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

Submission | DPMC

8 August 2023

infrastructureresilience@dpmc.govt.nz

Contents

Executive Summary

Thank you for the opportunity to comment on the DPMC's (**the department's**) discussion paper relating to strengthening the resilience of Aotearoa New Zealand's critical infrastructure system.

Spark puts a lot of effort into the resiliency our networks and services. We have governance structures in place for the assessment and management of key risks, and we continue to invest heavily to make our infrastructure more resilient. There are good commercial pressures for this focus – we face demand from our end user customers for reliable services and specific resilience requirements from our emergency service, government, and critical infrastructure provider customers.

Nonetheless, while critical infrastructure providers are focused on resilience, we agree that the increasingly complex nature of the risks we face, and interconnected nature of critical infrastructure, means that it is timely to review how the critical infrastructure system is working.

The priority should be to resolve gaps in governance and lead agency structures

The paper highlights gaps in the current framework. The department notes that successive Governments have failed to take a coordinated approach to critical infrastructure resiliency, and no single agency has had policy or regulatory responsibility for New Zealand's critical infrastructure system.

We agree that this is an important gap in our approach. There should be a whole of government approach with a lead agency looking across all dimensions of the system - identifying critical services and infrastructures and national resiliency objectives, facilitating collaboration across providers and funders, and launching initiatives to improve the functioning of the system.

The absence of a lead agency has also likely contributed to missing building blocks on which the system operates. The OECD has identified that a co-ordinated government approach, national infrastructure strategy and objectives, and a clear inventory of critical infrastructure services and assets, underpin a critical infrastructure framework. However, on the face of it, none of these building blocks are available to us. As a first step to implementing the framework, we recommend that the department identify a lead agency - this could be the department or other central government agency to take this forward - working with Te Waihanga.

Government should start with voluntary minimum standards to build trust in the framework before moving to regulated minimum standards

Conversely, we don't support proposals to regulate minimum service standards immediately, ahead of the framework and governance issues being resolved and the framework being bedded in. We have yet to establish the governance framework for the critical infrastructure system, which we see as a necessary first step before we will be able to determine national resiliency gaps and initiatives to close those gaps with confidence.

Instead, we recommend that Government starts with a voluntary framework for resilience minimum standards in order to build trust with industry and critical infrastructure providers while the new regulatory framework is bedded in and the new lead agency confirms the national resilience policy that these minimum standards will be designed to meet.

This mirrors the approach being taken by other administrations. The OECD survey of member states found that authorities have implemented twenty-two policy voluntary and mandatory policy initiatives, with a clear preference from authorities to implement voluntary initiatives to promote resiliency outcomes. The preference for voluntary initiatives makes sense as managing the interdependencies across parties requires collaboration and trust.

From a practical perspective, there is a significant risk that an immediate move to regulated minimum standards and a compliance framework will simply result in providers adopting a compliance mindset in their relationship with the lead agency and the framework, that is focused on mitigating compliance risk rather than on developing a collaborative culture, innovation and initiatives that improve overall resiliency.

The lead agency will have an important role aligning Government's approach to resilience as a customer, funder, and policy maker

In our view, gaps between existing resilience standards and Government's resilience expectations are most likely to reflect the public benefits of higher resilience standards that critical infrastructure providers and customers are unable to access, rather than by underinvestment. Our observation both within our sector and in other critical infrastructure sectors is that New Zealand infrastructure owners are responsible and strive to deliver resilient networks that meet their customers' needs. We do not observe any obvious pockets of supernormal profits or rents in New Zealand infrastructure sectors.

If Government wants to establish resilience levels that exceed those that customers are willing to pay for, this will be because it sees public benefits over and above the private benefits customers see. Ensuring that Government is facilitating efficient funding mechanisms (which provide positive incentives on infrastructure providers to invest in more resilient networks) for these types of benefits will be as important, if not more important, as regulating minimum standards (which rely on penalties or negative incentives to drive that investment).

Government can provide co-funding positive incentives to invest in two ways:

- Government is the largest customer of infrastructure networks and services and thus largely drives resilience standards already. If Government was to take a more deliberate approach to valuing resilience higher as a customer this will naturally lead to increased resilience investment from infrastructure providers.

