Microsoft

Microsoft Submission to the PJCIS Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

Microsoft commends the Australian Government's efforts to improve the security of critical infrastructure and appreciates the opportunity to provide feedback to the Parliamentary Joint Committee on Intelligence and Security (the "PJCIS") on the proposed Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the "Proposed Legislation"). The comments offered here draw from our experience as an industry leader in security investments and a hyperscale provider of cloud services across the Australian economy and globally.

At the outset, we note the considerable effort that the Government has put forth to understand and address the complex challenges associated with securing critical infrastructure in an era of digital transformation. The Proposed Legislation properly recognises that risk management and public-private partnerships are central to ensuring the availability, reliability, and integrity of critical infrastructure. The Proposed Legislation and the accompanying explanatory memorandum (the "Explanatory Memorandum") also indicate that the Government recognises the importance of flexible, risk-based assessments; leveraging global standards; and ensuring the interoperability and deconflicting of security requirements across critical infrastructure sectors.

As we noted in our engagement with the Department of Home Affairs a few months ago, the Proposed Legislation is complex. Identifying and prioritising national risks, facilitating interoperable approaches across sectors, and exploring appropriate Government responses to significant events are massive undertakings. The protection of essential services for Australians, some physical and many based online, enhances the complexity and the need for a clear articulation of national priorities and risk. We greatly appreciate the PJCIS considering our recommendations on the Proposed Legislation and urge the Committee to incorporate additional rounds of feedback as it studies the legislation. As the legislative process moves forward, reasonable timetables that allow for robust input, ideally over several waves of exchange, will help to ensure that both public and private sector stakeholders understand the impacts of and are prepared to operationalise requirements. Similarly, throughout the process of implementing the resultant legislation, it is imperative that there be meaningful exchange and consultation with relevant stakeholders – such as through a 60-day comment period on draft sector-specific requirements.

With regard to the Proposed Legislation, Microsoft respectfully offers the feedback detailed below to the PJCIS. While we appreciate and commend the Australian Government's efforts to address these important issues in a nuanced and thoughtful manner, several aspects of the

Proposed Legislation could be improved, raise issues of serious concern or could unintentionally make Australia's security posture less secure. We welcome the opportunity to further engage with the PJCIS and the Australian Government more broadly on these important issues and offer our perspective on any alternative proposals for effectively addressing security and resiliency priorities.

Among the various important items discussed in more detail in this Memorandum, Microsoft would like to specifically highlight the following critical requests to the PJCIS:

- The Proposed Legislation should reflect cognizance of existing international cybersecurity standards, best practices and regulations and put forward an approach that will be consistently applied across various sectors, enabling streamlining with existing regulations, avoiding conflicting or duplicative regulations, and supporting interoperable approaches across interdependent sectors.

- The Proposed Legislation should not permit the Government to mandate the installation of software on operator systems, as such software could result in interoperability, vulnerability management and maintenance challenges, while introducing additional risk and undermining the security of these systems.

- The incident reporting requirements in the Proposed Legislation should be modified to provide for a 72-hour reporting window for *all* cybersecurity incidents, including those with "significant impact," which is the reporting window most frequently prescribed in security regulations, and allows an organisation to focus solely on containing and remediating malicious activity during the initial phase of incident response as opposed to shifting resources during this critical window where the full extent of hostile activity is typically not yet understood.

- The focus of the Proposed Legislation should recognise the importance of maintaining the relevant essential functions and not the underlying assets.

MICROSOFT'S RECOMMENDATIONS

I. GOVERNMENT MANDATED CYBER SECURITY REQUIREMENTS SHOULD BE HARMONISED ACROSS SECTORS AND INCORPORATE INTERNATIONAL STANDARDS & BEST PRACTICES

Adopt Outcomes-Focused Standards to Mitigate Risk and Respond to Threats

Microsoft has consistently advocated for a flexible, outcomes-focused approach to cyber security frameworks and use of standards, enabling risk prioritization and agility to respond to a dynamic threat environment and changing technology landscape.[1] We appreciate that the Australian Government has adopted a similar approach, which we believe is reflected in the Positive Security Obligations. Outcome-based standards allow enterprises to be flexible in adapting and responding to evolving threats, including by leveraging new security capabilities. They also allow organisations to leverage common, cross-sector security baselines that not only reduce risk, but also reduce the complexity and cost of compliance, ultimately enabling more resources to be directed toward security operations and network defense.

