Microsoft Submission in Response to Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Microsoft welcomes the Australian Government's continued engagement with industry on further measures to secure Australia's critical infrastructure. As noted in our February 2021 submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) (PJCIS Submission) and June 2021 testimony before that Committee (PJCIS Testimony) regarding the then-proposed *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (Original Bill), Microsoft recognises the importance of public-private partnerships in developing and implementing these critical reforms to cyber risk management. Microsoft remains committed to partnering with the Government to improve Australian cybersecurity and contributing our experience as a leading global cloud services provider.

We respectfully offer the following submission in response to the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (Bill Two). This submission builds on our prior contributions to public consultation on the current program of reforms to the *Security of Critical Infrastructure Act 2018* (Cth) and associated legislative instruments, including the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth). We appreciate the Government's consideration of the issues detailed below and welcome additional opportunities to discuss the further refinement of Bill Two in advance of its passage into law.

SYSTEMS OF NATIONAL SIGNIFICANCE: IDENTIFICATION (PART 6A) AND ENHANCED CYBERSECURITY OBLIGATIONS (PART 2C)

Part 6A of Bill Two carries forward the powers proposed under Section 52B of the Original Bill for the Minister to declare regulated assets critical to the security, economy, and sovereignty of Australia as a System of National Significance (SoNS). This designation also empowers the Secretary of Home Affairs to impose a broad range of additional cybersecurity obligations under Part 2C of Bill Two, including the adoption and maintenance of statutory incident response plans, mandatory cybersecurity exercises undertaken under the supervision of Government officials, vulnerability assessments, and access to or reporting of system information, which may require the installation of software provided by the Australian Government in some cases.

Microsoft reiterates our significant concern over the security and privacy implications of several aspects of Part 2C powers. As noted in our PJCIS Submission and PJCIS Testimony, the introduction of untested third-party software into a cloud service provider's systems creates real and serious risks of collateral consequences that could interrupt critical services. Microsoft believes that the risks of Government intervention far outweigh any potential benefits for many critical data storage and processing sector participants, particularly parties with established histories of cooperation with the Government and complex architectures

such as hyperscale providers. While we welcome the Government's statements that these powers are not intended to be used on providers of Microsoft's size, scale, and sophistication, we strongly encourage the Government to clearly articulate this in the legislation and the guidance material that will be released by the Department of Home Affairs.

The Minister should clearly define and limit the assets subject to a SoNS to those strictly qualifying under the national significance test. Given the structural interdependencies in cloud service assets, the Secretary should also limit the application of Part 2C powers to the narrowest set of assets required to satisfy the objectives of the legislation. Should Microsoft be designated as a SoNS, the Government should acknowledge Microsoft's existing cybersecurity capabilities in lieu of imposing duplicative or additional obligations under Part 2C.

GOVERNMENT-MANDATED CYBERSECURITY REQUIREMENTS SHOULD BE CONSISTENT AND INTEROPERABLE ACROSS SECTORS AND INCORPORATE INTERNATIONAL STANDARDS AND BEST PRACTICES

In our PJCIS Submission, we advocated that the legislation should recognise established global cybersecurity frameworks implemented by regulated entities, including relevant international standards and best practices. In our PJCIS Testimony, we explained that a failure to leverage existing frameworks may lead to duplicative or inconsistent obligations on data storage or processing service providers. This threatens to (a) divert providers' security resources toward formalistic compliance exercises; (b) drive up the complexity of compliance and enforcement; (c) undermine providers' ability to comply across jurisdictions; and (d) inhibit the ability of small and medium-sized businesses to access opportunities across the global economy. Microsoft recommended that the proposed reforms strive for consistency and interoperability across sectors and across jurisdictions by leveraging existing international frameworks and definitions. This approach was endorsed by other sector representatives appearing before that Committee. Microsoft continues to recommend this approach today.

However, the Exposure Draft of Bill Two does not require the Minister to consider existing regulatory frameworks outside of obligations imposed by the Commonwealth or a State or Territory Government, or recognised by Standards Australia, in specifying rules for a critical infrastructure Risk Management Program following consultation. Microsoft urges the Government to broaden the scope of items that the Minister must consider prior to rulemaking to include recognised global frameworks and standards.

Relevant international cybersecurity standards and best practice frameworks that support cross-sector and cross-region interoperability and consistency include ISO/IEC 27110: 2021, *Cybersecurity framework development guidelines*, which specifies guidelines for developing

a cybersecurity framework and is designed to be applicable across sizes and types of organisations; ISO/IEC 27103: 2018, *Cybersecurity and ISO and IEC Standards*, which provides guidance on how to leverage existing international standards in a cybersecurity framework; and the *Framework for Improving Critical Infrastructure Cybersecurity*, the latest version of which was published by the U.S. National Institute of Standards and Technology (NIST) in 2018 and for which a forthcoming update is planned with global stakeholders to capture risks and best practices that have become heightened or have emerged in the intervening years. We urge the Australian government to consider these existing standards and best practices and incorporate them into the national critical infrastructure regulatory framework.