- Government operates a number of co-funding programmes already in critical infrastructure industries including telecommunications. None of these are explicitly targeted at improving resilience. In contrast, we see a much more mature approach to resilience-focussed co-funding programmes in countries like Australia. These programmes can encourage investment into otherwise-uneconomic resilience – especially in rural areas.

We recommend that the lead agency be given explicit responsibility for ensuring alignment between Government's purchasing policies and co-funding strategy and its national resilience strategy.

Introduction

1. Thank you for the opportunity to comment on the DPMC's (**the department**) discussion paper on strengthening the resilience of Aotearoa New Zealand's critical infrastructure system.

2. The paper recognises that today's critical infrastructure resilience policies must reflect the more diverse and complex events we are facing, more interdependent systems and countries, and the fast pace of innovation in infrastructure sectors.

3. Accordingly, the discussion paper seeks:

    a) To raise awareness of the trends that are placing New Zealand's critical infrastructure system's resilience under pressure.

    b) To understand how critical infrastructure failures have affected New Zealand communities and businesses.

    c) To start an open conversation with New Zealanders about what steps we should all take to support resilience.

4. In doing this, the department notes that it is particularly interested in views on:

    a) Whether this document accurately identifies the issues with New Zealand's current approach to regulating the critical infrastructure system

    b) Where relevant, ideas for possible reforms that may help address these problems.

5. The paper helpfully sets out the increasingly complex environment we operate in and highlights gaps and potential areas for improvement in our policy framework, such as a whole of government view of infrastructure and a lead agency able to work across the parties to develop national priorities and facilitate sharing of information. These are key issues that the OECD notes underpin any national resiliency framework[1]. However, there is no clear pathway for resolving the gaps identified in the paper and we recommend that this should be the priority for the department.

6. Further, the paper foreshadows a regulatory framework that would set minimum resiliency standards, place accountability mechanisms on critical infrastructure providers to verify that legal requirements are being met and empowers the Government to "step in" during a major event, directing providers to take or refrain from specific action. Our principal concern is that implementation of these powers before we have even established a specialist body to "own" critical infrastructure resilience policy for Government risks incorrect or inefficient policy specification.

7. These issues are discussed below.

Resilient Spark infrastructure

8. We face strong incentives to provide resilient services - we face demand from our customers and, as a listed entity, have comprehensive governance and reporting requirements. Accordingly, Spark takes the resiliency of its network and services seriously:

    a) We have comprehensive resiliency and governance frameworks in place. Our Business Continuity and Crisis Management Policy framework works to protect customers from

[1] The OECD Governance report sets out the key enablers in chapter 3.

the impact of disruptive events and ensures value generating activities are resilient and comply with relevant external standards, for example Civil Defence and 111 obligations. Spark's framework is benchmarked to ISO22301 and ISO 22313 and overseen by a Board committee. Spark's business continuity framework performed well when called upon during the Covid-19 pandemic and Cyclone Gabrielle.

b) Our climate change disclosures and reporting is aligned to the international Task Force on Climate-related Financial Disclosures framework. We are engaging with our industry peers, via the TCF, to explore opportunities for a sector-based approach to climate scenario analysis, partly in response to new climate reporting requirements. We have also engaged in the development of the National Adaptation Plan. improved,

c) We have a particular focus on cyber security. We take cyber security threats seriously and work hard to ensure the safety and security of both our own and our customers' networks. We have one of the largest security operation centres in the country with over 100 security subject matter experts. We have processes in place to ensure that appropriate ownership, oversight, and ongoing risk management is applied to our customers' and Spark's IT systems and data, with our cyber security subject matter experts providing oversight.