Cooperate with Industry to Develop Standards

We appreciate that the Proposed Legislation and Explanatory Memorandum also indicate that sector-specific standards will be co-designed with industry, and we encourage the Government to holistically ensure cross-sector interoperability of standards. As part of this process, we would welcome the opportunity to participate in the development of any sector-specific standards that are co-designed with input from technology providers and with other sectors for which we provide services that will be impacted by those standards.

In previous comments, Microsoft has also emphasised that domestic frameworks and standards should leverage existing global baselines, standards, and certifications to the greatest extent practicable. Doing so would greatly alleviate the risk of duplicative and/or conflicting requirements – not only across sectors, but also across jurisdictions – and increase market access. Technology providers – and hyperscale cloud providers in particular – often operate global services that leverage global security standards and international best practices. In addition, among those operating domestic services, leveraging global standards and best practices eases integration into global supply chains, especially as global providers increasingly improve their supply chain security by requiring downstream suppliers to meet consistent requirements. Moreover, global standards and best practices reflect broad input and experiences on managing threats and securing infrastructure, services, and operations. The Government can enable domestic providers to access global technology and integrate into global supply chains by supporting the development of and leveraging global standards and

[1] *See* http://download.microsoft.com/download/4/6/0/46041159-48FB-464A-B92A-80A2E30B78F3/MS-riskmanagement-securitybaselines-WEB.pdf

best practices. Existing best practices and international standards provide useful frameworks for cross-sector baselines, and they support cross-region and cross-sector interoperability, including: ISO/IEC 27101; ISO/IEC 27103; and the *Framework for Improving Critical Infrastructure Cybersecurity* (commonly referred to as the NIST Cybersecurity Framework).

Streamline with Existing Regulations

Similarly, we believe the Government can avoid duplication and promote efficiency (for organisations and for the Government) by mapping existing Australian regulatory requirements and security obligations and then supplementing those requirements as necessary. Many providers of cloud services, for example, have invested in Australian certification programs such as the Information Security Registered Assessor Program (IRAP), which allows providers to serve Government customers. Leveraging the requirements associated with this certification regime, for example, could avoid unnecessary administrative and compliance burdens.

II. GOVERNMENT INTERVENTION AUTHORITIES MUST BE CAREFULLY DEFINED AND RESTRICTED AND SHOULD NOT BE USED WHEN ORGANISATIONS ARE CAPABLE OF MANAGING RESPONSE & RECOVERY OF THEIR OWN NETWORKS

Direct Governmental Intervention Undermines Objectives of Proposed Legislation

The Proposed Legislation gives the Government authority to intervene in certain circumstances involving serious cyber security incidents. Microsoft has significant concerns about this authority and would welcome the opportunity to better understand specific risks the Government seeks to address as well as discuss alternative solutions that introduce less risk.

As an initial matter, Microsoft recognises the Government's interest in ensuring that critical assets can withstand major cyber incidents and that appropriate remediation tactics can be quickly deployed in the event of an incident. However, we believe that a policy allowing for direct governmental intervention would undermine the Government's objectives of defence and recovery. Rather, in many cases, it is the individual organisations themselves, and not the Government, that are best positioned to determine how to appropriately respond to and mitigate the impact of cyber incidents. This is because an individual organisation is more familiar with its own unique network and its configuration, risk profile, threat environment, security policies, customers, and cyber capabilities than is the Government. It would take a preclusive amount of time for the Government to come into a live incident, properly understand the fact pattern, the technologies in play and the challenges of any decisions, and then be able to direct an appropriate response. This contributes to what military strategists have referred to as the "Fog of War," which is a concept that has been applied to cyber incident response, where additional risk is introduced during the initial phases of an ongoing crisis because the ability for subject matter experts and network defenders to adequately respond is

hampered by an onslaught of information requests, speculation, and well-intended ideas from individuals or organisations, when the malicious activity is yet to be fully understood by anyone.

Further complicating any such operation is the fact that the Government would be doing so without a thorough understanding of the specific resources and protocols available for deployment, and that the resources required to obtain such knowledge would be prohibitively expensive, logistically complicated, and amount to an extremely invasive governmental intervention. As such, the danger of having a government direct a private sector entity's response without complete knowledge of the situation and the technology cannot be understated. Moreover, individual organisations are not only best positioned to respond; they also have as equal an incentive as the Government to protect their own networks and maintain the trust of their customers. Risk of unilateral intervention by the Government greatly increases the risk of unintended collateral consequences, impacting customers directly and indirectly by undermining trust, and threatens to make entities less secure.

