

One NZ submission on the DPMC discussion document on strengthening the resilience of Aotearoa New Zealand's critical infrastructure system

8 August 2023

Introduction

1. We welcome the opportunity to comment on the Department of the Prime Minister and Cabinet's (DPMC) discussion document on strengthening the resilience of Aotearoa New Zealand's critical infrastructure system (**the Discussion Document**).
2. One NZ is supportive of the outcomes that DPMC is seeking to achieve and its recognition that a pan-sectoral, systematic approach is required to strengthen resilience across New Zealand.
3. Our submission comments on the specific questions raised in the Discussion Document and includes recommendations for DPMC to consider in developing more concrete proposals and options for enhancing critical infrastructure resilience. We look forward to continuing to engage with DPMC on this project.

Summary of key recommendations

4. Summary of One NZ's key recommendations:
 - a. Include non-regulatory options for enhancing critical infrastructure resilience, alongside those that would require regulatory reform, for public consultation as part of the next phase of this project, recognising that a range of public policy tools are available to Government to drive resilience outcomes. Government should engage with critical infrastructure operators on developing alternative options, which could

be a more proportionate and equally effective means of achieving the outcomes sought. We suggest that broader options should be explored and reflected in further consultation.

- b. If the minimum resilience standards approach is adopted, the standards should:
 - i. be outcomes/principles-focused allowing flexibility on how they are practically achieved, including recognising alignment with existing regulatory/legislative frameworks as potential means to meeting the standards (particularly in sectors that are already subject to extensive regulation and oversight);
 - ii. be proportionate, recognising the differing levels of existing regulatory mechanisms and investment across different critical infrastructure sectors;
 - iii. be consistent across different categories of critical infrastructure (i.e. one type of infrastructure should not be subject to more onerous requirements than another). This acknowledges the interdependence of different infrastructure categories, and any single category cannot be more resilient than those it relies on. This is denied if inconsistent resilience requirements are applied across sectors; and
 - iv. apply to critical assets rather than critical infrastructure entities.
- c. If the Government decides to pursue enhanced resilience outcomes through regulation, methods for government co_investment and a clear cost pass-through mechanism to those who benefit must be part of the overall approach.
- d. Government should encourage and incentivise more effective information sharing across critical infrastructure operators.
- e. Assessment and monitoring of whether any resilience requirements are met must sit under a single Government agency to ensure a consistent and accurate view, which properly accounts for the interconnected and co_reliant nature of different critical infrastructure categories. In our view, Te Waihanga is best placed to perform this function.
- f. If compliance and enforcement mechanisms are adopted as part of a minimum standards approach, we recommend that:
 - i. compliance and enforcement mechanisms are developed through genuine engagement with critical infrastructure operators;
 - ii. any enforcement mechanisms are introduced under a phased approach; and
 - iii. the same rigour applies across both private and public sector critical infrastructure providers when it comes to enforcement of any minimum standards.

One NZ approach to resilience

5. Maintaining resilient networks is a core part of One NZ's business and is a critical consideration when investment decisions are made. We operate in a highly competitive market where strong incentives exist to invest into resilience to meet our customers' and shareholders' expectations.
6. As recognised in the Discussion Document, resilience has a number of domains, including physical resilience, cyber and information system resilience, and supply chain and procurement security. This broad view of resilience is reflective of how One NZ assesses risk in its own operating environment and the measures it takes to achieve resilience across our business. An overview of One NZ's approach in the key domains is provided below.

7. s9(2)(b)(ii)



8.

9. We support DPMC's recognition that 'resilience is one of many competing objectives for the infrastructure system,' with others including operating in a highly competitive environment,

affordability, efficiency and sustainability¹. The nature of competing objectives means that One NZ is required to strike the right balance between cost of resilience enhancements and associated risks. Some investments that would result in enhanced resilience outcomes cannot be achieved on a commercial basis. For example, the resilience of mobile network coverage in an area can be increased by investing in more than one backhaul link (to transfer data between a mobile site and the core network), and by duplicate electricity links or backup power supply (to maintain electrical power to a site). Whether this makes sense will depend on the characteristics of each mobile site, including its location and utilisation.