   Our Chief Information Security Officer has responsibility for Spark's cyber security, while all members of the Spark Board's Audit and Risk Management Committee have governance responsibility. We govern our security programme using the industry's best practice frameworks, including ISO27001 and NIST CSF (National Institute of Standards and Technology Cyber Security Framework). All Spark services and networks are built with multiple checks in place during the 'design', 'build' and 'operate' phases, to ensure that they are deployed with industry leading levels of security. Our security roadmap includes initiatives that will enhance our wider cyber security capabilities.

d) We are an important provider to other critical infrastructure infrastructures and services such as health, government and emergency services, and financial institutions. Our critical infrastructure provider customers determine their resiliency requirements, and

e) To support this, we continue to invest in resilient networks. We recognise that our customers rely on us to provide networks and technology that are highly reliable and available in the face of unpredictable events – from unexpectedly high levels of usage during lockdowns, to extreme weather events. Recent investments include a third "core" network to our existing mobile network core, the progressive build out of the next generation Optical Transport Network with five times the data capacity of our current network and "self healing" capabilities and upgraded Access and Aggregation network. All of these investment work to add resilience to our infrastructure and services.

9. We are keen to engage further with Government to promote resilient networks. Hence, we welcome the department stepping back and considering the framework within which resiliency is determined. On the face of it, a key issue for us is that there is no all of government perspective on resiliency to foster effective collaboration. We are dealing with multiple agencies on resiliency, none of which appear to be operating within an overall national resilience framework.

10. We further observe a difference in government attitude to resilience when government is acting as a customer as compared to when it is acting as a policy maker – an important role for a lead resilience agency to play in aligning government's resilience positions across these different roles.

Identifying the lead agency

11. We support proposals in the paper to establish clear accountabilities across government and to identify a lead agency responsible for the totality of the infrastructure system, with the capability to drive coherent policy setting[2]. Resolving the governance issue should be a priority for the department as this is an essential precursor for effectively responding to the changing environment.

A complex environment requires a system based and collaborative approach

12. We live in a more complex environment with increasing weather events and vulnerability of connected infrastructure to cyber-attacks. As noted in the paper, new technologies are deepening the connections between critical infrastructure, meaning they are more reliant on one another and – as an interconnected "system" – also more vulnerable. Overseas authorities are responding to the changing environment by3:

    a) Taking a systems approach to assessing and responding to risks across interconnected infrastructure. This requires the focus to shift from the resilience of each distinct infrastructure asset, to how infrastructure assets and the networks between them can contribute to the resilience of the whole infrastructure system4.

    b) Taking a coordinated approach to climate adaptation, in particular understanding the long-term impacts of climate change on critical infrastructure and the communities and places it serves.

    c) Focusing on how they might promote collaboration by infrastructure providers with each other, and across emergency responders, local and central government, and communities.

13. Te Waihanga and New Zealand's National Adaptation Plan for climate change both recommend taking a coordinated, systematic approach to building infrastructure resilience. Essentially noting that infrastructure resilience requires alignment, coordination and accountability across sectors, agencies and jurisdictions responsible for infrastructure planning, climate-risk management, emergency management, community resilience and land use planning.

14. Accordingly, governments have a key role to play in a resilient system, taking responsibility to ensure security and safety for communities, but also as an infrastructure policy maker, and regulator, owner or operator in some cases, and major user or client.

15. However, we don't have a joined-up approach across government that would enable this system to develop. The department notes in the discussion paper that successive New Zealand Governments have not taken a comprehensive or coordinated approach to critical infrastructure regulation. No single agency has had policy or regulatory responsibility for New Zealand's critical infrastructure system. Instead, New Zealand's regulatory approach is asset- and sector-centric.

---

[2] Page 44
[3] There are several frameworks provided by authorities - including the UN and OECD – with consistent themes.
[4] At para 62 of the discussion paper and discussed in the Australian Pathway to Resilience paper https://www.infrastructureaustralia.gov.au/sites/default/files/2021-08/Advisory%20Paper%201%20-%20A%20pathway%20to%20Infrastructure%20Resilience%20FINAL.pdf

16. The lack of a lead agency has caused problems across the board with the paper also reporting that[5]

> *The lack of a lead agency for the system has complicated coordination between the range of government agencies that do have policy or regulatory responsibility for specific sectors (for example, the Ministry of Business, Innovation and Employment in respect of energy and telecommunications). It also creates difficulties for agencies with responsibility for policy issues that cut across infrastructure sectors, such as the planning system (where accountabilities are split between central and local government).*