We recognise that the Proposed Legislation requires that, prior to issuing a Ministerial authorisation for an intervention, the Minister must be satisfied that the relevant entity is unwilling or unable to take reasonable steps to respond to a particular incident. While we appreciate that this is intended to establish a baseline procedure for cases of intervention, we believe the Government's objectives would be better served by withdrawing this authority and establishing a public-private partnership to help organisations build their defence and response capacities.

Government Should Identify Clear Procedures and Assume Full Liability in cases of Intervention

If the Government nonetheless believes it must retain authority to intervene in situations of extraordinary national emergency, we urge the Government to work with organisations in a transparent and iterative consultation process to help establish the procedures that will be used to determine on a case-by-case basis whether an entity is indeed unwilling or incapable of meeting the baseline requirements for security and response. The Government should clarify in advance the processes organisations must have in place to manage response without intervention and commit to working through public-private partnership rather than intervention if those processes are established and activated in response to an event. Consistent with the principles of due process, there should also be a fair process to appeal decisions about sufficiency of response processes.

In light of the attendant risk of unintended collateral consequences resulting from governmental intervention, the Government should also be prepared to assume full liability by indemnifying organisations for any collateral harm caused by its intervention. The Government should immediately begin to clarify how this authority would work in a crisis, so that chaos is not added to a national emergency with new individuals and processes being introduced "on

the fly," thereby initiating the "fog of war" risk and impact we describe above. In addition, impacted entities should have appropriate due process and transparency, which should include the right to contest or appeal Government intervention, requests for information, or any orders that would direct an organisation to undertake a specific action. We recognise the limited protections from liability for damages when operating under Ministerial Direction afforded under applicable Australian law, but we believe these protections are too narrow in scope. Our recommendation remains, however, that the Government consider withdrawing altogether this authority from the Proposed Legislation.

III. Recognise the Unique Characteristics of the "Data Storage or Processing Sector" in order to Facilitate More Effective Threat Assessments & Risk Management

Data Storage or Processing, Generally

The "Critical Data Storage or Processing Sector" is currently defined as the sector of the Australian economy that involves providing data storage or processing services, and "data storage or processing service" within the context of the Proposed Legislation means a service that enables end-users to store or back-up data, or a data processing service. The proposed definition encompasses three types of cloud services (IaaS, PaaS, and SaaS) as well as the management of data centres and other cloud infrastructure.

Microsoft understands the Australian Government's desire to ensure that this sector leverages appropriate risk management steps. Cloud services and data centre operations offer important support to their respective customers. Providing these services demands sophisticated risk management, robust implementation of security controls, and continuous monitoring to ensure the integrity and availability of services.

However, we believe two structural aspects of the Government's proposed approach toward this broadly defined sector should be reassessed and addressed.

Distinguish between Cloud Services and Data Centre Operations

First, we encourage the Government to consider important distinctions between cloud services and data centre operations and to reflect those distinctions in legislative designations and sector-specific implementation efforts. Whereas cloud services are computing systems and software that are logically separated from the physical hardware that run within data centre environments, data centres are tied to a specific geographic location, and data centre operators focus on securing a physical asset. Recognising and reflecting these differences will allow the Government to focus on distinct risks and risk management steps relevant for each category, ultimately driving more prioritised and effective efforts to enhance security and resiliency.

The key difference between traditional information technology (IT) environments such as data centres and cloud services is that the IT resources and services underpinning cloud services are not necessarily tied to one physical location. As such, focusing on the functions that cloud services provide – such as storage, compute, security, or collaboration functions – is more relevant and important than focusing on physical assets. This distinction is even more true for *hyperscale* cloud providers, which maintain and distribute services across multiple data centre sites to ensure continuity of service delivery. Hyperscale providers often operate geographically distributed networks that enhance the resiliency and availability of the services they provide. Given the nature of their services and networks, hyperscale cloud providers also invest significantly greater resources in proactively addressing software vulnerabilities and preventing unauthorised virtual access to networks and sensitive data.

