National Security Group
Department of the Prime Minister and Cabinet
Level 8 Executive Wing, Parliament Buildings,
Wellington 6011
[by email: infrastructureresilience@dpmc.govt.nz]

8 August 2023

Re: <u>Comments on the *Strengthening the resilience of Aotearoa New Zealand's critical infrastructure system* discussion document</u>

Amazon Web Services New Zealand Ltd. (AWS) is grateful for the opportunity to comment on the Department of Prime Minister and Cabinet's June 2023 Discussion Document on *Strengthening the resilience of Aotearoa New Zealand's critical infrastructure system*.

AWS is the cloud computing arm of Amazon.com, Inc. AWS has been operating in New Zealand for 10 years. We have offices in Auckland and Wellington and employ more than 150 New Zealand staff. In September 2021, AWS announced that it will establish an AWS Region in Auckland in 2024, which will bring world-class cloud computing infrastructure onshore to New Zealand. The Economic Impact Study[1] that accompanied this announcement estimated that AWS's NZ$7.5 billion investment will create around 1,000 new jobs and contribute approximately NZ$10.8 billion to New Zealand's GDP over the next 15 years.

Today, our customers in New Zealand host important workloads on AWS's secure and extensive global cloud infrastructure, and use AWS to achieve their compliance, security and resilience requirements. The planned AWS Region in Auckland will give existing and new customers the opportunity to leverage new AWS infrastructure in New Zealand. These customers will also retain the ability to maintain active workloads and/or back up important data in AWS Regions of their choice overseas. By providing New Zealand customers with multiple options for deploying their workloads, AWS enables customers to achieve extremely high levels of resilience to meet their specific requirements. AWS customers also benefit from a cloud and network architecture built to meet the requirements of the most security-sensitive organisations, including governments, and financial services and healthcare providers. Each AWS Region is fully isolated and comprised of multiple Availability Zones (AZs), which are fully isolated partitions of our infrastructure. AZs offer AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than those that rely on traditional single data centre infrastructures or multi-data centre infrastructures.

AWS supports the government's objective of uplifting the resilience of critical infrastructure in New Zealand. AWS welcomes the government's intention to undertake a deliberate consultative process with the community and industry to get the resilience framework right. AWS welcomes the recognition in the discussion document that critical infrastructure is interconnected and that a shared understanding of key threats and hazards is important. AWS supports the approach of identifying minimum resilience standards to help 'lift the floor' across critical infrastructure in New Zealand. An effective critical infrastructure resilience framework will help focus our collective attention and

[1] AWS, Economic Impact Study, New Zealand Region (2021)

resources on the greatest threats and hazards to critical infrastructure assets, and will define clear expectations on the resilience outcomes to be achieved.

Our detailed comments on the discussion document are contained in **Appendix A**. We would be pleased to provide additional input on any of the points raised in our submission and/or to schedule a meeting to discuss these issues should you be interested. Please do not hesitate to contact me at pdkeatin@amazon.com should you wish to follow up on our comments.

Sincerely,

Paul Keating
Head of Public Policy
Amazon Web Services New Zealand Ltd.

Appendix A.

AWS Comments on Critical Infrastructure Resilience Discussion Document

Amazon Web Services New Zealand Ltd (AWS) is grateful for the opportunity to comment on the Department of Prime Minister and Cabinet's June 2023 Discussion Document on *Strengthening the resilience of Aotearoa New Zealand's critical infrastructure*.

Consultation

AWS welcomes the government's intention to undertake a deliberate consultative process with industry and the community to get the resilience framework right. **AWS recommends that this consultation continue throughout the development of the framework, including in defining the specific threats, resilience outcomes and standards for critical infrastructure** that the framework will regulate. This will ensure that industry and community experience and best practices are harnessed in the design of the resilience framework**. We further recommend that policy makers consider establishing an ongoing industry-government partnership mechanism for operationalising the framework and for continuous review of New Zealand's critical infrastructure resilience efforts**.

Objectives

AWS welcomes the objectives of the critical infrastructure work programme as described on page 7 of the discussion document. AWS agrees with the characterisation of critical infrastructure assets as often having interconnected dependencies, and the assertion that baseline resilience standards will help 'lift the floor' across New Zealand's critical infrastructure. AWS also agrees with the government's emphasis on identifying and addressing 'weak points' in critical infrastructure that may be more exposed to identified threats or hazards. Further, we welcome the priority that government is placing on developing a shared understanding of important threats and hazards across both the public sector and private sector. However, the proposed work programme envisages an expansive *all* hazards and threats approach, which is likely to dilute focus on the highest impact threats and hazards facing New Zealand's critical infrastructure. **We recommend that the next phase of work identify the most important hazards and threats to help prioritise collective efforts and limited resources towards addressing these first.**

Principles

AWS welcomes the balanced and pragmatic principles proposed in paragraphs 8(a) - 8(e) of the discussion document. **We recommend these principles be employed at all stages of developing and implementing critical infrastructure policy and regulation**.