17. Te Waihanga similarly observed in the 30 year strategy that[6]:

> ***Coordinated approach to managing risk:*** *A sustained increase in resourcing is needed to ensure a coordinated approach to managing risk across our critical infrastructure. Lead government agencies need clearer roles for the coordination of resilience activities within and across critical infrastructure sectors. This reflects the interdependencies of infrastructure networks. These changes are required to clarify expectations of the resilience of our critical infrastructure and the roles and resourcing of the different parties involved in delivering a resilient infrastructure system.*

18. A co-ordinated approach across government is important. The OECD recommends that governments adopt a whole of government approach to critical infrastructure resiliency, ensuring the interests of all stakeholders are managed and to make the relevant trade-offs. The key policy questions being:

> *Is there a national strategy or policy document for critical infrastructure resilience? Is there a definition for critical infrastructure? Is a pre-defined list of critical infrastructure sectors in place? Is there a whole-of-government approach to the development of critical infrastructure resilience? Are all relevant hazards and threats considered in the critical infrastructure resilience policy? Is there a dedicated coordination entity responsible for designing, monitoring and adjusting the national critical infrastructure resilience policy?*

Ensuring a lead agency and whole of government approach

19. We believe that the lack of a lead agency has led to little progress being made on other enablers for a more resilient system such as the identification of national resiliency objectives, identification of critical services and infrastructures that the system needs to cater for, and development of guidelines. For example, the OECD's 2019 survey below – in effect an indicator of the maturity of the member country frameworks – suggests that New Zealand has no:

    a) Lead institution responsible for bringing together and co-ordinating across government and industry (New Zealand has sector specific leads).

    b) Overarching critical infrastructure strategy, nor

    c) Settle definition of critical infrastructure for our context or national inventory of critical services and infrastructure assets.

[5] At para 115

[6] At page 93. https://media.umbraco.io/te-waihanga-30-year-strategy/1sfe0qra/rautaki-hanganga-o-aotearoa-new-zealand-infrastructure-strategy.pdf

Figure 11.8 from the OECD 2019 survey of member country implementations[7]

Version 1 - Last updated: 08-Jul-2021
Disclaimer: http://oe.cd/disclaimer

11.8. Critical infrastructure strategy, definition and national inventories, 2016 and 2019

	Critical infrastructure protection strategy		Definition of critical infrastructure	Sectors identified	Lead institution identified	National inventory of critical infrastructure assets, systems, functions or operators
	2016	2019	2019	2019	2019	2019
Australia	●	●	●	●	●	●
Austria	●	●	●	●	●	●
Belgium	...	...	●	●	●	...
Canada	●	●	●	●	●	●
Chile	...	●	○	●	●	●
Czech Republic	...	●	●	●	●	...
Estonia	●	●	●	●	●	●
Finland	●	●	●	●	●	○
France	●	●	●	●	●	●
Germany	●	●	●	●	●	●
Greece	...	○	○	●	●	○
Iceland	...	●	...	●	...	...
Ireland	●	●	●	●	●	○
Israel	●	●	●	●	●	●
Italy	...	○	○	●	○	...
Japan	●	●	●	●	●	○
Korea	●	●	●	●	●	●
Latvia	○	●	●	●	●	●
Luxembourg	●	●	●	●	●	●
Mexico	...	...	●	●	...	...
Netherlands	●	●	●	●	●	●
New Zealand	...	...	●	●	...	...
Norway	○	●	●	●	●	●
Poland	●	●	●	●	●	●
Portugal	○	○	●	●	○	●
Slovak Republic	...	...	...	●	...	...
Spain	●	●	●	●	●	●
Sweden	●	●	●	●	●	○
Switzerland	●	●	●	●	●	●
Turkey	...	...	●	●	...	...
United Kingdom	●	●	●	●	●	●
United States	●	●	●	●	●	●
OECD Total						
● Yes	19	24	27	32	25	19
○ No	3	3	3	0	2	5
... Missing	10	5	2	0	5	8

Source: OECD Survey on Governance of Critical Infrastructure (2016, 2018 and 2019-2020)

20. Accordingly, resolving limitations in the New Zealand framework should be as priority as – without a settled governance structure and strategy – it is not possible to make material progress on national resiliency, nor know whether any specific policy initiatives are likely to improve or detract from overall resiliency outcomes.