Conversely, data centres and the services they provide are tied to one physical location. As a result, the risks to data centres can be differentiated from those impacting cloud services; they are often connected to physical controls, personnel access, and continued supply of energy and telecommunications network connectivity. Notably, while providers of cloud services are often *customers* of data centre operators, it is not uncommon for a data centre to provide infrastructure for several cloud service providers from a single location.

Combining cloud services and cloud infrastructure (data centres) into one sector without acknowledging and addressing these distinctions risks creating confusion and regulatory misalignment. Separate designations for these two categories of assets within the broadly defined "data storage or processing" sector would allow the Government to identify risks and develop regulatory requirements that are more specific, appropriately tailored, and manageable for the operators of critical functions, services, or assets. Ultimately, even if these two categories are combined together, it will be important for the Department of Home Affairs to tailor regulations specifically to the respective sub-categories and ensure maximum efficacy and protection for each.

Department of Home Affairs is Regulator Primarily Responsible for Critical Data Storage or Processing Sector

Second, we urge the Australian Government to recognise the unique nature of the "data storage or processing sector". To a greater extent than many other sectors, entities providing cloud services operate *horizontally* across the Australian economy and serve critical infrastructure operators in most if not all sectors. The regulatory framework set forth under the Proposed Legislation creates a real risk that providers of cloud services and data centre infrastructure may face regulation across *several* critical infrastructure verticals and through *several* unique sector-specific requirements.

We appreciate that in the absence of a designated regulator, the Department of Home Affairs will serve as the default regulator. Given the broad regulatory mandate, it will be imperative for the Government to expressly ensure that the Department of Home Affairs is primarily responsible for overseeing the "critical data storage or processing" sector, and has overarching authority to set baseline requirements and authority to harmonise and deconflict requirements that may be imposed from other sector-specific regulators. Assuming this is accomplished, we think that having the Department of Home Affairs serve as the single primarily regulatory body makes sense as it can more effectively drive harmonisation of the applicable regulations and ensure equal enforcement thereof across the various verticals.

Lastly, it is essential to note that once the Department of Home Affairs is confirmed as the primary regulator, it will need to engage in a sector-wide risk assessment in order to understand the risks and critical functions of the sector. As the Government knows well, not all data will be critical. Without a clear articulation at the national level of the essential functions that Australia seeks to protect, individual organisations will have difficulty identifying and prioritising risk. This will decrease the effectiveness of risk management plans and security baselines. Understanding what functions are essential will enable a hyperscale cloud provider, for example, to work with its customers in critical infrastructures and evaluate for itself what is truly critical.

IV. Clearly Identify "Systems of National Significance" and Only Exercise Government Authority over Assets that Require Attention

Systems of National Significance, Generally

Section 52B of the Proposed Legislation outlines the process for designating an asset as a "system of national significance." This designation carries with it substantially enhanced cyber security requirements and obligations. The responsible entity for a system of national significance may be subject to incident response planning obligations, mandatory participation in cyber security exercises, required vulnerability assessments, and, where the designation relates to a computer system, the responsible entity could be required to provide periodic or event-based reports of system information. Moreover, the Proposed Legislation indicates that a responsible entity for such a computer system could be required to allow for the installation of software that transmits system information to the Australian government – a proposal that (as explained further below) Microsoft strongly opposes.

Microsoft urges the Australian government to re-evaluate several aspects of this proposal.

Focus on Protection of Critical Functions, Not Assets

First, Microsoft recommends that the Australian government consider an approach that identifies the functions that must be protected and preserved, regardless of the network,

system, or asset used to provide it. Protecting those functions becomes the foundation for a national risk management program and enables companies to incorporate the management of that risk into their own corporate processes. We believe it is the essential building block for this approach to be successful. This begins by identifying the critical functions of Australian life that must be preserved by critical infrastructure, then identifying the systems and assets needed to support those functions. This exercise should be a cooperative endeavour between the Government and operators and provide sufficient time for careful consideration of input from the responsible entities relevant to the function, asset, or system. To that end, Microsoft recommends that the period of time allotted for responsible entities to provide initial submissions on a system of national significance designation be extended from the proposed 28 days to at least 56 days. This additional time would not only allow for more thoughtful submissions from responsible parties but also provide a meaningful opportunity for the exchange of information between the Government and the responsible entity on the Government's intent and desired security outcomes and ways to appropriately scope a designation and its impact in response. Additional time may be needed to ensure that "systems of national significance" clearly identify *functions* of national significance, so that each sector can assess what is "critical" from a system or asset perspective once that baseline is set.

