and specific; whether or how the Government would objectively assess if its directions or assistance will improve the situation; what an entity can or cannot be directed to do or not do; what checks and balances will apply; and whether an entity has rights of review and appeal.

[1] ISO27000 series comprises information security standards published by the International Organisation for Standardisation and the International Electrotechnical Commission
SOC – System and Organisation Controls Report
PCI – Payment Card Industry Data Security Standard

We urge the Government to work closely with industry and other relevant stakeholders to define whether these new powers are needed, and if so how they will apply, before legislation to put these powers into effect are introduced into the Parliament.

C. SPECIFIC COMMENTS ON A REGULATORY FRAMEWORK FOR DATA AND THE CLOUD SECTOR

Recommendation 6: Ensure the definition of critical infrastructure and regulated critical infrastructure entities in the Data and the Cloud sector captures all relevant entities within that sector. We believe that the current definition of critical infrastructure in the Critical Infrastructure Resilience Strategy is appropriate and fit for purpose. We also generally support expanding the critical infrastructure regime to include the 'Data and the Cloud' sector.

We believe it will be important to appropriately scope what entities and infrastructure are included in the "Data and the Cloud" sector because these terms can be used to describe many different things. Our view is that the scope of critical infrastructure and regulated critical infrastructure entities in the Data and the Cloud sector should be broad enough to capture all relevant entities within that sector, such as data centre operators, co-location data centre operators, data storage providers, and cloud service providers (whether they use their own data centres or co-location data centres). This will ensure that the enhanced regulatory framework applies consistently to all entities that manage, process, host, or store data – whether in a cloud or on-premise. This coverage is essential to meeting the Government's objective of improving Australian security across multiple sectors.

The Government could achieve this by:

a) ensuring that any definition of a critical infrastructure or regulated critical infrastructure entity encompasses both owners and operators of Australian data centres, and providers of data or cloud services that use Australian data centres; and
b) including a threshold (e.g., power usage or number of server racks) in the definition of "data centre" to capture only those data centres that are likely to be critical infrastructure.

For (b), we would propose the objective test of "a data centre containing IT equipment capable of consuming more than 100kW of power in total", so that operators of infrastructure have clarity on whether they are covered.

Recommendation 7: The PSO in the Data and the Cloud sector should only apply to physical Australian data centre security, and should not require a regulated critical infrastructure entity to implement security measures that are outside of their control. As mentioned above, we are concerned that the Consultation Paper's view of applying the enhanced regulatory framework will apply at the "owner and operator level, not at [a] specific piece of technology", will lead to negative consequences. Our recommendation is that the PSOs for the Data and the Cloud Sector apply to physical data centre security rather than software or services running in those data centres. To reflect modern technology and IT models, the PSO should also avoid requiring regulated critical infrastructure entities to implement security processes outside of their control.

Applying the PSOs to physical security in data centres is the right approach because the Government has experience doing so; there are well known international standards for securing and maintaining data centres; data centre security is important to the security of the nation; and data centre security is often critical to keeping interdependent services and entities running smoothly.

This approach will further the objectives of the Government stated in the Consultation Paper and appropriately balance those objectives with costs of compliance, the impact on regulated critical infrastructure entities, and the cost of administration.

In contrast, there are many compelling reasons not to apply the PSO to the software and services running in the data centre. Firstly, if a PSO applies to the software running in a data centre and the services of a cloud services provider (and not the physical data centres it uses) each of those services will need to meet the requirements even if it is not being used by a critical infrastructure entity. This approach will slow the pace of innovation, delay the launch of new services in Australia, increase the costs of compliance and drive up the cost of services to all Australian customers.

Secondly, it is important software and services deployed in data centres can be used in infinitely different ways. Many modern technology models, including cloud services, emphasise the control and configuration options that are given to customers and intentionally not managed by the data centre owner or cloud service provider. This does not mean that the use of software and services will go unaddressed. We expect that for some sectors there will be sector specific requirements that address the way regulated critical infrastructure entities deploy software regardless of whether it is in their own data centre, a third party data centre, or using a cloud service provider. This balance of security and regulatory responsibility would better reflect the direction of modern technology.

In addition, the PSO should reflect that an entity is only able to implement security processes that is within its control. For example, it would not be possible for a cloud service provider to implement security controls for applications the customer controls. Instead, the law should specify that PSOs do not apply to aspects of security that are outside an entity's control. We think such a proposed allocation of responsibility will enable all regulated critical infrastructure entities to clearly understand their respective security obligations, thereby ensuring that the Government's security objectives are met.

Recommendation 8: The Data and the Cloud sector regulator should be experienced in network infrastructure regulation, and adopt a collaborative approach to developing sector regulations. Given our recommended regulatory focus on the physical security of data centres, as well as the need for cross-sectoral coordination, we believe that an experienced regulator will be required for the Data and the Cloud critical infrastructure sector. We recommend the Government hold off appointing a sector regulator until it has confirmed the breadth of the overall regulatory regime for the sector. The Government should make a final decision on the appropriate sector regulator after comprehensive consultation with industry over all possible options and approaches to regulatory oversight.