21. We appreciate this is a material bit of work that will require sustained effort. Again, the OECD survey of member countries illustrates the range of critical infrastructures and government organisations that would need to be engaged in national resiliency. However, identifying a lead organisation and developing a whole of government view on resiliency is a critical first step for addressing these gaps.

[7] All figures from OECD Good Governance for Critical Infrastructure Resilience. https://www.oecd.org/governance/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm The New Zealand response reflects that we have sector specific lead agencies and frameworks rather than a lack of any framework.

Information sharing and scenario analysis

22. Under the new climate reporting regulation individual infrastructure companies are required to undertake climate scenario analysis to understand risk. Organisations have been encouraged to engage at the sector level, and the XRB has published guidance on sector-level climate scenario analysis. Critical infrastructure involves the interdependencies of multiple sectors, meaning a sector-by-sector approach to climate scenario analysis may not adequately identify risks and mitigation opportunities.

23. The alignment of critical infrastructure sector climate scenario analysis, and a coordinated approach to the integration of critical infrastructure risk into the next national climate risk assessment, has the potential to strengthen our collective response. However, without a central coordinating agency it will be difficult to align across multiple sectors.

Resolving for gaps in the resiliency framework

24. The lead agency will have an important role aligning Government's approach to resilience as a customer, funder, and policy maker.

25. In our view, gaps between existing resilience standards and Government's resilience expectations are most likely to reflect the public benefits of higher resilience standards that critical infrastructure providers and customers are unable to access, rather than by underinvestment.

26. Our observation both within our sector and in other critical infrastructure sectors is that New Zealand infrastructure owners are responsible and strive to deliver resilient networks that meet their customers' needs. We do not observe any obvious pockets of supernormal profits or rents in New Zealand infrastructure sectors. Nor do we see evidence of regulators or investors consistently making inefficient trade-offs between resiliency and recovery costs.

27. If Government wants to establish resilience levels that exceed those that customers are willing to pay for, this will be because it sees public benefits over and above the private benefits customers see. Ensuring that Government is facilitating efficient funding mechanisms (which provide positive incentives on infrastructure providers to invest in more resilient networks) for these types of benefits will be as important, if not more important, as regulating minimum standards (which rely on penalties or negative incentives to drive that investment).

28. Government can provide co-funding positive incentives to invest in two ways:

    a) Government is the largest customer of infrastructure networks and services and thus largely drives resilience standards already. If Government was to take a more deliberate approach to valuing resilience higher as a customer this will naturally lead to increased resilience investment from infrastructure providers.

    b) Government operates a number of co-funding programmes already in critical infrastructure industries including telecommunications. None of these are explicitly targeted at improving resilience. In contrast, we see a much more mature approach to resilience-focussed co-funding programmes in countries like Australia. These programmes can encourage investment into otherwise-uneconomic resilience – especially in rural areas.

29. Conversely, an approach that relies on minimum regulated standards and the principle that those who benefit should pay is likely to be difficult to apply in practice and inefficient. There is more risk of miss-specifying the desired level of resiliency, and the shared nature of infrastructure and costs means that multiple groups will benefit from additional investment. The

proposed approach risks pushing the funding burden on to telecommunications consumers least able to avoid the costs rather than from those who benefit from the investment most.

30. We recommend that the lead agency be given explicit responsibility for ensuring alignment between Government's purchasing policies and co-funding strategy and its national resilience strategy.

Regulatory proposals

31. The department also proposes to develop a regulatory framework that would:

    a) Set minimum standards for infrastructure providers, and

    b) Place accountability mechanisms on critical infrastructure providers to verify that legal requirements are being met. Mechanisms could include targeting of the provider itself (regular reporting and performance assessments) and/or directors and other responsible individuals in a similar way to workplace health and safety.