Adopt a Flexible and Tailored Approach to Security Obligations

Second, where the Government designates a system of national significance, a logical, flexible approach to imposing enhanced cyber security obligations is critical to meeting the Government's risk management needs in a way that also leverages and reflects private sector capabilities and responsibilities. Instead of a one-size-fits-all approach to government exercises or vulnerability assessments, enhanced security obligations that are tailored to Government needs and provider sophistication can incorporate responsible entities' existing, mature risk management plans and robust security controls. Operators like Microsoft, for example, provide services that anticipate and surpass our (as well as our customers') security compliance requirements, and devote significant time and resources to developing extensive cyber security protocols and delivering response and recovery capabilities. If a mature organisation with sophisticated risk management and security controls were to be impacted by a designation of a system of national significance, we would urge the Government to partner with the entity and build on voluntary cooperation and engagement, thereby only imposing obligations on entities as necessary to address significant ongoing risks in a way that is consistent with private sector responsibilities. To structure a logical, flexible approach, we also recommend that the Government consider developing a mechanism and process by which entities could be given a "statement of compliance" if the entity can demonstrate that it meets high risk management, security, and recoverability thresholds that protect the functions of national significance. The benefit of this approach is twofold: the option to be exempted would reward operators that meet or surpass the cyber security standards, and it would allow the Government to focus its own risk management and response resources in a more targeted

way on systems of national significance that require protection and continued attention. We recommend that exemptions be allowed where, for example, an operator can demonstrate that it can: (i) meet the Government's incident reporting requirements within a specified time period; (ii) respond to requests for information in a timely manner; and (iii) implement certain incident response and recovery capabilities at a level acceptable to the Government.

Respect and Protect Privacy and Security of Information

Third, with respect to any information reporting requirements, to avoid the risk of undercutting privacy and security for end users, technical detail about an incident should only be required where the customer's existing contractual rights, privacy obligations, and other relevant obligations do not prohibit (and expressly allow for) the sharing of such information. This proposed approach is consistent with the manner in which entities share information today under the EU National Information Sharing Directive ("EU NIS Directive"). Operators must retain some autonomy and discretion in order to ensure that disclosure of information is consistent with contractual obligations and applicable law in other jurisdictions.

Installation of Third-Party Software Undermines Security Objectives of Proposed Legislation

Finally, and most significantly, Microsoft strongly opposes any authority that would grant the Australian Government the ability to compel installation of software or devices of any kind on its networks, systems, or assets. We believe this authority, however narrow and theoretical, is misguided and urge the government to reconsider. Inclusion of third-party software on an operator's network – particularly on the operator of a hyperscale cloud service – threatens to compromise the security and integrity of the network and creates additional points of vulnerability for the asset, function, or service that the Government is seeking to protect. The introduction of any third-party device or software that the operator has not developed, tested or vetted will harm the safe and reliable operation of the system, thereby undermining the principal goals of the Proposed Legislation. We also note that the failure to maintain, update and patch software remains the most common cause of cyber incidents, even for significant cyber espionage and attack activity. The Government should seek to enhance the security posture of critical infrastructure operators through public-private partnership, enhanced education, and two-way models for sharing threat information. Even the possibility of compelled installation of software or devices that transmit signals back to the Government threatens to undermine trust, integrity, and security of the very networks the Government is seeking to protect. We believe this to be the case for any system of national significance as currently defined, or against any function of national significance. Direct government access to the network, systems, and assets of data is a dangerous precedent and introduces risk to Australians worldwide.

V. CLARIFYING CERTAIN DEFINITIONS IN THE PROPOSED LEGISLATION

The Proposed Legislation could be improved by clarifying certain key definitions. Doing so would avoid potentially overbroad regulation and focus attention more clearly on assets that warrant greater attention.

Critical

One of the most important terms used in the context of the Proposed Legislation is the term "critical." Although it is used with regard to critical assets, critical sectors, and critical infrastructure, the Proposed Legislation does not define what is critical to Australia. We believe further explicating what is critical to Australia will greatly benefit the entire legislative and regulatory framework.