10. Consumers' willingness to pay for enhanced resilience outcomes which they will value only in the context of rare events is low. This view is based on our past experience where we invested in network enhancements (e.g. 4G and 5G services with greater capability and higher speeds), but there was no willingness among consumers to pay more for these enhanced services. The same customer response can be expected in relation to resilience enhancements, where the benefits of enhanced resilience may not be known and will not be valuable to consumers outside of specific events. Customers accessing critical infrastructure through competitive markets for services are primarily driven by price. According to Research New Zealand Consumer Telecommunications Survey (commissioned by the Commerce Commission), 'pricing' is by far the most important driver of customer satisfaction, followed (to a lesser degree) by 'coverage and availability' and 'quality of customer service'². Enhanced services, including increased resilience of services, does not show up as a factor that consumers would be prepared to pay a premium for.
11. Many resilience options are simply not economical because they must be funded through services sold in competitive markets. In competitive markets there is no certainty that costs of investment can be either passed through or recovered. An operator that prioritises resilience and invests more in its own network face competition from operators who adopt a lower cost model, offering services via less resilient network assets but at lower prices that

¹ Department for Prime Minister and Cabinet, *Strengthening the resilience of Aotearoa New Zealand's critical infrastructure system discussion document*, p. 7

² Research New Zealand, Consumer Telecommunications Survey, July 2021, p. 31, https://comcom.govt.nz/data/assets/pdf_file/0030/265539/Research-New-Zealand-Consumer-Telecommunications-Survey-2021-14-September-2021.pdf

are attractive to consumers. We've addressed this point further in the financial considerations section of this submission.

12. Where critical infrastructure is provided in competitive markets – without any clear mechanism for recovering costs of enhanced resilience outcomes – it makes more sense to focus on the readiness to respond to emergency events and restore services quickly. As recognised in the Discussion Document, ‘an organisation that uses less robust assets that are easily replaceable may be more resilient from a service delivery perspective than one that relies on highly engineered assets that take a long time to replace when they fail.’³ We agree that readiness to recover from events is as important (and sometimes even more important) than costly investments into resilience hardening.

13. **Physical resilience:** One NZ operates mobile and fixed networks. The physical, passive infrastructure that is used to deliver mobile services is now owned by FortySouth. We ensure common set of resilience standards through our agreement with FortySouth. The active equipment for delivering mobile services (e.g. antennae and spectrum), as well as power supply to the cell sites, is owned by One NZ. Disruptions to mobile connectivity are most often the result of what can be viewed as a grid failure, i.e. power outages or backhaul failures. s9(2)(b)(ii)

s9(2)(b)(ii)

s9(2)(b)(ii) During Cyclone Gabrielle, there was no damage to the integrity or structure of mobile sites or equipment on them. Mobile connectivity outages were all a result of power failure and fibre backhaul breaks. As soon as power and backhaul were restored, mobile services were up and running at full capacity. One NZ also owns an extensive fixed fibre network in the country that delivers services to businesses (but not consumers). Our consumer fibre services rely on the infrastructure owned and operated by Chorus and the Local Fibre Companies (LFCs).

14. **Cyber resilience:** s9(2)(b)(ii)

s9(2)(b)(ii)

Relative to many critical infrastructure sectors, the telecommunications industry is

³ Department for Prime Minister and Cabinet, *Strengthening the resilience of Aotearoa New Zealand's critical infrastructure system discussion document*, June 2023, p. 13

well advanced. This reflects the immediate and growing nature of cyber risks faced by our sector, the premium that our customers place on management of these risks (which drive focus and investment), and existing regulatory settings (including obligations on network operators to safeguard areas of specified security interest under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA)). One NZ invests heavily in technology solutions, including via our Cyber Defence Centre (CDC) and we prioritise cyber security to protect our customers and our network.

s9(2)(b)(ii)

s9(2)(b)(ii)

15. An example of a systemic risk related to cyber resilience is a cyber attack taking out all data centres.

s9(2)(b)(ii)

s9(2)(b)(ii)

There are an increasing number of data centres being built in New Zealand which will help mitigate this risk.

s9(2)(b)(ii)

s9(2)(b)(ii)

1 This

underlines the interconnected nature of critical infrastructure sectors, and we welcome DPMC's inclusion of data centres in the indicative list of critical infrastructure assets.

