Department of the Prime Minister and Cabinet

By email: InfrastructureResilience@dpmc.govt.nz

14 July 2023

MICROSOFT SUBMISSION ON THE NEW ZEALAND CRITICAL INFRASTRUCTURE PHASE 1 CONSULTATION

Background

1 Microsoft welcomes the opportunity to submit on the Department of the Prime Minister and Cabinet's (*DPMC*) Critical Infrastructure Phase 1 Consultation Paper (the *Consultation Paper)*.

2 Microsoft supports the New Zealand Government's efforts to improve the resilience of New Zealand's critical infrastructure. Modern infrastructure will underpin Aotearoa's growth and strengthen its economic resilience and national security.

3 Microsoft also notes that New Zealand faces a number of relevant trends, including a complex geopolitical and national security environment, with increasing cybercrime and the potential for sophisticated attacks on critical infrastructure, as recognised by the Ministry of Foreign Affairs and Trade in its recent Strategic Foreign Policy Assessment [1]. Microsoft agrees that improving the resilience of New Zealand's infrastructure is an important focus in light of these developing trends.

4 Critical digital infrastructure has an integral role in supporting New Zealand's critical infrastructure, with digital transformation moving many of New Zealand's critical infrastructure functions into the cloud. Microsoft submits that adopting cloud-based technology solutions, increasing the resilience and security of those solutions, and implementing an appropriately designed regulatory framework can help strengthen the resilience of New Zealand's critical infrastructure as a whole.

5 As a global cloud service provider to public and private sector customers, Microsoft has developed a strong understanding of how government can effectively design and implement critical digital infrastructure regulation. Our comments below are based on our practical experiences and expertise.

6 In this submission, we would like to convey Microsoft's commitment to partner with the New Zealand Government to establish effective frameworks for increasing the resilience and security of technology that supports New Zealand's critical infrastructure. We also provide our general commentary on how best to implement critical digital infrastructure regulation.

Consistency with the Emergency Management Bill

7 Microsoft recognises that the proposed Emergency Management Bill (which will replace the Civil Emergency Defence Management Act 2002) will go some way to enhancing New Zealand's critical infrastructure resilience. In particular, the shift in focus from 'lifeline utilities' to 'critical infrastructure' is an important step forward for New Zealand's emergency management regulatory regime. However, Microsoft considers that further steps are still needed to adequately strengthen New Zealand's critical infrastructure resilience – noting that

[1] Navigating a shifting world June 2023 PUBLIC-v4.indd (mfat.govt.nz)

the Emergency Management Bill focuses on emergency management, rather than critical infrastructure resilience.

8 We also note that issues raised in the Consultation Paper will be both dependent on and relevant to the development of the Emergency Management Bill, and we urge DPMC to ensure consistency of regulation across all critical infrastructure resilience legislation.

Executive summary

9 Microsoft submits that critical infrastructure resilience regulation should:

9.1 encourage the development and adoption of cloud-based technology, and promote secure digital transformation;

9.2 establish a single regulatory agency responsible for managing the critical infrastructure resilience system, with the authority to harmonise and deconflict regulatory obligations across all critical infrastructure sectors and jurisdictions;

9.3 be consistent with other critical infrastructure regulation, including the Emergency Management Bill and any sector-specific critical infrastructure resilience regulation, to ensure the regulatory environment does not become convoluted or unwieldy; and

9.4 align with global regulation, including by adopting existing international best practice and standards where possible to reduce the regulatory burden and cost.

Benefits of using cloud-based technology solutions

10 Microsoft considers that adopting cloud-based technology solutions can improve the operational resilience of critical infrastructure entities. The benefits of using cloud-based technology solutions were identified in Cabinet's recent endorsement of a refreshed Government Cloud First Policy[2], and include:

10.1 **Security:** Migrating data and services to a cloud environment enhances data governance and helps critical infrastructure entities maintain oversight over the data they retain and how that data is treated. Migration to a cloud environment also mitigates cybersecurity risks associated with the convergence of Information Technology-Operational Technology environments.

10.2 **A better understanding of the threat environment:** Adopting cloud-based technology helps critical infrastructure entities form a wider security intelligence view - enhancing threat identification and mitigation. For example, Microsoft quarantines and examines email attachments blocked by its advanced threat protection service. If malware is found, Microsoft will then use that information to proactively protect all of its customers (including critical infrastructure clients) from similar threats.