Defining critical infrastructure

AWS supports the observation at paragraph 84 that focusing on specific critical infrastructure 'assets' is likely to be the best approach to regulating critical infrastructure. Carefully defining specific physical assets in New Zealand as critical infrastructure will give organisations that control or operate those physical assets clarity on how to apply regulatory requirements, and will ensure that efforts to uplift security and resilience will focus on the most important assets for New Zealand. **AWS recommends that critical infrastructure regulation focus on specific, identifiable physical 'assets' and not on broader 'sectors' or 'entities' or broad definitions of 'asset'.** We have previously seen broad 'sector' or 'entity' definitions of critical infrastructure and broad 'asset' definitions create confusion, protracted definitional debate, and unnecessary regulation of assets and business activities that are not critical infrastructure. This may undermine the intent of ensuring appropriate attention and investment goes toward safeguarding infrastructure that is critical to New Zealand, and may create inefficiency and added cost without corresponding benefit.

Industry specific critical infrastructure

Given the significant differences in assets and operating models across different industries, **we recommend that government work closely with each industry to identify which specific assets are critical infrastructure** within that industry.

For the digital technology industry, the discussion document uses a range of terms including 'data centres', 'data storage providers', 'cloud service providers', 'data facilities' and 'digital service providers'. **AWS recommends that critical infrastructure regulation apply to specific "data centre facilities" in New Zealand that exceed a minimum size-based threshold**, and we welcome further consultation on appropriate thresholds. To achieve the objectives of the critical infrastructure work programme, **any regulation should apply equally to all data centre facilities** in New Zealand that exceed the applicable threshold, whether owned and operated by government or by industry, whether locally or foreign-owned, and whether operated as part of a service for third-party customers or solely for an organisation's internal requirements (known as 'on-premises'), including any 'hybrid' model that combines two or more these characteristics. It is important that regulation addresses the critical assets that underpin all of these business models. This approach will create a high baseline standard for all types of data centre facilities and will avoid vulnerabilities arising from unregulated facilities.

"Significant" critical infrastructure

The discussion document contemplates that certain infrastructure may be identified as "significant critical infrastructure" and that enhanced resilience expectations may apply to this infrastructure. This approach is likely to create unnecessary complexity and confusion, and may undermine the desired outcome of uplifting the resilience of a specific subset of New Zealand's infrastructure. **We recommend that policy makers adopt a straightforward approach that distinguishes infrastructure assets as either critical or not, without introducing additional complexity at this time**.

If the government does pursue a distinction between "significant" and "not significant" critical infrastructure, **we recommend that the assessment model for criticality be based on the 'holistic model' (option 2, page 36), which focuses on a broader range of societal and economic considerations.** We do not see the alternative 'simple model' as a viable alternative, as it uses a set of variables (i.e. number of customers and geography) that, in many industries, are likely to be too narrow and less relevant than other factors. **We also recommend that government consult further with the community and specific industries before finalising any model for assessing the significance of different categories of infrastructure.**

Resilience domains

The discussion document proposes five 'domains of resilience'. The application of the various factors in these domains and the methods for uplifting infrastructure resilience will differ significantly across different industries and critical assets. Accordingly, **we recommend that the further development of the resilience domains and corresponding requirements should:**

1. **Involve close consultation with business, public sector and community organisations that are most familiar with operating different types of critical infrastructure assets;**
2. **recognise that the controls and expectations associated with each domain will likely vary depending on the nature of specific threats to specific assets;**
3. **wherever possible, align with leading industry standards such as those maintained by the Industry Standards Organisation (ISO); and**
4. **ensure that organisations are only responsible for what they can reasonably control, and are empowered to reasonably rely on credible third-party attestations and certifications**

(such as ISO certifications) and contractual commitments from vendors or service providers to achieve compliance.

We further recommend combining the supply chain and procurement domains into a single domain, covering the relevant factors under these two domains.