The Explanatory Memorandum, paraphrasing amended section 9, states:

> Critical infrastructure assets across each sector have been identified through an assessment of criticality to the social or economic stability of Australia or its people, the defence of Australia, or national security. In particular, considerations include, but are not limited to, whether, if destroyed, degraded, or rendered unavailable, there would be a significant detrimental impact on:
>
> - maintaining basic living standards for the Australian population – this includes those essential services and other services without which the safety, health or welfare of the Australian community or a large section of the community would be endangered or seriously prejudiced;
> - industries, commercial entities and financial institutions that underpin Australia's wealth and prosperity;
> - the security of large or sensitive data holdings which, if undermined, could lead to the theft of personal or commercially sensitive information, intellectual property or trade secrets, and national security and defence capabilities.

This comes closest to an articulation of what functions the Government deems critical, but more is needed. A more specific articulation and focus on the critical functions supporting Australian society is essential to any organisation's effort to track and manage the networks, systems, and assets required to enable and maintain that function. In a crisis, relying on a clear articulation of essential national functions and a process to manage risks to those functions will be critical to the success of securing Australian national infrastructure. It is the foundation for this work.

Business Critical Data

We urge the Government to consider narrowing the scope of impacted cloud services and data centres, with more focus on risks and functions of heightened concern. The Government might consider narrowing the scope of impacted cloud services to those that provide more important functions to other critical infrastructure sectors, enabling a focus on cascading risks. In addition, the Government could narrow the definition of business critical data. As noted in the Explanatory Memorandum, 'Business critical data' will be defined in the Bill as:

a. personal information (within the meaning of the Privacy Act 1988) that relates to at least 20,000 individuals; or
b. information relating to any research and development in relation to a critical infrastructure asset; or
c. information relating to any systems needed to operate a critical infrastructure asset; or
d. information needed to operate a critical infrastructure asset; or
e. information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.

With such a broad definition, we believe it would be difficult to find a server that does not have some connection to any one of these categories in an organisation's network. By way of example, if an organisation has its risk management plans stored on a file share and emailed to a number of colleagues responsible for its execution, all of those devices and the servers where the data resides would be considered critical. Vacation coverage plans for data centre operational staff stored on a server would be similarly swept in. Historical reports and reference materials on past risk management plans would be similarly be categorised as critical. And any company with consumer customers and a catalogue mailing list would also be required to address that information as "critical infrastructure." We do not believe that overbroad categorisation is (or should be) intended by the Proposed Legislation. We believe this again highlights the need for a clearly defined set of national functions that must be preserved, which would then allow definitions like this to be narrowly tailored to support those national needs and interests.

As another example, the definition of "business critical data" includes "information relating to any research and development in relation to a critical infrastructure asset." This category of "business critical data" is extremely broad and not tied to any operational or risk management priorities, and is unlikely to aid in the response to a nationally significant event. The cost of having to protect all information from a critical infrastructure organisation's R&D on its own processes would be high, and the benefit from the additional security is unclear. As such, the definition may have the unanticipated consequence of capturing large amounts of information that is not helpful for managing the integrity of or securing critical infrastructure. We recommend narrowing this category from information relating to *any* research and development in relation to a critical infrastructure asset to "information related to research and

development of functions or components necessary for the continued operation of a critical infrastructure asset." This narrower definition will focus efforts on more critical data elements.

Cyber Security Incident

When governments require organisations to report cyber security incidents, we believe the governments should clearly articulate the rationale behind the need for data. Cyber security incidents, if broadly stated, are less helpful indicators to track than incidents that are connected to clearly articulated national priorities. For example, tracking incidents connected to resiliency requirements, events of national significance, or critical restoration needs following a disaster can provide actionable data for the government to engage. Understanding whether essential national functions are being protected is an important goal.

The Proposed Legislation defines "cyber security incident" very broadly to include a wide range of events involving unauthorised access, modification, or impairment. "Unauthorised access, modification or impairment" is, in turn, also broadly defined. However, reporting obligations are limited to when an entity responsible for a critical infrastructure asset "becomes aware that: (i) a cyber security incident has occurred or is occurring; and (ii) the incident has had, or is having, a *significant impact* (whether direct or indirect) on the availability of the asset." (Emphasis added.) The term "significant impact" is undefined and ambiguous. We believe that the broadness of this definition may fail to recognise important benefits of cloud computing – and certainly of hyperscale cloud computing – in that even if a particular asset becomes unavailable, the cloud workload or service function is still available, powered by other computing resources. As described above, in the context of cloud services that are not tied to a physical location, an asset-based approach is less relevant; here, an asset-based approach to defining significant incidents misses the underlying priority – the identification of the essential function in the country, the loss of which has a serious impact on the national security or economic stability of Australia. We believe that standard – what functions are most essential to Australia – needs to be at the centre of this space.