10.3 **Resiliency and recoverability design principles:** Cloud-based technology solutions are designed with resilience at their core. The solutions are designed to identify and respond to the actions of malicious users; environmental disasters; malware infections; and physical machine, network device, and storage array failures. Cloud-based technology solutions employ data centre replication, data mirroring and other redundancy, failover, and recovery capabilities, which in turn improve resilience. Cloud

[2] Proposals-for-refreshing-the-Cloud-First-Policy-and-strengthening-cloud-adoption-across-the-public-service-16-May-2023.pdf (dia.govt.nz)

solutions also assist critical infrastructure clients when responding to emergencies and block distributed denial of service attacks more effectively than on-premises solutions.

10.4 **Outsourcing of security maintenance and capabilities:** Cloud providers undertake patch management, vulnerability and other security configuration scanning (including critical security maintenance activities) as part of their service provision. Cloud providers manage advanced security capabilities and features, such as the encryption of data while data is processed, at rest, or in transit. Cloud services also employ the use of IoT, big data, and artificial intelligence - catalysing the development of new security capabilities.

Partnership principles

11 Microsoft is committed to partnering with the New Zealand Government to establish effective frameworks that increase the resilience and security of technology that supports society's most critical functions. Our approach is grounded in the following six key principles:

11.1 **Regulation should embrace secure digital transformation:** We note that while most critical infrastructure operators are adopting cloud-based solutions, we still hear concerns about modernising critical workloads. To combat these concerns, we consider that regulatory frameworks should publicly acknowledge the benefits that digital transformation can offer, including security, resiliency, availability, sustainability and compliance. Digital transformation will also act as a critical tool to enable the transition from a carbon-based economy.

11.2 **Regulation should increase public trust in digital technologies, including the cloud:** Effective regulation should provide end users with confidence that critical functions in the cloud will operate as designed. To achieve this goal, regulations must ensure security and integrity for critical infrastructure functions; ensure availability and minimise disruption of critical cloud functions; strengthen resiliency; and promote transparency and assurance. Regulations must also recognise the importance of both digital and physical cloud infrastructure - allowing critical functions for business continuity to be maintained in the event of a disruption, as technology, functional requirements, and risks evolve over time.

11.3 **Improve security through the digital ecosystem:** An effective regulatory framework should be designed to ensure that critical infrastructure cybersecurity risks are appropriately managed. To achieve this aim, we support the establishment of public-private partnerships in information sharing to ensure New Zealand remains one step ahead of the ever-changing global threat landscape.

11.4 **Be clear and achievable**: Regulatory requirements should be designed and carefully tailored to advance clearly stated objectives. In addition, regulations imposed on cloud providers should be clear, effective, and achievable. This approach will help ensure that local organisations and cloud providers can understand and implement regulatory obligations, and will better position the regulations to produce the desired national results.

11.5 **Accelerate global regulatory harmonisation:** Microsoft recognises that current regulatory requirements are assessed and defined at both a sectoral and a national level. Overlapping or conflicting requirements can lead to confusion and make it harder for governments, regulated entities that rely on cloud, and cloud providers to deliver the desired results. Microsoft supports the New Zealand Government in establishing principle-based, baseline regulatory obligations for critical functions in cloud services

across all critical infrastructure sectors. Microsoft encourages the New Zealand Government to collaborate with their counterparts in other jurisdictions to harmonise regulatory standards across international borders. And Microsoft notes the importance of ensuring a consistent, harmonised regulatory approach in New Zealand, including in the legislative process for the new Emergency Management Bill.

11.6 **Recognise and support legitimate sovereign interests:** Microsoft notes that effective legal frameworks must be designed to recognise and support the legitimate sovereign interests of nation states while simultaneously considering executability, effectiveness, and global implications.

Defining and designating critical infrastructure

12 We understand the Emergency Management Bill will define 'critical infrastructure' and 'critical infrastructure entity' for the purposes of any future critical infrastructure regulation, and that DPMC is focused on seeking feedback on the regulatory reforms that are proposed to apply to those entities, rather than the criteria that should be used to designate entities as critical infrastructure.

13 Microsoft believes that clearly and accurately defining these terms is crucial to ensuring subsequent regulation is effective and will reduce the regulatory burden placed on infrastructure providers. We urge DPMC to consider whether the designation criteria and process set out in the Emergency Management Bill will remain appropriate for broader critical infrastructure regulation, in light of our comments below.

Critical functions should be regulated separately from the entity that provides them

14 While an entity may be designated as a 'critical infrastructure entity', not all functions or services it provides to customers will or should be considered 'critical'. Microsoft agrees that regulating critical assets (and systems), and not critical entities as a whole, is a more targeted and effective approach.

