TCF Submission to DPMC
On Lifting Resilience of New Zealand's Critical Infrastructure
8 August 2023

Introduction

1. Thank you for the opportunity to comment on the discussion document on enhancing the resilience of Aotearoa New Zealand's critical infrastructure. We appreciate the work DPMC is doing in this area.

2. This submission is provided by the New Zealand Telecommunications Forum (TCF). The TCF is the telecommunications sector's industry body which plays a vital role in bringing together the telecommunications industry and key stakeholders to resolve regulatory, technical and policy issues for the benefit of the sector and consumers. TCF member companies represent 95 percent of New Zealand telecommunications customers.

3. We cover the following areas in our submission:

    a. Support for an integrated and systems-based approach to critical infrastructure resilience

    b. An introduction to telecommunications infrastructure and investment

    c. Some international examples of an integrated approach to infrastructure regulation and investment

    d. Cost assumptions

    e. Minimum resilience standards

    f. Information sharing

    g. Powers for national security risks

h. Government coordination

i. Other barriers to resilience (resource management system and land access issues).

4. This submission focuses on the physical infrastructure resilience domain.

Executive summary

5. The TCF supports, in principle, a **move to a more integrated and systems-based approach** to infrastructure resilience. However, we think further work is needed to determine the most appropriate policy options to achieve the systems-based approach and whether regulation is needed.

6. We recommend that Aotearoa New Zealand follow OECD best practice and work through the seven steps (set out below at paragraph 14) for governments looking to develop critical infrastructure resilience policies. This will involve a staged process starting with work to assess interdependencies, put information sharing mechanisms in place, build partnerships, foster collaboration and develop a strategy for resilience of critical infrastructure that sets out a vision with objectives we can all get behind.

7. Once the above work has been done we can move to step five, choosing the right mix of policy tools for Aotearoa New Zealand. Regulatory approaches are just some of the 22 options in the OECD policy toolkit. The OECD recommends[1] that countries at the early stages of the policy making process for resilience of critical infrastructure should take a staged approach, starting with a focus on creating stakeholder partnerships and voluntary approaches that encourage collaboration. Most countries are currently taking a voluntary approach.

8. If a decision is made to take a regulatory approach with minimum resilience standards, we agree that it makes sense to start with the critical infrastructure sectors that are currently unregulated and less advanced in their resilience investment. We think it's useful to **distinguish between**:

    a. Privately owned critical infrastructure (such as telecommunications) that is highly regulated and very competitive, with strong incentives from customers and shareholders to continue to invest in resilience where it makes sense. The telecommunications sector invests around $1.62 billion per year, and has recently completed major upgrades with the move from copper to fibre and the introduction of 5G. We also meet the costs of fixing our infrastructure when it is damaged.

[1] See chapter three: https://www.oecd-ilibrary.org/sites/02f0e5a0-en/1/2/3/index.html?itemId=/content/publication/02f0e5a0-en&_csp_=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book

b. Publicly owned infrastructure systems (such as water) where there has been years of underinvestment and a number of recent failures.

9. If a **choice of minimum standards** is to be made, we think principles or outcomes based regulation is the way to go. The advantage of standards that focus on outcomes is that it provides flexibility to use a range of approaches, innovations and emerging technology to provide resilience. Ideas for any sector specific minimum standards should first be discussed with the relevant sectors to see if voluntary approaches can work, rather than reserving these ideas for legislation which may be overly prescriptive and have unintended consequences.

10. We also note that while some countries that have applied minimum standards to critical infrastructure, regulation is often complemented with **government co-investment**. Aotearoa New Zealand should do the same if a decision is made to regulate. Government would also need to provide financial support to households on low incomes that could not afford inevitable price increases, and ensure that other regulatory systems (such as resource management) support resilience efforts.