32. We do not support the proposed regulatory proposals. We can't know whether any proposed standard would lead to the right level of resiliency without clarity on national resiliency objectives and a proper understanding of the linkages between critical infrastructure providers. Further, without these building blocks in place, we can't be confident that any regulatory initiatives will improve (or detract from) the desired levels of resiliency.

33. The OECD advises that while mandatory requirements have strengths, they can also prove costly and create lags of time between technological developments in many sectors that require regular updates. Further, the OECD recommendation highlights that policy initiatives are specific to the national circumstances and culture. For example, the OECD survey of member countries identified 22 policy initiatives – ranging from prescriptive regulatory tools, compensation mechanisms, to voluntary frameworks based on partnerships between government and operators – with a clear preference for voluntary frameworks to strengthen critical infrastructure resilience. There is no one size fits all.

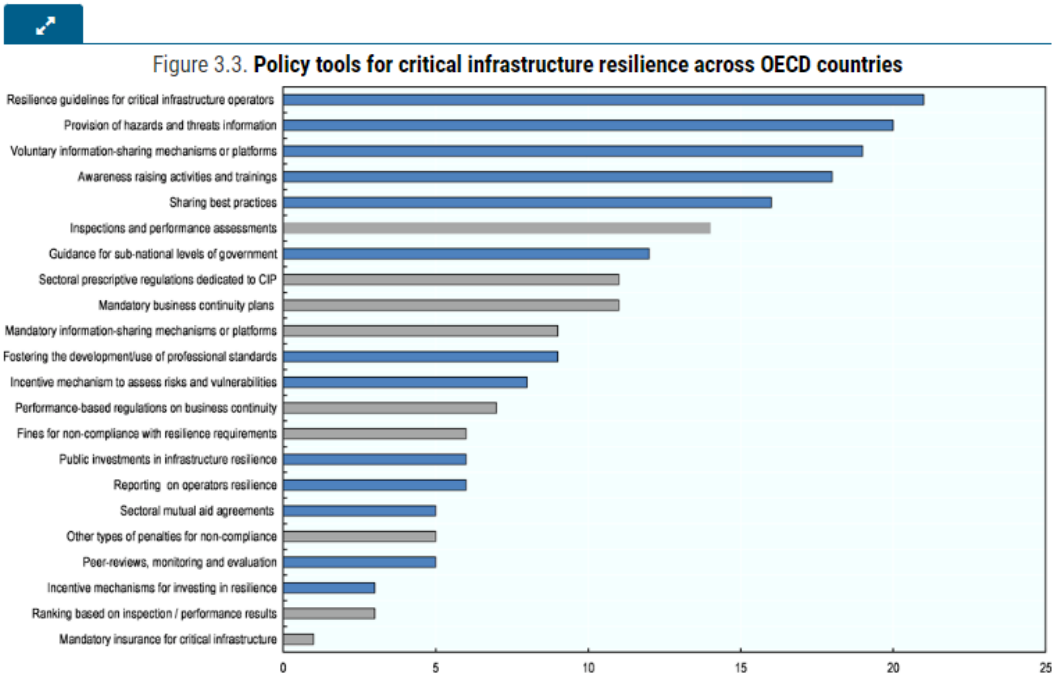
34. The OECD further reports that – overall – countries need to find the right combination between mandatory and voluntary frameworks to enhance stakeholder engagement in resilience:

    a) Instruments such as guidance for sub-national levels of governments, awareness raising activities and trainings, provision of hazards and threats information, resilience guidelines for critical infrastructure operators and voluntary information sharing mechanism are the policy tools that are the most commonly used by OECD governments.

    b) On the contrary, more stringent tools, such as inspections and performance assessments, sectoral prescriptive regulations, or mandatory business continuity plans, are less utilised by OECD countries to foster critical infrastructure resilience.

35. The OECD attributes the preference for voluntary frameworks to authorities seeking to engage operators in broad multi-stakeholders' partnerships with governments, which enables building trust between the public and the private sector. The OECD expects mandatory approaches to become more acceptable in future years once trust has been established and the value of these partnerships widely acknowledged.