15 To manage this separation, regulation should first articulate the national level functions that must be protected and preserved, regardless of the network, system, or asset used to provide those functions. Protecting those national level functions should become the foundation for a national risk assessment programme, enabling entities to incorporate the management of that risk into their own corporate processes.

16 Once critical functions are identified at the national level, regulation can create a process for identifying the systems and assets needed to support those functions (e.g., the designation process established under the Emergency Management Bill). We recommend any process to designate a particular system or asset as 'critical' should be a cooperative endeavour between the chosen regulator (or Minister, in the case of the Emergency Management Bill) and relevant industries, with clear consultation requirements. The process should provide sufficient time for the careful consideration of input from responsible entities relevant to the functions, asset, or system.

Distinction between cloud services and cloud infrastructure

17 Microsoft submits that critical infrastructure regulation should distinguish between cloud services and cloud infrastructure. We note that drawing this distinction will allow for more effective regulation, especially if there is an intention to impose prescriptive standards in order to manage specific risks and vulnerabilities.

18 Data centres are fixed, physical assets reliant on the energy and telecommunication networks that connect to them. In contrast, cloud services are computing systems and software that are

logically separated from the physical hardware that runs within a data centre environment. These systems and software are often not tied to one physical location.

19 This distinction means that the risk to data centres and cloud services are related but distinct. For data centres, the risks are often connected to physical controls and personnel access as well as disruptions to energy supplies or telecommunications network connectivity. For cloud services, the risk is more often related to potential software vulnerabilities and virtual access to data.

20 Creating separate designations for data centre operators and cloud service providers will ensure regulation is focused on each sector's specific set of threats and interdependencies. Crucially, it will also ensure regulation can focus on the different relationship each service has with other critical infrastructure operators as suppliers and customers.

Regulating critical cyber infrastructure

21 Cloud services operate differently to other 'vertical' industry sectors. Cloud services providers operate horizontally across New Zealand's economy and will themselves serve other critical infrastructure operators in most (if not all) sectors. Cloud service providers will also often have a global customer base and operate in many different jurisdictions.

22 Microsoft supports DPMC's focus on ensuring any minimum standards do not conflict with or duplicate standards in place under other regulatory regimes. We recognise that there is a risk that providers of cloud services and data centre infrastructure will face regulation not only across several critical infrastructure sectors (each with their own sector-specific requirements), but also across international jurisdictions.

23 We therefore support a regulatory framework that:

23.1 designates a single, central agency responsible for the resilience of the infrastructure system;

23.2 is consistent with the treatment of critical infrastructure in emergency management legislation, including the Emergency Management Bill;

23.3 leverages global best practice and standards for providers and operators that work across multiple jurisdictions; and

23.4 uses existing cloud security certifications and standards-based compliance frameworks.

Single regulatory agency should coordinate critical infrastructure system

24 Microsoft supports the designation of a central, coordinating entity responsible for the resilience of the infrastructure system, as proposed by DPMC. We recommend that the agency has overarching authority to set baseline requirements and harmonise and deconflict requirements proposed by other sector-specific regulators. If a single regulator is not given an overarching mandate, collaboration among regulators should be required to ensure consistency and avoid duplicative and/or conflicting compliance costs and obligations.

Global best practice and standards should be adopted where possible

25 Critical infrastructure sectors are becoming increasingly interdependent, demonstrating the need for cyber security requirements that can apply across several different sectors. Even today, supply chain integration and common leveraging of services mean cloud providers and other organisations must meet the security requirements of multiple sectors. Beyond the regulatory and compliance benefits, adopting cyber requirements that are consistent across

sectors creates a 'common language', increasing understanding of cyber risk management practices across supply chains and helping to illuminate where gaps in security may exist.

26 When regulating for resilience, we strongly support an approach that adopts cross-sector 'security baselines' for cyber risk management. Security baselines are a foundational set of policies, outcomes, activities, practices, and controls intended to manage cyber security risk.[3] Security baselines can include specific desired outcomes (e.g., 'know your organisational risks'); security activities or practices (e.g., conduct a risk assessment, document, review, and disseminate the results, and update the assessment regularly); and security controls (e.g., security policies are defined, approved by management, and communicated to employees and third parties). Many risks faced by critical infrastructure providers are similar. Cross-sector 'baselines' address a significant majority of the cyber risks applicable across organisations. Where the baselines do not address a sector-specific risk, they can be augmented with a narrow set of sector-specific requirements.