11. Improving **information exchange** between critical infrastructure entities and government, and between critical infrastructure sectors, is an area we support. We think government should start with voluntary approaches, building a secure information sharing platform, and providing ways for sectors to engage with each other to better understand interdependencies. We also recommend that information sharing mechanisms are co-designed to ensure they are effective and don't have unnecessary administrative burdens. It is also essential that critical infrastructure entities or sectors are not required to provide resilience information or report to multiple places in government.

12. We support the proposal for **a central, coordinating agency**. If this is done, the relationship to NEMA and sector based regulators should be clearly mapped out. The coordinating agency should also have more practical functions, such as bringing critical infrastructure sectors together to understand interdependencies and co-design solutions. This is essential to a systems approach. Te Waihanga could perhaps serve this function.

Support for a more integrated and systems-based approach to infrastructure resilience

13. We agree that a more integrated approach to infrastructure resilience is needed. The recent extreme weather events in the North Island highlighted the interdependencies between critical infrastructures, as set out in our recent resilience report.

14. In principle we also support the move to a systems-based approach to tackle the interdependencies of critical infrastructure. However, we do not think that Aotearoa New Zealand should jump directly to regulation to achieve the systems-based approach. Instead we recommend that government follow OECD guidance and work through the OECD's seven steps (set out below) for governments looking to develop critical infrastructure resilience policies.

> ## Towards a more structured approach: seven steps for critical infrastructure resilience policies
>
> This report proposes a Policy Toolkit on Governance of Critical Infrastructure Resilience, which invites governments to address the following seven interrelated governance challenges:
>
> 1. **Creating a multi-sector governance structure for critical infrastructure resilience**. Governments should adopt a whole-of-government approach to critical infrastructure resilience, covering the different risks and infrastructure sectors.
> 2. **Understanding complex interdependencies and vulnerabilities across infrastructure systems to prioritise resilience efforts**. Governments should adopt methodologies and metrics to identify the critical functions, systems and assets that should be prioritised for investment in building resilience.
> 3. **Establishing trust between government and operators by securing risk-related information sharing**. Governments should establish information-sharing platforms with operators of critical infrastructure for a comprehensive and shared understanding of risks and vulnerabilities, ensuring the security and confidentiality of information shared.
> 4. **Building partnerships to develop a common vision and agree on achievable resilience objectives.** Governments should establish a continuous dialogue with critical infrastructure operators from the public and the private sectors, taking public expectations as a starting point.
> 5. **Defining the policy mix to prioritise cost-effective resilience measures across infrastructure lifecycles.** Governments should define a mix of policy tools, informed by cost-benefit analysis, to encourage operators to invest in resilience and achieve resilience objectives.
> 6. **Ensuring accountability and monitoring implementation of critical infrastructure resilience policies.** Government should monitor implementation and evaluate progress in attaining resilience objectives, with a clear accountability framework for operators.
> 7. **Addressing the transboundary dimension of infrastructure systems.** Government should co-ordinate national critical infrastructure resilience policies with neighbouring countries and beyond, to address transboundary dependencies.

15. Under the OECD approach, regulation as a policy approach is not considered until step five. We note that New Zealand has not yet done the work needed for steps one to four. We do not yet have a multi-sector governance structure and clarity in government on who is responsible for what. There hasn't yet been an assessment of interdependencies. Information sharing platforms and other mechanisms are not in place. There hasn't been an attempt to build partnerships, or provide mechanisms for critical infrastructures to come together with government to discuss interdependencies and agree on a common vision or strategy and achievable resilience objectives or targets. The TCF recommends that government start with

partnership building, information sharing and strategy making. Then pause and review.

16. Once we get to step five, there is a wide range of options to consider. These range from voluntary frameworks based on partnerships at one end of the spectrum, to prescriptive regulatory tools at the other. Twenty two policy tools are identified (see table 3.1 below). The OECD advice is that the appropriate mix of policy tools should be informed by cost-benefit analysis. It is not possible to know the right policy mix for Aotearoa-New Zealand if the earlier steps have not been worked through.

17. The work on policy options (considering both voluntary and regulatory approaches), and the work in steps one to four, needs to be done before DPMC presents options for public consultation. Critical infrastructure operators should be engaged in the work.