Minimum resilience standards

As noted above, AWS supports the objective of future proofing New Zealand's critical infrastructure by setting minimum resilience standards. **We recommend that government, business and community organisations work together to identify and then understand and implement appropriate minimum resilience standards.**

We recommend that minimum resilience standards set out principles or objectives that must be met instead of prescriptions for specific technical or organizational measures or procedural requirements or checklists. This approach recognises that a range of controls and measures may be used to uplift resilience and mitigate threats and hazards to critical infrastructure assets. Additionally, as hazards, threats and mitigation measures evolve, a principles-based and outcomes-focused approach to regulation will ensure that the framework remains current over time. In contrast, prescriptive measures or process-based approaches may drive a narrow and overly procedural 'checklist' approach to demonstrating infrastructure resilience, and may overlook key considerations and risks that may undermine resilience outcomes; these approaches also do not promote government and industry working together to demonstrate and achieve desired resilience outcomes.

We also recommend that resilience standards for critical infrastructure align with existing industry standards where possible. In many industries, businesses and other organisations have invested significantly in complying with well-recognised standards, many of which relate to infrastructure resilience. In the technology industry, the following standards would, if implemented for all critical data centres in New Zealand, significantly 'lift the floor' of critical infrastructure resilience in New Zealand**:**

- ISO 27001 Information Security Management Standard
- ISO 22301:2019 Business Management Continuity Standard (BCMS)
- SOC2 for Disaster Recovery Plans
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

Finally, we recommend that any new standards should take into account, and should not conflict with or duplicate, other existing regulation and policy guidance designed to improve resilience in regulated industries in New Zealand – for example, outsourcing and cyber resilience guidance in the financial services sector**.** We welcome the recognition of this concern and intent to address this in the principles (paragraph 8) section of the discussion document.

Enabling improved critical infrastructure outcomes

In addition to the new obligations being contemplated under the programme, **we recommend that the government include proposals for how the resilience work plan can contribute directly to supporting critical infrastructure operators to enhance the resilience of critical infrastructure assets'**. For example, critical infrastructure assets could have some level of priority access to the infrastructure, products and services they need to maintain uninterrupted operations, especially during a disaster or emergency**.** This should include considerations for enabling expedited and priority access to the services, permits or rights required to:

1. accessing utility power and water supplies, generate power (especially renewable power), or obtain fuel for backup power generators;
2. own, build, operate, and/or access networking infrastructure;

3. acquire land and build additional capacity to meet resilience expectations; and/or
4. restore or maintain operations or supply of utility services following an emergency.

Information collection and reporting

We welcome continued consultation to help define future information collection and reporting requirements under critical infrastructure regulation. Paragraph 75(a) captures accurately a number of the concerns that organisations may have relating to information sharing. It is important to note that there will likely be intellectual property and commercial sensitivity concerns with disclosing certain information, and these should be appropriately accounted for in defining information collection requirements.

Paragraph 75(b) appears to contemplate an expansive and detailed information collection approach, which is likely to require disproportionately large amounts of information being reported (e.g. comprehensive data on outages, failures, incidents and potential threats, equipment types and suppliers). This degree of reporting would be unnecessarily burdensome for organisations and would not help achieve the desired resilience outcomes of critical infrastructure regulation unless paired with significant additional resources to sort through, analyse and use the information being collected. Unless this is the case, a narrower and more targeted approach to information gathering is warranted. In considering necessary information collection, **we recommend that government consult thoroughly with industry to identify appropriate relevance and materiality thresholds for reporting requirements, and ensure that these are implemented only to the extent necessary for achieving specific resilience outcomes.**

We also encourage policy makers to consider that the more times information is duplicated and shared (e.g., to comply with multiple information collection and reporting obligations across multiple agencies), the greater the risks to that information and the corresponding asset(s) (for example, because there is increased risk of accidental or unauthorised disclosure of, or access to, that information). Accordingly, in order to promote security and resilience of New Zealand's critical infrastructure, **we recommend that information gathering should be kept to a minimum, that streamlined and secure processes be established for receiving and storing information relating to critical infrastructure assets, and strict protocols be used to ensure that shared information remains confidential and secure. We further recommend that the government consider investing in developing a secure platform for sharing sensitive information about critical infrastructure assets.**

Compliance and enforcement measures

We welcome the government's focus on collaborative change management rather than compliance assessments and punitive enforcement. We believe that effective collaboration between government and organisations that control or operate critical infrastructure is the most effective way to significantly and rapidly uplift critical infrastructure resilience in New Zealand. This approach will allow the government to focus its resources on educating and supporting organisations to achieve resilience outcomes, rather than expending considerable resources on prosecuting what is may be a small number of outliers that are unwilling to engage in the uplift of critical infrastructure resilience.