27 If DPMC seeks to apply specific standards in order to mitigate particular cyber risks or vulnerabilities, we recommend these obligations leverage existing global security standards. As examples, ISO/IEC 27101 provides cyber security framework development guidelines that are applicable across sectors.[4] It also incorporates ISO/IEC 27103, which provides guidance on how to use existing ISO and IEC standards to implement risk management activities required by a cybersecurity framework.[5]

28 ISO/IEC 27103 leverages the Framework for Improving Critical Infrastructure Cybersecurity, commonly referred to as the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Globally, critical infrastructure providers have acknowledged the benefits of using these international standards.[6] Financial services, IT, and telecommunications providers use a 'common security baseline' across ISO/IEC 27103, the NIST Cybersecurity Framework, and sector-specific frameworks to enable consistency, while addressing the unique concerns of their regulators.[7]

Building a shared understanding of issues that are fundamental to system resilience

29 In principle, we support DPMC's interest in developing a shared understanding of hazards and threats between critical infrastructure entities and government. Microsoft has partnered with the New Zealand Government since 2003 under our Government Security Programme to build trust in and an understanding of Microsoft's products[8], and we actively engage with the Government on areas of national security interest. As we discuss above, strong information sharing partnerships are key to ensuring New Zealand stays ahead of the national threat landscape.

30 However, while we support policy goals and regulatory resource investments that promote the voluntary sharing of key information between critical infrastructure entities and government, we strongly caution against the introduction of any mandatory information

---

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

4 https://www.iso.org/standard/72435.html

5 https://www.iso.org/standard/72435.html

6 https://www.nist.gov/industry-impacts/cybersecurity-framework (highlighting use by Boeing, J.P. Morgan Chase, Nippon Telegraph and Telephone Corporation, and the Bank of England among others); *see also* https://www.nist.gov/cyberframework/perspectives

7 https://www.crx2.org/s/CR2-White-Paper_Seamless-Security.pdf

8 https://news.microsoft.com/2003/09/15/new-zealand-government-joins-microsoft-government-security-program/

sharing obligations. Customers deserve predictability about what happens with their data (and must retain ownership of that data), and mandatory regulatory reporting obligations risk undermining that public trust. Mandatory information sharing obligations can also have unintended side effects, such as diverting resources from critical security roles or creating new threat vectors that weaken the security of the relevant network and the customers that rely on it, contrary to the core policy goal of uplifting cybersecurity of critical infrastructure.

31 Voluntary information sharing, though, remains an important cybersecurity risk management tool. We encourage the development of a secure information sharing platform to enable the transmission, management, storage and safeguarding of sensitive information exchanged between government and critical infrastructure operators. Microsoft would welcome the opportunity to partner with the Government to develop such a platform, and leverage our comprehensive security and rights management controls.

Managing national security risks to the critical infrastructure system

32 The Consultation Paper references the government intervention power adopted in Australia, which would enable the Minister of Home Affairs (and Australian government agencies) to manage a specific cyber security incident in place of a critical infrastructure operator. While we recognise the intention and purpose of an intervention power, we strongly believe such actions would undermine the Government's objectives in a national cyber security incident.

33 In many cases, it is the organisations themselves that are best positioned to determine how to appropriately respond to and mitigate the impact of cyber incidents. The individual organisation will be more familiar with its own unique network, systems, configurations, risk profile, threat environment, security policies, customers, and cyber capabilities. In practice, it would take an extended period of time for a government team to properly understand the fact pattern of a live cyber incident, the technologies in play, and challenges of any decisions to be made before directing an appropriate response. This process often introduces additional risk, as specialised analysts must navigate requests, speculations, and well-intended ideas from individuals/organisations who do not have a full understanding of the incident, instead of managing the incident itself.

34 Individual organisations are not only best positioned to respond, they also have a strong incentive to protect their own networks and maintain the trust of their customers. The possibility of unilateral intervention by government greatly increases the risk of unintended collateral consequences, impacting customers by undermining trust, while threatening to make entities less secure.

35 If an intervention power remains desirable, we strongly recommend it is established under a framework that incorporates robust checks and balances. Use of such power should be subject to a significant threshold, be time limited, and require independent authorisation. As an example of a hyperscale cloud provider, Microsoft spends over $1 billion per annum on cyber security, and has demonstrated an ability to defend itself against significant and repeated cyber threats. We continue to work cooperatively with cyber security agencies to share threat intelligence and respond to cyber incidents. We recommend that any proposed intervention framework (and threshold) recognises these capabilities and existing levels of collaboration.

36 Microsoft appreciates the opportunity to contribute insight learned from its practical experiences and we welcome further dialogue on these topics as DPMC progresses its consultation process.

37 Please do not hesitate to get in touch with our team if you have any questions in relation to this submission.

Kind regards,

Maciej Surowiec
Government Affairs Lead
Microsoft
Maciej.Surowiec@Microsoft.com