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

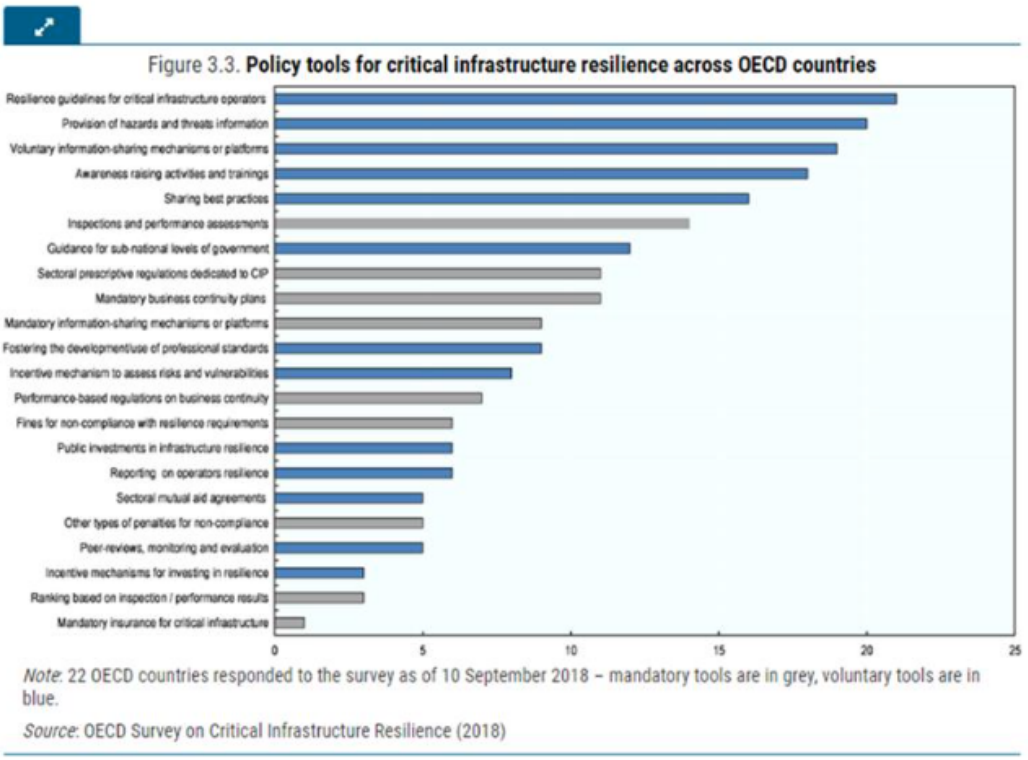
Note: This listing of policy tools was prepared by the OECD Secretariat, based on approaches presented at the OECD High Level Risk Forum and desk research

Source: OECD Secretariat

18. The OECD notes that most countries are currently using voluntary tools, such as resilience guidelines, awareness raising activities and training, providing all hazard and threat information, and putting in place voluntary information sharing mechanisms. Tools such as sectoral prescriptive regulations are used less often. The OECD recommends[2] that countries at the early stages of the policy making process for resilience of critical infrastructure should take a staged approach, starting with a focus on creating stakeholder partnerships and voluntary approaches that encourage

[2] See chapter three: https://www.oecd-ilibrary.org/sites/02f0e5a0-en/1/2/3/index.html?itemId=/content/publication/02f0e5a0-en&_csp_=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book

collaboration. Figure 3.3 (from the OECD toolkit), shows that voluntary approaches are more common.



19. If, once government has worked through the OECD steps, and put in place systems-based governance, partnership and information sharing mechanisms, and cost benefit analysis suggests that regulation is needed, we are of the view that regulation needs to be part of a broader package that also includes:

    a. government co-investment models for uneconomic levels of investment in resilience (we discuss some international precedents for this below)

    b. support for households on low incomes that will not be able to afford inevitable price increases

    c. practical support to bring critical infrastructure operators together to identify interdependencies and co-design resilience improvements

    d. other regulatory systems, such as resource management, supporting and enabling the sector to carry out resilience-related activities.