Adopt outcome-focused standards to mitigate risk and respond to threats

Microsoft also continues to advocate for flexible and outcome-focused cybersecurity frameworks and practices with respect to reforms deferred to Bill Two, which we believe provide the best means for organisations to prioritise risk and navigate a rapidly changing technological and cyber threat environment.

Microsoft is encouraged by the Government's adoption of a principles-based approach as reflected in the Part 2A Risk Management Program Positive Security Obligations. In particular, Microsoft appreciates that rulemaking regarding Risk Management Programs may recognise that existing industry standards and practices are sufficiently protective to satisfy the Part 2A obligations. Leveraging existing standards and best practices will benefit Australian customers by reducing risks and by reducing the cost and complexity of compliance.

Cooperate with industry to develop standards

As noted in our PJCIS Submission, Microsoft also welcomes the opportunity to participate in the development of "data storage or processing" sector rulemaking, as well as rules impacting other critical infrastructure sectors. Microsoft and other cloud providers increasingly operate horizontally across the Australian economy and can assist in realising the Government's stated aims of de-conflicting requirements, minimising the complexity of compliance, and reducing the overall administrative burden for the Government. As noted above, the Government can best accomplish these goals by leveraging global standards and best practices. Doing so would not only streamline compliance for all entities (including cloud service providers and small- and medium-sized businesses) but would also advance global efforts to better protect national critical infrastructure. The Government aligning the definition of "data storage or processing" with international definitions—such as those used by NIST and the EU's NIS Directive—is a step forward, and providers like Microsoft can assist the Government in further harmonising the legislation and resulting regulatory framework with global best practices.

Streamline with existing regulations

Microsoft additionally welcomes the Government's continued intention to recognise and build on existing frameworks to minimise the regulatory burden on impacted entities in Bill Two, as exemplified by its retention of public interest criteria for Part 2A rulemaking regarding Risk Management Programs.

The Government will need to proactively identify areas of duplication in existing regulatory requirements that impose equivalent protections to those contemplated under Part 2A to support this approach. We therefore encourage the Government to undertake a regulatory mapping exercise to determine areas of duplication and assist the Minister in applying the relevant public interest criteria to decisions regarding rulemaking.

Regulatory mapping is particularly important for cloud service providers who have pre-existing relationships with Australian Government customers and that have already invested in certification under the Information Security Registered Assessor Program (IRAP). IRAP certification based on the *Anatomy of a Cloud Assessment and Authorisation* is already informed by the Government's best cybersecurity guidance in the form of the Information Security Manual and Protective Security Policy Framework. Recognition of an IRAP certification through a carve-out or safe harbour framework will avoid unnecessary administrative and compliance burdens and reduce the scope and duration of industry consultation required to adequately assess rulemaking.

MICROSOFT'S UNIQUE POSITION AS A HYPERSCALE CLOUD SERVICES PROVIDER

Microsoft appreciates the Government's recognition of the substantial investments sophisticated hyperscale cloud providers like Microsoft make in providing secure and resilient services, maintaining the technical expertise necessary to respond to and remediate cyber incidents, and sourcing the latest threat intelligence. In our PJCIS Testimony, we stressed that Microsoft is already in the business of bolstering the security of our critical infrastructure customers. Maintaining a secure and reliable service is as important to our success as it is to our customers. Microsoft was, therefore, encouraged by discussion before that Committee that queried the necessity of applying *all* elements of the Government's cyber uplift policy to sophisticated cloud providers. We urge the Government to recognise the unique role of hyperscale providers and reflect that position in its forthcoming guidance.

Microsoft supports the Government's objective to increase cyber resilience across the Australian economy by establishing and maintaining a sector-wide baseline for the data storage and processing sector, as participants in this sector have varying degrees of security investments and risk management maturity. Microsoft welcomes greater scrutiny of investments made by sector participants and urges the Government to avoid concessions for participants who fail to establish the necessary security infrastructure or expertise

required to protect their customers and Australia's increasingly complex digital supply chains.

RISK MANAGEMENT PROGRAM (PART 2A)

Microsoft appreciates the stated intention of the Government in the Explanatory Document to Bill Two to build on existing regulatory frameworks, deconflict existing obligations and minimise the regulatory and compliance burden on industry. This commitment is particularly relevant both for the activation of Part 2A Risk Management Program obligations and the design of rules determining program requirements that may apply to specific classes of critical infrastructure assets.