We recommend narrowing the definition of a cyber security incident to "any event having an actual adverse effect on the security of network and information systems," which is consistent with the definition of "incident" in the EU NIS Directive, and consistent with its definition of essential services in Section 5(2) of the Directive.

With respect to the incident reporting windows set forth in the Proposed Legislation, we appreciate that the Australian Government has lengthened the reporting window from 24 to 72 hours for cyber security incidents with "relevant impact" (per Section 30BC(1)(d) of the Proposed Legislation). However, we believe the 12-hour reporting window for a critical cyber security incident (i.e., an incident with "significant impact" under Section 30BC(1)(d)) remains

too short and could thereby negatively impact the ability of the organisation to manage the incident. In major cyber security incidents, the first 24-48 hours involve a combination of ongoing investigation and analysis, and assessments change as new facts are uncovered. Adrenaline flows as fast as information in the incident response teams, as they try to understand how a system was impacted and the consequences of an incident. The Proposed Legislation's consideration of a 12-hour mandatory reporting window for critical cyber security incidents with significant impact would be harmful to response efforts as well as potentially unhelpful to the Government's understanding, as the fact pattern is inconclusive at best and evolving rapidly. The window is simply too short to provide meaningful information in many cases. Hyperscale cloud providers are extremely motivated to keep customers connected and informed, and so information is released publicly as quickly as possible. The U.S. Department of Defense defined "rapidly report" to mean "within 72 hours of discovery of any cyber incident" in its regulation for contractors.[2] Short-term reporting takes responders away from the investigation and response effort, which harms everyone relying on that service. We believe 72 hours is the standard – and for good reason. Moreover, the 72-hour period has not been proven to be problematic, and we believe it is sufficient to meet the Government's need for transparency and visibility into a cyber security incident. We believe that the 72-hour reporting interval works well and should be adopted in the Proposed Legislation.

Critical Infrastructure Risk Management Program

The Proposed Legislation 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." As written, this language could place an unreasonable expectation on 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 critical infrastructures assess their risks, with a clear understanding of national confidentiality, integrity, and availability priorities. That articulation helps critical infrastructures set priorities and manage risks or hazards that occur.

The fact that a hazard "could have an impact on an asset" is insufficient 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 meaningless when the cloud can shift workloads dynamically. If the focus of the risk management conversation is about the

[2] SUBPART 204.73 - SAFEGUARDING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (osd.mil)

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.

We recommend editing this language to clarify that entities are not expected to identify every possible hazard; rather, responsible entities should only be expected to identify those hazards that are reasonably foreseeable. We believe this modest revision provides 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 possible to do so." We also recommend language that references basic cyber hygiene[3] as a foundation for a risk management program, so that basic cyber risks cannot become material and systemic problems. This becomes essential for smaller and medium-sized entities in a critical infrastructure that may lack the resources or technical capabilities to address significant cyber risks, at least initially.

VI. CONCLUSION

Microsoft welcomes further engagement and the opportunity to comment on future iterations of this Proposed Legislation. We believe that several additional rounds of dialogue may be necessary and encourage the Government to continue to engage deeply with industry prior to taking action. Finally, we urge the Government to take the time to explore and respond to industry concerns prior to taking action. We would welcome the opportunity to participate in any working groups or sector-based activities to help articulate (1) national essential functions; (2) clear risk management priorities; (3) modified definitions; (4) cross-sector harmonisation strategies for both regulators and sector members; and (5) incident reporting outcomes. We know significant work is ahead, and we remain committed to partnering with the Government of Australia to help protect the vital interests of the Australian people.

[3] Foundational cyber hygiene practices include policies and practices that protect resources, detect issues or anomalies and limit damage, and ensure readiness to respond to and recover from issues and incidents. To protect resources, organisations must take basic steps like deploying patches, changing default passwords, and leveraging multi-factor authentication. To detect issues or anomalies and limit damage, organisations must inventory devices and software, monitor networks, and restrict administrative privileges based on user duties. And to ensure readiness to respond and recover, organisations must manage regular backups of critical data.