20. In the event that the government decides to take a regulatory approach, we share our thoughts later in this submission on how potential regulatory approaches, and in

particular minimum standards and reporting, would need to be considered by government to avoid unintentional consequences.

21. We do have some concerns that despite DPMC's best intentions for a systemic and integrated approach to resilience regulation, some interdepartmental chaos will result. This starts with the Emergency Management Bill being progressed separately and on a different timeline. We share MBIE's concerns[3] about the risks of regulatory confusion and unnecessary compliance costs. To this list we add the risks of departmental confusion, responsibilities being duplicated or falling between the cracks, and resourcing issues. Obviously DPMC can't control the timing of the Emergency Management Bill, but the disjunct in the timing means that DPMC will need to pay extra attention to departmental responsibilities as part of this and related policy processes. It will also be important to stay involved in the implementation phase and conduct the interdepartmental orchestra.

An introduction to telecommunications infrastructure and investment

22. In this section we provide some background information on infrastructure investment in the telecommunications sector.

What is telecommunications infrastructure?

23. Telecommunications infrastructure is the physical assets and systems needed to run telecommunications networks. It includes cables (underground, overground, and undersea), towers and antennas that enable mobile communication through the use of radio spectrum, satellites, central offices/exchanges that contain the electronics that provide service to customers, and roadside cabinets that store electronics, back-up power supply, and other equipment.

Incentives to invest in resilience are different for private and publicly owned infrastructure

24. Privately owned telecommunications infrastructure exists within a highly competitive and regulated industry with incentives to invest in infrastructure resilience, to meet customer and shareholder expectations. These incentives are not necessarily present for publicly owned infrastructure, such as water, where there has been significant underinvestment and infrastructure failure around the country.

25. Telecommunications is a sector where new technology is continuously evolving and being adopted by consumers and rolled out across networks. Take for example the transition from copper to fibre in recent years. This project has been the envy of many countries, including Australia. The 5G roll out is another example. 5G technology will enable a diverse range of products and services across multiple

[3] MBIE's concerns are set out in the proactively released Cabinet paper on the Emergency Management Bill.

sectors and make a significant contribution to the economy. As will future and emerging developments such as satellite.

There is ongoing significant investment in telecommunications infrastructure

26. The telecommunications industry invests around $1.62 billion per year in fibre access, mobile, core and backhaul networks, and the IT systems needed to make all this work[4]. In the ten year period from 2011-2020, $16.08 billion was invested[5]. This investment in the reach and performance of networks is critical to resilience.

27. Here are some (non-exclusive) examples of resilience work and investment our members have on the go at the moment:

    a. Building more diversity into core networks (which provide intercity or town linking) to better serve communities. This is about building new routes and improving the resilience of existing ones

    b. Auditing power requirements

    c. Upgrading batteries that need replacement to ones with greater capacity

    d. Adding to the generator fleet

    e. Distributing more cell sites on wheels (portable cell sites with backup power) around the country

    f. Making improvements to central offices (exchanges)

    g. Real-time monitoring of power outages, generator placements and site alarm status.

Some international examples of an integrated approach to infrastructure regulation and investment

28. We noted in our introductory comments that an integrated approach to infrastructure resilience needs to include models for government co-investment. Here are some examples of countries where governments are co-investing with telecommunications providers to improve resilience. We also provide examples of countries that are developing resilience strategies that signal priorities, and providing mechanisms for critical infrastructure sectors to engage with each other and with government.

---

[4] Information from Commerce Commission. See page 25 of ANNUAL TELECOMMUNICATIONS MONITORING REPORT

[5] See table on page 5 of this Commerce Commission report.