Although discussion regarding more detailed requirements applying to "data storage or processing sector" assets has been deferred, Microsoft wishes to underscore our ongoing investments in existing risk management certifications, including those established for satisfying the requirements of Australian Government customers.

As a Certified Strategic provider under the Digital Transformation Agency's Hosting Certification Framework (HCF) for all 180 core online services, Microsoft is the only provider that is currently certified for IaaS, PaaS and SaaS under the HCF. Microsoft believes entities meeting the higher levels of risk management obligations imposed by Government customers through HCF are appropriate candidates for exemption from the activation of Part 2A requirements. As we have suggested, the proactive mapping of existing regulatory scheme requirements against the proposed Part 2A obligations will provide comfort to industry while also reducing the implementation timeline for the resulting rules.

INFORMATION SHARING PROVISIONS FOR REGULATED ENTITIES

Consistent with Microsoft's commitment to strengthening public-private partnerships in the service of achieving shared cybersecurity objectives, Microsoft wishes to deepen existing cyber incident and threat intelligence-sharing partnerships with the Australian Government. Voluntary cooperation between partners provides the best security outcomes while also reducing reliance on rigid and prescriptive legislated obligations.

EXPANSION OF LIABILITY PROTECTIONS

Microsoft welcomes the provision of statutory liability exemptions where Microsoft acts in accordance with Government instructions pursuant to government intervention powers. That said, we are concerned that these provisions do not consider or resolve the attendant risk of additional harm to our customers or harm arising from reputational damage to Microsoft, neither of which are easily quantifiable and may exceed the loss of business from a specific impacted customer.

Microsoft therefore also has concerns regarding the 'good faith' qualifier as a precondition of an exemption from liability in these circumstances. It is currently unclear what constitutes good faith and whether protections would be forfeited in the event Microsoft exercised available legal remedies to enjoin certain government interventions that we may believe are inappropriate. A liability exemption that requires an organisation to forfeit fundamental legal rights and remedies or negotiate a preferred course of action under the legislation would be deeply problematic. Microsoft urges the Government to clarify the intended applicability of the 'good faith' standard and ensure that it does not undermine an entity's legal rights.

DEFINITION OF CRITICAL INFRASTRUCTURE RISK MANAGEMENT PROGRAM

As noted in our PJCIS Submission, Bill 2 defines "critical infrastructure risk management program" as a written program that entities responsible for critical infrastructure assets use to "*identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset*." This language could be clarified to give more specific instruction to entities regarding the identification of hazards. Foundationally, Australia should have a clear articulation of national risks and priorities, and the *functions* that it seeks to protect at a national level. Those should guide how responsible entities assess their risks, with a clear understanding of national confidentiality, integrity, and availability priorities. That articulation assists responsible entities to set priorities and manage risks or hazards that occur.

The fact that a hazard "*could have an impact on an asset*" is potentially overbroad as a standard. As noted above, assets themselves become less relevant in a cloud-based environment, where risk is assessed and managed at the functional level. If the function remains available, then reliability- and resiliency-related risks are managed. The material risk that a hazard could impact an asset – a server, for example – becomes less meaningful when the cloud can shift workloads dynamically. If the focus of the risk management conversation is about the confidentiality, availability, or integrity of a data centre as an "asset," then the definition needs to be more specific as to the appropriate scope of a risk management plan.

Microsoft recommends that this language should clarify that entities should only be expected to identify those hazards that are *reasonably foreseeable* with a focus on critical *functions*, not assets. This modest revision will provide more appropriate instruction to entities as they work to identify risks and is consistent with the definition's analogous obligation that a critical infrastructure risk management program should minimise or eliminate any material risk of such a hazard occurring "so far as it is reasonably practicable to do so."

CONCLUSION

Microsoft commends the Government on its continuing engagement with industry on efforts to refine Australia's ongoing critical cybersecurity reforms. Given the deferment of substantial components of the Original Bill in accordance with PJCIS recommendations, continuing consultation on the proposed reforms remains critical to the success of the Government's cybersecurity uplift policy.

Microsoft appreciates the Government's review of this submission and welcomes further opportunities to contribute our substantial experience as a trusted provider of critical technology services across many sectors of the Australian economy. We are well positioned to contribute meaningfully to future discussions, particularly those concerning pragmatic and effective data storage and processing sector rulemaking.

We once again thank the Government for the opportunity to respond to the Exposure Draft of Bill Two and reaffirm our commitment to being a productive security partner of the Government and the Australian people.