CAUDIT
THE COUNCIL OF AUSTRALASIAN
UNIVERSITY DIRECTORS OF INFORMATION TECHNOLOGY

Strengthening the resilience of Aotearoa New Zealand's critical infrastructure system:

Critical Infrastructure Phase 1 Consultation

Universities New Zealand (NZ) and Council of Australasian University Directors of Information Technology (CAUDIT) response

Universities New Zealand (UNZ) is the peak body for New Zealand's eight universities. UNZ helps universities deliver high-quality education through robust quality assurance systems; co-ordinate international education policy; provide sector coordination, inform, and influence decision-making, and administer scholarships.

The Council of Australasian University Directors of Information Technology (CAUDIT) is the peak member association supporting the use of information technology and cyber technology in the education and research sector in Australasia. CAUDIT is a registered Not-For-Profit Association with 67 members which includes all public universities in Australia and New Zealand, those of Papua New Guinea and Fiji, and key national research and education organisations in Australia and New Zealand. Members are represented by the most senior person with strategic responsibility for Information Technology (IT) operations and digital transformation in their institution i.e., the CIOs, CDOs, and IT Directors of each member organisation.

UNZ and CAUDIT, with input from its members, submits the following submission to the Department of the Prime Minister and Cabinet (DPMC). UNZ and CAUDIT continues to welcome the opportunity to provide feedback and support the outcomes relevant to critical infrastructure in respect to Higher Education and Research.

UNZ and CAUDIT welcome the opportunity to collaborate with the New Zealand Government on the *Critical Infrastructure Phase 1 Consultation*. Please note, the views expressed in this submission result from contributions of many organisations (Universities New Zealand and CAUDIT Member Institutions), and, as such, may not represent the views of all participating organisations, rather, they are reflective of the overall expertise and interests of the collective sector-based group. Each partner or member institution may provide their own individual submission, as appropriate.

After consultation with UNZ and CAUDIT Partners and Members, we make the following general recommendation regarding the *Critical Infrastructure Phase 1 Consultation*:

1. Definition of Critical Infrastructure

We are aware that in other parts of the world, such as Australia, there have been suggestions that higher education be considered critical infrastructure in similar legislation.

This has been justified on grounds such as:

- Some non-university organisations (Government and private sector) depend upon a small percentage of university research and research infrastructure for their ongoing operations.
- Universities hold research materials such as chemicals and biological agents that could present a hazard to health and safety if improperly handled or in an accident.
- Universities hold large amounts of private information on staff, students, alumni, research subjects, etc. Any data breach could have consequences with regard to their rights and privacy.
- Universities house upwards of 20,000 students for large parts of each year and are a key source of health and wellbeing services to around 200,000 staff and students more generally.

Though we agree that all these grounds are important, we believe that these areas are already subject to adequate legislative and regulatory oversight. We would not support duplication of reporting, oversight, or other regulatory requirements.

We therefore strongly support the proposed definition of what is critical infrastructure in the consultation document. We would not support this being broadened in any way.

2. Responses to Discussion Paper questions

Prelude: Objectives for and principles underpinning this work programme	
Does more need to be done to improve the resilience of New Zealand's critical infrastructure system?	• Yes. We are appreciative for DPMCs focus on NZ critical infrastructure and would welcome improvements to resilience, particularly if this was undertaken in conjunction with existing requirements, frameworks, and legislation.
Have you had direct experience of critical infrastructure failures, and if so, how has this affected you?	• At a sector level, a loss of critical infrastructure (i.e., network, power), would have a detrimental impact on the entire business operations and research outputs. Research data may be compromised.
How would you expect a resilient critical infrastructure system to perform during adverse events?	• Core services such as medical, energy, and telecommunications are crucial for safety during adverse events, and we would expect a minimal level of operation for core emergency services.
Would you be willing to pay higher prices for a more resilient and reliable critical infrastructure system?	• This would depend on the significance of the costs and the services received.
The work programme's objective is to enhance the resilience of New Zealand's	• Yes

critical infrastructure system to all hazards and threats, with the intent of protecting New Zealand's wellbeing, and supporting sustainable and inclusive growth. Do you agree with these objectives? If not, what changes would you propose?	
Do you agreed with the proposed criteria for assessing reform options? If not, what changes you would propose?	• Yes
Section 1: Background and context	
The paper discussed four mega trends: i) climate change, ii) a more complex geopolitical and national security environment, iii) economic fragmentation, and iv) the advent and rapid uptake of new technologies. Do you think these pose significant threats to infrastructure resilience?	• Yes, in particular our expertise lies in ii) and iv). • Climate change should be diversified to include natural risks including earthquakes and cyclones which have already had a significant impact and will continue to do so. Critical infrastructure should address the risk of these reoccurring events through diversity, design and appropriate standards addressing the risk, for example construction standards.
Are there additional megatrends that are also important that we haven't mentioned? If so, please provide details.	• A fifth megatrend is significant health impact, for example, a pandemic, or an uprise in debilitating human health