Australia

29. Australia is a good place to look, as it has the regulatory model DPMC is considering. Australia doesn't just regulate - it recognises it also must co-invest in resilience. For telecommunications this investment started in response to the Australian bush fires in 2020 with the STAND (Strengthening Telecommunications Against Natural Disasters) programme. The Mobile Network Hardening Programme (MNHP), part of STAND, is still operating. Stage one of the first MNHP round provided grant funding to enhance battery back up at mobile sites. Stage two provided grant funding for resilience upgrades. Round two will focus on improving multi-carrier mobile coverage on regional roads.

30. Australia also has a Telecommunications Disaster Resilience Innovation Programme that funds projects to improve the preparedness of Australia's telco networks against increasing climate risks and natural disasters. Round one is focused on innovative solutions to strengthen resilience of telecommunications against the impacts of power outages.

Norway

31. Norway co-invests in the telecommunications resilience requirements it imposes. On the regulatory side it provides that sites designated under the Enhanced Electronic Communications Programme (EEC) must be able to run up to a certain number of hours, and have a physically diverse redundant backhaul route. The regulator chooses the sites and estimates funding requirements in consultation with mobile operators. Grant funding is provided for capex and opex over a 10 year period.

Canada

32. The Investing in Canada Plan has a number of objectives, including support for resilience of communities. In the first phase of the Plan, funding was made available for the repair and modernisation of key infrastructure. As part of its resilience spend it is, for example, investing in broadband networks, mobile and cellular projects, and energy efficiency and reliability. Much of the funding is being delivered through bilateral agreements between Infrastructure Canada and the provinces and territories. Funding is provided on a cost sharing basis.

33. This investment sits alongside sector resilience initiatives such as its Telecommunications Reliability Agenda. The Canadian Government uses a mix of tools to progress this agenda including the investment mentioned above, as well as government-industry committees, programmes and regulatory instruments.

34. The Canadian Forum for Digital Infrastructure Resilience is a voluntary, consensus-based action-orientated public-private collaboration formed to enhance

the resilience of Canadian critical digital infrastructure. It was established to support Canada's National Strategy for Critical Infrastructure. The Strategy provides a common approach that enables partners to respond collectively to risks and target resources to the most vulnerable areas of critical infrastructure. It has a strategic objective to build partnerships to support and enhance critical infrastructure resiliency. Sector networks are an important part of this. The Strategy also refers to the development of a wider range of information sharing products and improved delivery and security mechanisms.

United Kingdom

35. The UK also has a resilience strategy - the UK Government Resilience Framework. The Framework focuses on the foundational building blocks of resilience, developing a shared understanding of contingencies, and setting out a plan to 2030 to strengthen the frameworks, systems and capabilities which underpin the UK's resilience. Systemic changes are being made over time.

36. Strengthening partnerships with the private sector, information sharing and government investment are part of the Framework. The UK Government will provide guidance on risk in order to help the private sector meet new standards on resilience. Standards for critical infrastructure will be common but flexible. These standards will be enforced through regulation only in the highest priority cases and where sectors are not already regulated.

Testing some assumptions about where the costs lie

The taxpayer (government) doesn't pay to fix our infrastructure

37. The paper raises some concerns about under investment in resilience leading to costs to the taxpayer to repair critical infrastructure if it is damaged in a major event. This is another area where we need to distinguish privately owned infrastructure (such as telecommunications) from publicly owned infrastructure (such as roads, bridges and the national electricity transmission system). If telecommunications infrastructure is damaged in a natural disaster, the cost of repairing it (as a temporary fix and long term) sits with the companies who own it, not the government/taxpayer.

38. Our members are, for example, absorbing the costs of repairing and replacing fibre cables damaged during Cyclone Gabrielle through road collapse.

It is cheaper to invest ahead of time than to pay to fix things when they break

39. Telcos invest in resilience ahead of time, for example by hardening key mobile sites and investing in duplicate backhaul, and through business continuity measures. The likelihood of an event occurring and the number of customers in a given area may mean it is not always economic to build in diversity ahead of time. Sometimes it

makes more sense - even in the longer term - to have a plan to fix damaged infrastructure and restore service quickly, rather than building in additional resilience that is costly and unlikely to be needed.