16. **Supply chain and procurement resilience:** One NZ deals with the resilience of these two areas together. We acknowledge the risks | in this space, which in One NZ's case are predominantly a result of our dependency on international suppliers for critical inputs into our infrastructure and services (for example, s9(2)(b)(ii) We have a well-developed process for addressing robustness of resilience of parties' that we do business with, which is integrated into our supplier selection process. Things like good business continuity plans and good methods for managing risk are factors that we take into consideration when deciding who to do business with. Nevertheless, there are limitations to the amount of influence we are able to exert in negotiations with large international suppliers.
17. At one of the workshops with DPMC on this consultation, a comment was made that the Government has no jurisdiction over international companies operating critical infrastructure in New Zealand which would act as a limitation when it comes to enforcing any resilience standards to these companies. An idea was floated that New Zealand-based operators of critical infrastructure could build enhanced resilience commitments into the contracts when procuring products or services from international suppliers. While we would always seek optimal commitments from suppliers, the reality is that many international suppliers offer products and services on standard terms and will not amend these to reflect the requirements of a (relatively small) local market. This is particularly true where local requirements would involve the supplier having to adjust standard operating processes or support models. If critical infrastructure resilience standards compelled local operators had to "pass through" requirements to international suppliers, we expect that this would a) be frustrated in many cases (i.e. by inability to reach agreement with suppliers that achieve this outcome), and b) limit the suppliers available to local operators, noting that many globally traded products and services – which are inputs to critical infrastructure – do not have local substitutes.

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?

18. There is a need for a more systematic approach to strengthening critical infrastructure resilience. There are currently differing levels of focus and investment in resilience across

critical infrastructure sectors – as recognised in the Discussion Document, this is an issue in a system that is so interlinked and dependant on each other for resiliency. Critical infrastructure is a system of systems, and the system is only as strong as its weakest elements. To date, beyond the work on emergency management across lifeline utilities under the Emergency Management Bill, resilience has mostly been looked at on an “intra-sector” basis, in isolation and without accounting for the interconnectedness and dependencies between sectors. For example, addressing the impact of electricity outages on telecommunications connectivity can’t be considered or addressed without the involvement of the electricity sector.

19. One NZ has been engaged in conversations about telecommunications resilience with respective portfolio Ministers for several years. While we accept there are opportunities to enhance resilience in our sector, we have also identified the need for a more joined-up approach to improving resilience, the need for immediate focus on weakest elements of the interdependent system of critical infrastructure, and a framework approach for financing of non-economic investments. It is good to see these themes addressed in the Discussion Document.
20. Accordingly, we are supportive of the outcome that DPMC is aiming to achieve of strengthened resilience across the critical infrastructure system. However, DPMC should consider different ways that this outcome could be achieved before opting for hard legislation aimed at setting and enforcing minimum resilience standards on critical infrastructure operators which is contemplated in the Discussion Document. We note that the next steps in DPMC’s work programme include ‘development of options for regulatory reform, which will then be presented for a subsequent round of public consultation.’ Non-regulatory options should also be considered as tools for enhancing resilience as part of this next phase.
21. There are a number of ways to achieve intended outcomes that don’t involve hard regulation. This could be done through tax incentives, targeted subsidies, and system improvements such as improved information sharing mechanisms. For publicly owned critical infrastructure, the Government can drive resilience outcomes through funding and procurement strategies. For example, by mandating or incentivising achievement of standards for preparedness and mitigation of cyber risks, the Government could materially reduce the impact of these risks in many of the critical infrastructure areas within its control, including the health sector where vulnerability and impact of this risk are most acute.

22. We note that the Discussion Document also recognises that non-regulatory mechanisms and existing sector-based regulatory regimes have a role to play in enhancing resilience ‘at the least cost to businesses, consumers, and government.’⁴
23. The OECD recommends seven steps for critical infrastructure resilience policy-making, with the fifth step on this list being for governments to ‘define a mix of policy tools, informed by cost-benefit analysis, to encourage operators to invest in resilience and achieve resilience objectives’ - regulation is just one of the policy tools available to government, and should not be jumped straight to before the other steps are looked at⁵. When it comes to public policy tools, OECD notes a range of options available to governments (as per the table below). We recommend that DPMC considers and consults on the different tools to deliver critical infrastructure resilience objectives, including the respective advantages and disadvantages of approaches that don’t involve regulatory reform, to develop an effective and proportionate means of achieving these outcomes.