	conditions (this may impact available workforce, etc).
Do you think we have described the financial implications of enhancing resilience accurately? If not, what have we missed?	• Yes
Section 2: Potential barriers to infrastructure resilience	
Building a shared understanding of issues fundamental to system resilience	
How important do you think it is for the resilience of New Zealand's infrastructure system to have a greater shared understanding of hazards and threats?	• Education is a crucial part of a successful strategy. Furthermore, collaboration amongst critical infrastructure sectors has a direct positive impact to education and learning.
If you are a critical infrastructure owner or operator, what additional information do you think would best support you to improve your resilience?	• Currently, higher education and research are not classified as CI in NZ under existing legislation. • If the sector were classified, we would hope to have support in terms of Government briefings, assistance in uplift requirements, grace reporting periods, and ongoing consultation with both Government and fellow CI operators (to share relevant threat intel for example).

What do you think the government should do to enable greater information sharing with, and between, critical infrastructure owners and operators?	• Regular trusted information sharing forums, which allows for introductions and ongoing information sharing.
Setting proportionate resilience requirements	
Would you support the government having the ability to set, and enforce, minimum resilience standards across the entire infrastructure system? If so: **– what type of standard would you support (eg. requirement to adhere to a specific process or satisfy a set of principles)?** **– do you have a view on how potential minimum resilience standards could best complement existing approaches to risk management?**	• We recommend building from existing standards, such as the Protective Security Requirements.
Would you support the government investing in a model to assess the significance of a critical infrastructure asset, and using that as the basis for imposing more stringent resilience requirements? If so: **– what options would you like the government to consider for delivering on this objective?**	• Utilise existing frameworks where possible.

What criteria would you use to determine a critical infrastructure asset's importance? Investing in a model to assess a critical infrastructure asset's criticality, and using that as the basis for imposing resilience requirements that are more stringent on particularly sensitive assets? If so: **– what options would you like the government to consider for delivering on this objective?** **– what features do you think provide the best proxies for criticality in the New Zealand context?**	• Risk based approach, which has the most stringent requirements on the most critical infrastructure (i.e., health, telecommunications, energy, food). The most critical Government entities, i.e., Defence, should be held to the same requirements.
Managing significant national security risks to the critical infrastructure system	
Do you think there is a need for the government to have greater powers to provide direction or intervene in the management of significant national security threats against a critical infrastructure? If so: **– what type of powers should the government consider?** **– what protections would you like to see around the use of such powers to ensure**	• Any government intervention would need to be clearly defined, have appropriate risk-based thresholds and governance, and ensure the government has the capability to intervene.

that they were only used as a last resort, where necessary?	
Creating clear accountabilities and accountability mechanisms for critical infrastructure resilience	
Do you think there is a need for a government agency or agencies to have clear responsibility for the resilience of New Zealand's critical infrastructure system? If so: **– do you consider that new regulatory functions should be the responsibility of separate agencies, or a single agency?** **– do you consider that an existing entity should assume these functions or that they should be vested in a new entity?** **– how do you see the role of a potential system regulator relative to sectoral regulators?**	• It makes sense to tie it under an existing agency, uncles there is a clear need for duty separation in any of the proposed legislation.
Do you think there is a need for compliance and enforcement mechanisms (eg. mandatory reporting, penalties, offences) to ensure that critical infrastructure operators are meeting potential minimum standards? If so:	• Financial penalties don't address the core of the issues with the state of information security. These issues are multifaceted and include resourcing limitations, compliance requirements, increasing costs, and supply chain risks. By fining those unfortunate to suffer

– do you consider that these should be applied to the entity, to the entity's directors/executive leadership, or a mix of the two, and why?	breaches, it deters a collaborative approach to information security, and is detrimental to increasing cybersecurity maturity. Reconsider penalties, instead consider education and early intervention (if penalties necessary, they should be appropriate to business size and turnover.

Thank you for the opportunity to provide feedback on the New Zealand Governments Critical Infrastructure Phase 1 Consultation.

If you would like further information, or to explore any of the recommendations or comments, please contact:

Rochelle Gribble, Programme Director – Complex Workstreams

Universities New Zealand

T +64 4 381 8516 | M +64 21 336 665 / Rochelle.Gribble@universitiesnz.ac.nz

Greg Sawyer – Chief Executive Officer

Council of Australasian University Directors of Information Technology (CAUDIT)

+61 414 385 539 / greg.sawyer@caudit.edu.au

Nikki Peever – Director, Cybersecurity

Council of Australasian University Directors of Information Technology (CAUDIT)

+61 450 331 287 / nikki.peever@caudit.edu.au