Will government subsidise increased costs for people experiencing income poverty?

40. The discussion paper notes that regulating for infrastructure resilience could or probably would drive up costs that would be passed on to consumers. It goes on to says that government would minimise the scale and consequences of cost increases in a number of ways, including by considering direct government support for more vulnerable New Zealanders, to ensure that resilience does not reduce their access to critical services. An alternative approach could be to co-invest with infrastructure providers so they don't have to pass on costs of uneconomic upgrades to consumers.

41. If government is seriously considering government subsidy as an option we recommend that the necessary policy work is approved by Cabinet and a budget bid be progressed before any new regulation is enacted. Our experience to date is that government has not been prepared to provide long-term investment in supporting New Zealanders experiencing income poverty to be able to access essential services such as internet. Although there is a precedent for electricity with the Winter Energy Payment. DPMC should talk to DIA (GCDO) about the difficulty it has experienced in progressing digital equity policy.

Minimum standards

42. The discussion document asks for feedback on the idea of minimum standards as part of a systems-based approach to regulating for critical infrastructure resilience. While we do not think New Zealand should move to a regulatory option at this stage, we share our views on minimum standards if this approach is progressed:

    a. Principles or outcomes based regulation is our preferred approach. It has worked well for the roll out of UFB around the motu. The advantage of regulating for outcomes is that it provides flexibility to use a range of approaches, innovations and emerging technology to provide resilience. The government's focus here should be on setting outcomes that it is seeking to achieve and leaving it up to each critical infrastructure operator to determine the most efficient and cost-effective way to achieve this. Existing sectoral regulatory frameworks should also be considered as appropriate means to meet any new standards.

    b. Process-based requirements, along the lines of those included in the Australian resilience legislation (e.g. a requirement to adopt a standard process or risk-based management framework, an annual requirement to

identify critical assets, or have a mitigation strategy) could be an approach that works for different types of critical infrastructure, regardless of where entities are at with their resilience journey. It would, however, depend on how these standards were framed. As noted above, we think there is value in providing some flexibility in how to comply. Process-based requirements are therefore not our preferred or recommended approach.

c. The possibility of sector-specific minimum standards has been discussed at the consultation hui. This approach would conflict with one of DPMC's key principles for its critical infrastructure work programme, that "any response will apply to all critical infrastructures equally". Further, as recognised in DPMC's discussion document, critical infrastructure is an integrated system, with the different assets relying on each other to deliver resilience across the board. Enhanced critical infrastructure resilience, and a systems-based approach, cannot therefore be achieved by tactical, sector-specific interventions. We do not support the idea of sector-specific minimum standards.

d. Minimum standards will not always improve resilience. Take for example PELOS - the planning emergency levels of service - proposed under the Emergency Management Bill. MBIE's advice[6] was that PELOS is unlikely to provide meaningful information to communities, other critical infrastructure operators or CDEM groups because of the significant number of assumptions and caveats operators will need to put on restoration times. Minimum standards that prescribe response or recovery times are problematic when matters are beyond the control of an infrastructure entity. For example when they rely on the services of others, and cannot control for acts of god/natural hazards outside human control. These sorts of minimum standards are also difficult because they do not speak to specific scenarios or context.

e. There is a high risk that introducing minimum standards would create barriers to entry and reduce competition in the telecommunications sector. Larger (existing) participants may be better able to implement the systems contemplated under the Australian approach. It would be a shame to lose these competition gains, and the incentives to invest in infrastructure resilience that competition brings. We can see tensions between wanting to keep prices low and competition high, and requirements to invest in non-economic elements that would drive up costs for consumers and operators, including new entrants.

[6] In the proactively released Cabinet paper on the Emergency Management Bill.

Powers for national security risks

43. The discussion document discusses last resort powers for national security risks, to enable government to act in a hurry. The suggestions are a directions power and intervention powers (as per the Australian approach), with safeguards such as good faith negotiations with critical infrastructure owners or operators.