⁴ Department for Prime Minister and Cabinet, *Strengthening the resilience of Aotearoa New Zealand’s critical infrastructure system discussion document*, p. 9

⁵ <https://www.oecd-ilibrary.org/sites/02f0e5a0-en/1/2/5/index.html?itemId=/content/publication/02f0e5a0-en&csp=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book>

Table 3.1. **Policy tools to foster critical infrastructure resilience**

| | |
|--|---|
| 1. Provision of hazards and threats information | 12. Inspections and performance assessments |
| 2. Voluntary information-sharing mechanisms or platforms | 13. Fines for non-compliance with resilience requirements |
| 3. Mandatory information-sharing mechanisms or platforms | 14. Other types of penalties for non-compliance |
| 4. Awareness raising activities and trainings | 15. Ranking based on inspection / performance results |
| 5. Resilience guidelines for critical infrastructure operators | 16. Reporting on operators resilience |
| 6. Fostering the development/use of professional standards | 17. Sharing best practices |
| 7. Incentive mechanism to assess risks and vulnerabilities | 18. Public investments in infrastructure resilience |
| 8. Incentive mechanisms for investing in resilience | 19. Guidance for sub-national levels of government |
| 9. Sectoral prescriptive regulations dedicated to CIP | 20. Mandatory insurance for critical infrastructure |
| 10. Performance-based regulations on business continuity | 21. Peer-reviews, monitoring and evaluation |
| 11. Mandatory business continuity plans | 22. Sectoral mutual aid agreements |

Note: This listing of policy tools was prepared by the OECD Secretariat, based on approaches presented at the OECD High Level Risk Forum and desk research

Source: OECD Secretariat

How would you expect a resilient critical infrastructure system to perform during adverse events?

24. The Discussion Document notes that resilience is not about hard assets but the ability to continue to deliver critical services. We agree with this view. One NZ's approach to resilience is centred around how we can adapt, flex and adjust to continue to provide services to our customers. Our core service is connectivity, and we are continuously looking at a range of innovative ways in which we can provide and improve connectivity to customers. During adverse events, we believe it is important to set the expectation that connectivity services may be limited to text, voice and basic data only due to the need to manage capacity when sites are down. One NZ's partnership with SpaceX to provide direct-to-cell services from 2024 is the latest example of our investment in innovation and diversifying ways in which we deliver connectivity through the provision of a network that can provide coverage across the landmass of New Zealand and its territorial waters. Once this service is up and running, our customers' access to satellite coverage will mean that they can remain connected if land-based mobile services are unavailable (as was the case most recently during Cyclone Gabrielle). This type of technology innovation adds an additional layer of resilience and is an example of the type of resilience investment that is incentivised by market-based competition, where the costs of this investment can be recovered on an economic basis.

Do you agree with the proposed criteria for assessing reform options? If not, what changes you would propose?

25. We note the proposed criteria for assessing reform options to strengthen critical infrastructure resilience as follows:
- a. Criterion A: how well does the option enhance infrastructure resilience?
 - b. Criterion B: how does the option change regulatory burden and regulatory certainty across the community?
 - c. Criterion C: how does the option change the regulatory system's complexity?
26. We support these criteria and recommend adding additional considerations that include:
- a. Is the option the most cost-effective way to achieve desired resiliency outcomes?
 - b. Is the option selected the most proportionate means of achieving the outcome having regard to factors including the specific outcome sought, costs and where they fall, the complexity of any change to existing processes, operations or arrangements, activities required to implement change and the timeframe within which change is sought?
 - c. Does the option promote consistency and certainty of outcomes across all sectors comprising the critical infrastructure system?
 - d. Is the option practical and achievable having regard to real world conditions?

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?

27. Having a greater shared understanding of hazards and threats is critical, and effective information sharing is a key tool for enabling this outcome. Information sharing plays an important role in fostering effective co-operation between critical infrastructure providers, both at the resilience hardening stage and during emergency management. It can also act as a way to better protect physical infrastructure: improving the quality of infrastructure location information in planning records would assist in reducing the risk of network outages that are caused by cable breaks where construction activity occurs.
28. Information sharing across sectors can also support co-investment. For example, if a local power grid is being upgraded and we had better information about when/where/how, we may consider getting involved to co-invest around more reliable and robust links to mobile sites. The initial absence of connectivity along the Transmission Gully motorway route is an

example of a missed opportunity when there is a failure to consider all critical infrastructure providers when a project is delivered. In this case, insufficient recognition and priority was given to the need to ensure mobile coverage was available when the road was opened.

