By online submission
Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Microsoft Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

08 July 2021

Thank you for the opportunity to share our expertise with the Committee as it considers this important reform.

Microsoft is a leading global cloud service provider and aims to support organisations across the Australian economy. In addition to our commercial offerings, we are committed to providing industry-leading cyber security protection for our customers and driving broader security improvements across industries and sectors. We therefore support the Government's efforts to improve the overall resilience of Australia's critical infrastructure and support many aspects of the *Security Legislation Amendment (Critical Infrastructure) Bill* (**Proposed Legislation**).

Microsoft recognises the difficult task before the Australian Government in addressing the emerging security risks while guarding against regulatory confusion that may inadvertently decrease the overall security of Australia's critical infrastructure assets. That said, we have been encouraged by the Government's acknowledgement of the central role public-private partnerships will play in creating logical regulation, and we are ready to partner with the Department of Home Affairs as it begins developing sector-specific security frameworks.

We also appreciate the Government's recognition of the substantial investments organisations like Microsoft continue to make to enable our customers to be more secure, resilient, and better prepared for variety of threats. Unlike other new critical infrastructure verticals identified in the Proposed Legislation, the critical data storage or processing sector is unique in its exposure to, and familiarity with, cyber security threats. The sector includes hyperscale cloud service providers like Microsoft that operate horizontally across industries and provide services that form the foundation for the operation of other sectors. Supporting secure and resilient networks is essential to the core business of cloud service providers; as a result, entities within the data storage or processing sector are at the cutting edge of security investments, threat intelligence, and incident prevention and mitigation.

While we support the larger goals of the Proposed Legislation, we believe certain aspects of the bill undercut efforts to secure Australian critical infrastructure. It is therefore in the spirit of partnership with the Government to improve the security and resilience of Australia's critical infrastructure that we submit the following comments regarding the Proposed Legislation.

1. Withdraw the authority for the Government to intervene in Cloud Service Provider systems, including by introducing untested third party software

Microsoft is a leader in cloud security and maintains significant cybersecurity capabilities that are fundamental to the trust our customers place in the services we provide. Cloud service providers like Microsoft have strong commercial and moral incentives to protect our networks and respond to and mitigate cyber security incidents. Indeed, organisations familiar with their own systems are inarguably best placed to do so and this is particularly true for hyperscale cloud service providers that operate highly complex and interdependent systems.

As currently drafted, the Proposed Legislation introduces sweeping powers for the Government to, among other interventions, mandate the introduction of third-party software into highly complex environments operated by cloud service providers. We urge the Committee to consider removing this authority or limiting its scope so that it does not apply to entities who meet certain qualifications (*e.g.*, entities with a demonstrated history of cooperation with the Government and robust cyber security protocols). As with other government intervention powers, introducing third parties unfamiliar with a cloud service provider's systems and architecture risks compromising the security and integrity of these systems and creating collateral consequences, including the interruption of critical services and the creation of new vulnerabilities. While we appreciate the Government's interest in these powers, we cannot envision a scenario in which it would be appropriate for the Government to intervene or install software in complex systems operated by sophisticated hyperscale cloud providers.

The requirement in the Proposed Legislation that an organisation be unwilling or unable to respond to an incident prior to this authority being exercised is ambiguous and, in Microsoft's view, an inadequate protection against the uncertainty and risk of a potentially disruptive intervention by the Government. Microsoft believes the goals of the Proposed Legislation would be better served by meaningful public-private partnerships established to assist organisations in building their internal capabilities and facilitating the sharing of threat intelligence, both of which will develop sector-wide maturity in how organisations manage their responses to, and contain, incidents.

While Microsoft accepts that, on balance, the benefit of Government intervention for some entities may outweigh these risks, Microsoft believes that this is not the case for many organisations that comprise the critical data storage or processing sector. We therefore call for clear exemptions from Government intervention for entities that have a demonstrated history of working cooperatively and in good faith with the Government to secure Australian industry, who operate highly sophisticated and complex systems, and who are committed to substantial ongoing investment in security and risk mitigation.

2. Revise notification obligations for all cyber security incidents for clarity and to prioritise containment and remediation

In Microsoft's view, as currently drafted, the cyber incident reporting obligations under the Proposed Legislation should be clarified. The concepts which trigger reporting obligations under the Proposed Legislation, such as "cyber security incident" and "significant impact", are ambiguous and also differ from incident reporting requirements in other industries and jurisdictions. Without clarity and consistency, there is a real likelihood that this may result in unnecessary and immaterial notifications to the Government, particularly from hyperscale cloud service providers like Microsoft whose services are designed to continue to operate even when any particular asset becomes unavailable. Moreover, without international and sectoral harmonisation, organisations risk spending critical time deciphering differing mandates and reporting requirements. A patchwork of inconsistent or redundant obligations will debilitate organisations of all sizes.

Microsoft also urges the Committee to revise the 12-hour reporting timeframe proposed for critical cyber security incidents. This timeframe is impractically short and allocates organisational resources away from containment and remediation efforts during the most critical response period for an impacted organisation. Moreover, the obligation prioritises compliance over responding to and gathering of meaningful information concerning the incident which should be of higher priority to the Government in building a clearer picture of the threat environment in order to assist other organisations.

We believe a no-later-than 72-hour reporting threshold balances the need for transparency and visibility while permitting an organisation to prioritise containment and remediation. The justification for this truncated reporting window within the Explanatory Memorandum does not reflect the practical experience of organisations responding to cyber incidents.

3. Push to prioritise regulatory harmonisation and provide certainty for organisations subject to competing or duplicative obligations

"Data storage or processing service" providers operate horizontally across industries and support other regulated critical infrastructure sectors. We therefore urge the Committee, and the Government more

broadly, to ensure regulatory harmonisation across sectors and across jurisdictions so that organisations will not be subject to duplicative and/or conflicting regulations.

Given the risk of duplicative and inconsistent obligations, Microsoft believes it is imperative that the Proposed Legislation detail who has the ultimate authority to set baseline requirements and to resolve conflicts arising from cross-sector obligations. If the Department of Home Affairs is positioned to undertake this responsibility, it should be explicitly given this authority under the Proposed Legislation to proactively map and deconflict areas of concern.

The areas of potentially conflicting regulatory obligations exist not only across industries, but across jurisdictions. We therefore underscore the need for the Proposed Legislation and the resulting requirements to leverage existing global baselines, standards and certifications. While Microsoft supports the aims of this important reform, it is important that the resulting framework capitalise on the significant existing domestic investment and organisational expertise which have developed around current cyber security frameworks. This is particularly important given that many organisations may be responsible for regulated assets in multiple critical infrastructure sectors and/or provide services regionally or globally. The introduction of additional and unnecessary complexity to organisational risk management functions is likely to undermine the effectiveness of the proposed organisational risk management programs, as well as existing risk management protocols and procedures.

* * *

As Australia's reliance on cloud services increases, so too does the importance of these services to Australia's national interest and the attractiveness of these services to malicious actors. The Committee, like Microsoft, will no doubt be aware of a worsening global threat environment and increasing frequency of significant cyber-attacks on critical infrastructure at home and abroad.

Microsoft believes it is imperative that the Committee take the opportunity provided by this review to consider the issues raised by Microsoft and other cloud service providers in advance of the passage of the Proposed Legislation. We believe implementing the revisions we have proposed will ensure the efficacy and durability of these important reforms and better align public and private interests in protecting our shared critical infrastructure.

Microsoft continues to stand ready to assist the Committee and the Government in protecting Australia's digital security.