Of course, mandatory compliance and enforcement measures may be important for remedying persistent 'weak points' and addressing outliers where these emerge. We recognise also that enforcement and penalties may be required in cases of wilful, severe, or repeated non-compliance. In these instances, **we recommend that any penalties should follow reasonable warnings and opportunities to remediate, and should be reasonable and proportionate to each breach**. **We further recommend that organisations be exempt from penalties for breaches that are outside their reasonable control,** for example, an organisation that operates only part of a critical infrastructure asset should not be responsible for failures by a third-party organisation that independently operates a different part of that asset.

Cybersecurity risks

AWS welcomes the prioritisation of security in the critical infrastructure resilience framework. Cybersecurity cooperation between government and industry will be helpful as the complexity and frequency of cybersecurity threats grow. The top priority for security response should be quickly and effectively addressing the risk/responding to an event. **We recommend that the resilience framework ensure that organisations that control or operate critical infrastructure assets have sufficient flexibility to prioritise addressing cybersecurity incidents as quickly as possible and in the manner they determine will quickly and effectively address the risk. Any required cooperation with government or other impacted organisations should not interfere with those efforts.**

Extraordinary powers

The discussion document contemplates the introduction of new extraordinary powers, and specifically refers to future consideration of new ‘direction’ and ‘intervention’ powers. **We strongly recommend that the government pause on introducing these types of powers until the scope, necessity, benefits and risks of these powers have been carefully assessed and discussed with operators of critical infrastructure assets across different industries.** Given the complexity and variation among many types of assets, these types of powers can have significant unintended consequences, including disrupting responses to an emergency, and they may undermine (rather than help achieve) the objectives of critical infrastructure regulation. They can also cause confusion and disproportionate harm to organisations and their customers depending on how they are scoped and applied. Although such powers may exist in a small number of other jurisdictions, these are as yet largely untested.

Instead of extraordinary powers, we recommend that government focus on offering clearly identified capabilities and support to critical infrastructure operators (including early warning, coordination, communication and facilitation capabilities), and when requested working cooperatively with operators to respond to emergencies. Organisations with day to day control of critical infrastructure assets will almost always be best placed to identify and respond to particular security risks and incidents, and unsolicited involvement of an external entity may cause substantial delays and inefficiencies, and exacerbate harm.

Safeguards in relation to extraordinary powers

If the government ultimately decides to introduce certain extraordinary powers, which we recommend against, **the powers should be very specific and narrowly scoped, limited to a prescribed list of actions or directions, and appropriately tailored to different industries and different types of critical infrastructure. They should also be subject to strong guardrails and only exercisable following a transparent process with strong checks and balances. Minimum guardrails should include the following:**

- The powers should only be exercisable in a narrow and objectively defined high threshold emergency situation (e.g. significant and widespread risk to human life).
- The powers should only be used if they are absolutely necessary to achieve outcomes specified in the critical infrastructure regulation, if there is no other alternative, and to the extent it is proportionate, practicable, and feasible to do so.
- The decision to exercise the powers should be made by a clearly identified senior government official that is independent of the authority that will exercise the powers, and should be made after consulting with and obtaining agreement from the Attorney-General
- The assessment of whether to exercise the powers should consider the impact on, and the interests and capabilities of, the relevant operator of the critical infrastructure asset, and involve prior consultation with that operator.

- The assessment of whether to exercise the powers should also consider potential impacts on individuals and organisations that directly or indirectly rely on or use the critical infrastructure asset (to, for example, safeguard their data).
- The decision to exercise the powers should be subject to prior judicial authorisation should be appealable and subject to a merits review by an independent judge.
- The regulated organisation should be able to apply for urgent order suspending or terminating the exercise of the powers based on new considerations or circumstances.
- The regulated organisation should not be required to turn over or weaken intellectual property, take action outside of New Zealand, violate other laws, violate contractual arrangements, violate its health, safety, security or operational policies, harm third parties, or create vulnerabilities, weaknesses, backdoors, or weaken or bypass encryption.
- The regulated organisation should be immune criminal and civil actions arising from government exercising these powers, and should be entitled to recover reasonable costs resulting from any exercise of these powers.

Regulatory entities

The discussion document seeks feedback on options for regulatory entities to be responsible for critical infrastructure, including administering potential compliance and enforcement mechanisms. **We recommend that these decisions be deferred until there is greater clarity on the functions those entities would be asked to undertake**. In any case, relevant regulatory entities should have sufficient capability, including relevant industry expertise, to support and oversee the critical infrastructure assets for which they will have responsibilities, and should be well coordinated and, where necessary, share information effectively.