What do you think the government should do to enable greater information sharing with, and between, critical infrastructure owners and operators?

29. The process for sharing of information across critical infrastructure entities needs to be improved. For example, in our experience each electricity provider shares information on outages in different formats and use different map versions. Consequently, often the only way to get accurate updates on power outages and restoration times is through manually checking each power company's website or by calling them – this is time consuming and inefficient.
30. As the owner of a number of critical infrastructure assets, the Government could encourage relevant agencies to support such approach with a view that critical infrastructure providers should in the first instance work together to come up with information sharing improvements. Regulatory intervention should only follow if no improvements are agreed within a set period.

Setting proportionate resilience requirements

Would you support the government having the ability to set, and enforce, minimum resilience standards across the entire infrastructure system?

31. As noted earlier in this submission, there are a range of public policy tools that the Government could use to deliver desired resiliency outcomes. Consideration of and consultation on different tools should be carried out before a decision is made on whether minimum resilience standards are indeed the most appropriate way forward.
32. If minimum resilience standards are chosen as the tool for delivering resilience improvements across the entire infrastructure system after further engagement and consultation with stakeholders on all the options available, it will be critical that these standards are actually consistent across the different critical infrastructure assets and proportionate (in terms of both a) their substantive requirements; and b) how compliance with these standards is ensured practically), recognising the differing levels of resilience, existent regulatory requirements and investment across critical infrastructure sectors. A staggered approach should also be adopted when it comes to compliance with any standards, with the first priority being to level up critical infrastructure sectors where resilience shortcomings are more acute.

33. We do not support the involvement of a broad range of regulators or institutions in achieving practical compliance with resilience standards. Different institutions have different practices, priorities and approaches – and will approach the task differently. This would be at odds with the need for consistent application of standards across all infrastructure sectors, and the reality that inconsistent application in one sector will inevitably affect other sectors given the systemic linkages involved. We expand on this point later in this submission.

What type of standard would you support (e.g. requirement to adhere to a specific process or satisfy a set of principles)?

34. Our view is that a set of principles would be preferable over specific processes. If the minimum resilience standards approach is adopted, the Government's role in this should be around setting resilience principles or outcomes, but not being prescriptive about how those should be achieved. There will be more than one way to strengthen resilience across the targeted assets and operators of critical infrastructure will be best placed to determine the most efficient and cost-effective ways of achieving the set outcomes. In addition, in some cases providers of critical infrastructure will already meet or exceed the minimum resilience standards through compliance with existing sectoral regulations – this should be classed as an acceptable way to meet any resilience standards.

35. As regards whether resilience standards should apply to a critical infrastructure entity or to its critical assets, our preference is on the latter. In One NZ's case, not all of the services that we provide and activities we perform are critical. For example, our retail stores would not be considered as a critical service, at least not in their ordinary operating format. Having standards that apply to the entire entity would therefore risk adding undue burden on non-critical services of that entity, and result in the imposition of additional costs that are not faced by other entities participating in the competitive markets we operate in. Standards should instead be targeted specifically – and only – at assets that are critical.

36. Engagement with critical infrastructure operators should commence at the earliest opportunity if the Government decides to proceed with the minimum standards approach to ensure that they are practically achievable. For instance, when thinking about the minimum standards for physical assets, it is likely that consideration would be given to whether these standards should relate to where infrastructure is located. While such a standard might make sense in theory, it may not necessarily be achievable in all cases in practice. For example, fixed fibre cables mostly follow the roads as that is often the only infrastructure corridor available, and any requirement to diversify fibre routes would likely be constrained by practical land access issues. This is just one example of an issue that may come up when

thinking about specific standards and it's important that such limitations are taken into account when any standards are developed.

Do you have a view on how potential minimum resilience standards could best complement existing approaches to risk management?