Range of policy tools for critical infrastructure resilience across OECD countries and number of countries where they have been implemented[8]



36. We agree with the OECD. From a practical perspective, an immediate shift to the proposed regulatory compliance framework with regulated minimum standards is likely to undermine the development of the critical infrastructure system and outcomes. This is because the proposed approach will inevitably result in providers taking a compliance mindset to regulated obligations, focusing on managing their statutory compliance risk against the measure rather than resiliency itself. It will undermine the sharing of information and desired collaboration as parties will be concerned that they risk a compliance failure.

37. Further, it's unclear how the claimed benefits will come about in our sector. Infrastructure providers are already investing for resiliency, and our critical infrastructure customers – of which the Government is the largest – routinely set their desired communications resiliency and performance in contracts with telecommunications providers. Remaining resilience "gaps", then, largely reflect resilience investments that would deliver public benefits but not private benefits that neither telecommunications infrastructure providers nor customers can access. These gaps should be addressed through co-funding arrangements rather than regulated standards or imposts.

38. For the same reason, we also do not support the proposed PELOS which, in our view, are more likely to result in less useful information being made available to dependent parties (as any metric will need to be couched with riders depending on the restore scenario) and reduces flexibility in responding to an event (as providers will be focused on meeting a pre-defined metric rather than the otherwise highest value outcome during an emergency).

[8] Source: OECD Survey on Critical Infrastructure Resilience (2018). OECD countries responded to the survey as of 10 September 2018 – mandatory tools are in grey, voluntary tools are in blue.

39. The proposed regulatory responsibilities and standards assume a gap in resiliency outcomes but we haven't yet done the work to know whether or not the gap is real, nor which policy response will address any gaps and best promote desired system outcomes and investment in resilient infrastructure.

Other questions

40. The department has also asked for views on:

Information sharing

If you are a critical infrastructure owner or operator, what additional information do you think would best support you to improve your resilience?

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

41. Having access to data and modelling is essential to support Spark and other infrastructure providers to understand where infrastructure assets, and the services they provide, are exposed and vulnerable to the impacts of climate risk. Access to data and modelling enables prioritisation of investment for asset risk management to ensure services can continue if disruption occurs.

42. This data will also inform long-term decisions on infrastructure design and investment, so the right infrastructure is in the right places and the appropriate programmes of work are in place to maintain, upgrade, repair or replace existing infrastructure.

43. Spark believes it is vital to provide centralised modelling of natural hazards and climate change to ensure all organisations have equitable and consistent access to the best and most up to date modelling data. Our current RMA planning system often makes poor decisions due to the lack of current modelling data on climate and natural hazards. Data is critical to making good decisions as part of the National Adaption Plan, spatial planning via the Regional Strategic Plan, and supporting the location of activities and growth in Natural and Build Environment Plans.

Minimum regulated standards

Would you support the government being able 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?*

44. At this stage, we do not support mandatory minimum standards and compliance framework. It is unclear whether they are necessary and risk undermining collaboration necessary for implementing important elements of the framework. The Government priority should be to identify a lead agency and implement key enablers as set out in the OECD guidance.

Would you support the government investing in a model to assess the significance of a critical infrastructure asset is, 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?*
- *what criteria would you use to determine a critical infrastructure asset's importance?*

45. We agree that there may be critical infrastructure that requires more focus or higher levels of resilience. However, as discussed above it is unclear how this can be achieved ahead of the other framework enablers.

Step in powers to direct providers where a significant event arises

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?*

46. The decision to exercise powers should be made by the responsible Minister and be publicly notified.

Accountability within Government

Do you think that 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?*

47. There should be a single lead agency to co-ordinate and ensure a whole of government approach across the system. However, within that framework, there may be expert operational responsibility such as for cyber-security.

48. An effective resiliency framework would need to apply across all parties, including emergency services and publicly provided critical infrastructure. Therefore, the lead agency will need to work across a range of private and public critical service providers. We recommend a core government department with Te Waihanga could lead this activity.

Critical infrastructure compliance

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

- *do you consider that legal obligations should be applied to the entity, to the entity's directors/executive leadership, or a mix of the two?*

49. As above.

[End]