37. As noted above, it is important that, provided they are sufficient, existing approaches to risk management and relevant sectoral regulatory standards are deemed an acceptable way to meet any resilience standards if this approach is chosen by the Government.
38. For example, TICSA binds the telecommunications industry to a set of standards around security of our networks. Telecommunications operators are required to notify the Government Communications Security Bureau (GCSB) every time there is a change to our networks that meets a threshold set by the legislation. Such notifications are made on a proactive basis where any change to the operation of One NZ networks, systems, processes or suppliers affect an area of specified security interest.⁶
39. By way of illustration, notification has been made previously regarding changes in legal ownership of One NZ, the selection of technology vendors, selection of network equipment and location/outsourcing of operational functions. GCSB evaluate the impact of the change (whether it weakens, strengthens or is neutral on the security of our networks), meaning they have a high degree of visibility and control in the sector. Process exists for an operator to stop or undo a change that creates unacceptable risk. This existing standard is highly robust and provides for a high degree of resilience. In practice, the notification process captures any existing state or development that would create an actual or potential security risk affecting New Zealand's national security.
40. Practically, the effect of any notified action on the resilience of critical network infrastructure forms part of GCSB's consideration. This oversight process means that our sector is already

⁶ See [TICSA-Guidelines-2020-V2.0.pdf \(ncsc.govt.nz\)](#)

well advanced in cooperating and sharing information with Government on the management of risks, and a very limited, if any, additional measures are required to supplement these existing processes.

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 outcomes? If so, what options would you like the government to consider for delivering on this objective?

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?

41. The Discussion Document explores the idea of introducing additional, more stringent standards that would apply to significant critical infrastructure assets. If this proposal is adopted, a very clear criteria for what would qualify as significant and non-significant infrastructure entity would be needed.
42. Investing in a model to assess the significance of a critical infrastructure asset appears to be a sensible approach, but more detail on this model (and in particular the criteria that determine 'significance' in a consistent manner across different sectors) is required for us to comment on whether it would be a suitable tool. In addition, engagement with critical infrastructure entities would be a critical part of this exercise.
43. The significance of a critical infrastructure asset will depend on which resilience domain the assets are assessed against. For example, when it comes to physical resilience, electricity generation and distribution would likely qualify for the significant critical infrastructure asset category while financial institutions or the health sector likely would not. However, cyber and information security resilience would be highly relevant for financial and health sectors that hold highly sensitive information, and they may therefore be expected to follow more stringent cyber security standards if this two-tier system for setting minimum resilience standards is indeed adopted.
44. In any case, we do not consider that a two-tier system should be adopted from the outset. If the Government decides to proceed with the minimum standards approach, the immediate priority should be around levelling up resilience of critical infrastructure assets that have resilience issues and/or those that are not already subject to sectoral regulatory standards that drive resilience outcomes. We suggest that this would be a proportionate and effective primary focus, likely to generate the most substantial and immediate benefits for New Zealanders.

Financial implications

Do you think we have described financial implications of enhancing resilience accurately? If not, what have we missed?

45. We agree that the Discussion Document includes some helpful acknowledgements of the financial implications of enhancing resilience. It is important to recognise that resilience strengthening will come at a cost and the question of ‘who pays?’ needs to be considered accordingly.
46. We support Te Waihanga’s infrastructure funding and financing principles set out below⁷ and recommend that they are integrated into the work on how desired resilience outcomes should be funded.
 - a. ‘Principle 1: Those who benefit pay – Infrastructure services should be paid for by those benefiting from the services (the benefit principle) or creating a need for the service (the causer principle).
 - b. Principle 2: Intergenerational equity – Funding and financing arrangements should reflect the period over which infrastructure assets deliver services and be affordable for current and future generations.
 - c. Principle 3: Transparency – There should be a clear link between the cost to provide infrastructure services and how services are funded. Wherever possible, prices should be service-based and cost-reflective.
 - d. Principle 4: Whole-of-life costing – Funding requirements should include the ongoing costs to maintain and operate an infrastructure asset and the cost to renew or dispose of it at the end of its life as well as the up-front cost to construct or purchase it.


⁷ New Zealand Infrastructure Commission, *Providing and paying for infrastructure – What is fair? Issues paper*, May 2023

- e. Principle 5: Administratively simple and standardised – Administrative costs for both providers and users should be minimised unless there are clear benefits from more complex funding and financing arrangements.
 - f. Principle 6: Policies for majority of cases – Funding and financing policies should be written to work for the majority of cases. If needed, alternative or supplementary mechanisms should be added to provide flexibility and ensure fairness.’
47. For example, when considering funding of resilience hardening against Principle 3 above, it should be assumed that where services are provided in a competitive market, the prices to consumers are service-based and cost-reflective. This is the case for One NZ. We are frequently operating in a different context to infrastructure providers that offer a monopoly service, such as Transpower and Chorus. These monopoly operators can use a relatively straightforward cost pass-through mechanism in the form of a regulatory permission to on-charge the costs of compliance with a mandated resilience outcome or standard to their customers. In contrast, telecommunications providers offering services to consumers in highly competitive retail markets (with networks that are funded entirely from the provision of services in these competitive markets) can only pass on costs that consumers are willing to pay. For example, if One NZ made a \$250m investment into resilience to meet government-set standards, we would only be able to on-charge what the market will bear. If One NZ made this investment voluntarily, and other operators did not and did not incur the same cost, we cannot expect to increase prices to reflect the additional resilience benefit provided to customers. Even if all operators were required to make the same investment, there is no certainty that operators can pass this cost on to customers who benefit (because any single operator may choose not to, and may trade off lower prices and higher market share with those operators who seek cost recovery losing customers and market share to the lower priced competitor). This dynamic needs to be taken into account when the question of ‘who pays?’ for resilience hardening is considered and clear provision should be made for ability to pass through investment costs that are directly related to Government specified resilience objectives.
48. The Discussion Document notes that direct Government support for vulnerable consumers may be required to ensure that resilience does not reduce their access to critical services. If the Government is concerned with the issue of equity, then serious thought needs to be given to a mechanism that would enable appropriate support to be provided. The responsibility for providing this support should lie with the Government rather than operators of critical infrastructure. For example, operators cannot be responsible for setting access criteria for different categories of customers, and a scenario in which each does so and sets different eligibility standards would be undesirable. Support for vulnerable customers is best provided by direct and targeted transfer of funding to support access to critical services.

49. The Discussion Document recognises that the Government ‘has a responsibility to partner with industry’ to deliver resilience outcomes, including by supporting ‘owners and operators in making rational investments to enhance resilience.’⁸ We welcome and support this approach. In Australia, government co_investment models are part of the wider resilience regulatory system. It is critical that government co_funding models are built in at the time when resilience improvements are delivered and that they are aligned with Te Waihanga’s funding and financing principles included above, particularly Principle 4: that co_funding mechanisms apply to whole-of-life costings, including the ongoing costs to operate an asset.

50.

s9(2)(b)(ii)



51. Lastly, a number of essential critical infrastructure assets will be provided by the Government and so the Government will have a role to play in lifting resilience of those assets through funding models and investment decisions. It will be important that resilience outcomes are prioritised accordingly and are not traded away when funding and procurement decisions are made.

⁸ Department for Prime Minister and Cabinet, *Strengthening the resilience of Aotearoa New Zealand’s critical infrastructure system discussion document*, p. 8

Management of significant national security threats

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 that they were only used as a last resort, where necessary?

52. In our own sector, we seen no case for the Government having greater powers to intervene or direct activity in response to a threat. If contemplated, any powers to direct or intervene would require a high threshold to be used – akin to the threshold for a “step in” right under contract, where a counterparty has comprehensively failed to meet requirements, and this creates substantial risk to the party exercising the right. In addition, if the relevant threshold were met, Government would have to be confident that it has both the capacity and capability to intervene in the sector. In addition, Government intervention has potential to be significantly disruptive and it must be clear that intervention is likely to deliver benefit vs. a status quo of non-intervention. Intervention would not be appropriate, for example, simply where Government wants more information or greater collaboration from a sector, but where the sector is otherwise continuing to perform adequately in the context of a significant national security event. In the context of cyber-security events, as noted earlier in this submission, the telecommunications industry is already far advanced in this space, including through our legal obligations under the TICSA. The sector already works proactively and collaboratively with relevant agencies when faced with national security events, s9(2)(b)(ii) s9(2)(b)(ii) and we would do so in further events without Government direction or intervention. In exceptional cases, Government remains able to intervene or direct critical infrastructure sectors via legislation (as it did during the Covid-19 pandemic response) and we believe specific legislation is the appropriate course for dealing with exceptional events requiring Government response.

Creating clear accountabilities and accountability mechanisms

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?

53. Critical infrastructure is a system of systems, and the systems need to work together to achieve the intended outcome of strengthened resilience across the board. Responsibility for the resilience of New Zealand’s critical infrastructure system should therefore sit under a single agency. The Discussion Document notes that one of the principles underpinning this work programme is that ‘any response will apply to all critical infrastructures equally.’⁹ The way to achieve this and to bring a consistency of view is by dedicating this role to a single agency. We think that Te Waihanga, the New Zealand Infrastructure Commission, would be a suitable agency for this role, given its expertise and existent scope that spans across the critical infrastructure system.
54. Having multiple sectoral agencies responsible for resilience standards would very likely result in inconsistencies across critical infrastructure sectors, which would conflict with the equality principle. However, sectoral regulators will have a role to play by supporting the central resilience agency, such as through information sharing.

Do you think there is a need for compliance and enforcement mechanisms (e.g. mandatory reporting, penalties, offences) to ensure that critical infrastructure operators are meeting potential minimum standards? If so, 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?

55. As noted earlier in this submission, there are a range of public policy tools available to Government to drive specific resiliency outcomes. It is therefore important that the merits of more light-touch additional tools are seriously considered before proceeding with regulatory reform that includes minimum standards and enforcement mechanisms.
56. If compliance and enforcement mechanisms are adopted as part of a minimum standards approach, we recommend that:
-

⁹ Department for Prime Minister and Cabinet, *Strengthening the resilience of Aotearoa New Zealand’s critical infrastructure system discussion document*, p. 8

- a. Compliance and enforcement mechanisms are developed through genuine engagement with critical infrastructure operators.
- b. Any enforcement mechanisms are introduced under a phased approach.
- c. The same rigour applies across both private and public sector critical infrastructure providers when it comes to enforcement of any minimum standards.

Broader role of the Government

57. There are other areas where the Government could take action now to help strengthen resilience of the telecommunications services, including:

- a. Planning and consenting regulations: we are in need of urgent updates to the National Environmental Standards for Telecommunication Facilities 2016 (NESTF) to enable things like:
 - i. Making it easier for providers to undertake temporary activities, such as installation of temporary electricity generators and deployment of communications on wheels that are often used when networks are damaged in an emergency;
 - ii. More efficient deployment of self-contained power units (e.g. solar arrays, wind turbines and generators), which are currently excluded from NESTF, meaning that operators are required to obtain consents from individual councils in order to deploy this equipment – this is time consuming, inefficient and can result in inconsistent outcomes across different regions;
 - iii. Providing for more options for industry to install fixed line infrastructure over waterbodies; and
 - iv. Increasing the permitted footprint of cabinets to provide space for additional battery storage.

Under the proposed legislation that will replace the Resource Management Act 1991 (RMA), there is a provision for a national direction for telecommunications activities. It is critical that national direction remains the key component of the new planning system to ensure that any resilience improvements to physical infrastructure that require planning/consenting consideration are nationally consistent, rather than having to comply with differing local standards.

- b. Land access can often be a barrier to enhancing resilience. For example, public roads act as default infrastructure corridors which fixed connectivity cables run along because it is much easier than gaining access to private land or conservation estate for the purpose of laying fibre cables. If there was a desire for more diverse infrastructure corridors, land access needs to be made easier. s9(2)(b)(ii)

s9(2)(b)(ii)

- c. Procurement and funding strategy: the Government can play a role in increasing resilience across publicly operated critical infrastructure assets through its procurement and funding practices. For example, thought needs to be given to how standards around cyber security are actually going to be executed to government agencies that provide critical infrastructure, such as health.

s9(2)(b)(ii)

Confidentiality

58. Confidentiality is sought in respect of the information in this submission that is contained within square brackets and is highlighted (Confidential Information). Confidentiality is sought for the purposes of section 9(2)(b) of the Official Information Act 1982 on the following grounds:

- a. the Confidential Information is commercially sensitive and valuable information which is confidential to One NZ; and
- b. disclosure of the Confidential Information would be likely to prejudice unreasonably the commercial position of One NZ.

59. We ask that DPMC notify us if it receives any request under the Official Information Act 1982 for the release of any part of the Confidential Information, and that DPMC seek and consider its views as to whether the Confidential Information remains confidential and commercially sensitive before it responds to such requests.

60. Please contact the following regarding any aspect of this submission.

Tom Thursby

Head of Legal and Regulatory

e: tom.thursby@vodafone.nz

Kamile Stankute

Senior Public Policy Advisor

e: kamile.stankute@vodafone.nz