44. We note that regulation already exists in the telecommunications sector to address security concerns. The Telecommunications (Interception Capability and Security) Act 2023 (TICSA) is designed to prevent, mitigate or remove security risks from the design, build and operation of public telecommunications networks. TICSA establishes obligations for New Zealand's telecommunications network operators. The Director-General of the GCSB has a regulatory role for network security under Part 3 of TICSA.

Information sharing and collection

Supportive of more effective information sharing

45. The discussion document canvasses a number of ideas about information sharing. As a sector we are very supportive of information sharing for resilience purposes, and welcome government doing more to facilitate effective information exchange.

46. There are also improvements that should be made concerning sharing of information between critical infrastructure operators. No agency currently undertakes this function. This would support more efficient coordination between critical infrastructure operators during emergency events, and during the build process. For example, if there had been better information sharing concerning plans for Transmission Gully, telecommunications could have been built into this major project and mobile black spots would have been avoided.

Start with a voluntary approach

47. We have not seen enough evidence of a problem with critical infrastructure refusing to share information, to justify moving directly to a legislative requirement. We haven't been asked to engage in an information sharing regime. We therefore recommend starting with a voluntary regime. This could include guidance on the information needed, development of a secure information sharing portal, and facilitating information exchange between sectors.

Information to one agency

48. We have concerns about the potential for regulatory confusion and excessive compliance costs if more than one agency has the role of requesting information, or if the information requested wasn't fit for purpose. As an example we refer to the

inefficient information sharing process during Cyclone Gabirelle, where the telecommunications sector was asked to provide information to various government agencies in different formats. Having a single information depository would have been much more efficient.

49. The recently introduced Emergency Management Bill already creates the potential for critical infrastructure to need to provide information to multiple agencies. As a sector, we also have comprehensive reporting obligations to the Commerce Commission. A number of organisations also need to report on resilience as part of their climate related disclosures to the Financial Markets Authority (FMA). It is important to ensure that information sharing is coordinated and the information requests from government agencies focus on the information that is actually required for resilience purposes to avoid adding undue administrative burden on critical infrastructure operators.

50. We recommend that:

    a. Any new information sharing requirements are to a single agency - multiple agencies should not be able to request information from a critical infrastructure entity - to ensure that reporting of information does not become burdensome and meaningless. This could be organised at the sector level, through the agency that already has regulatory responsibility for a sector, such as MBIE for telecommunications. Alternatively reporting could be to the new coordinating agency.

    b. The specified agency has appropriate confidentiality obligations. Any new information sharing platforms will also need to have adequate security.

    c. Government (perhaps through Te Waihanga) co-designs the information and reporting requirements with critical infrastructure sectors. Getting the design and the requirements right could help keep compliance costs within reasonable limits while still meeting the policy intent, and make it easier to understand and use the information.

    d. There are standard formats for providing information. This could be addressed as part of the co-design process mentioned in (c) above.

    e. Government facilitates information exchange and discussion between sectors (it's not just about industry reporting to government). As the owner of a number of critical infrastructure assets, the government could play a role in incentivising public sector operated entities to work with other critical infrastructure operators to agree a framework for more efficient information sharing.

f. Existing reporting requirements are brought together with new ones, with government providing critical infrastructure sectors with a single view on what information and reporting is required where and when.

g. There would need to be a sufficient transition time for critical infrastructure providers to be able to comply with any new reporting requirements.

51. Para 35 of the discussion document refers to government supporting the resilience of critical infrastructure by providing information from agencies such NIWA. We note that NIWA charging for climate change information is a barrier to the resilience of critical infrastructure. We suggest this be considered as part of the broader government package on infrastructure resilience.

Government responsibility and coordination

52. A central, coordinating agency for the critical infrastructure system is proposed. As a sector we have been frustrated by the fragmented government landscape for resilience issues, so support the proposal in principle. We suggest the following issues are considered in the design of a coordinating agency:

    a. There is just one agency with the proposed functions to coordinate and set policy and regulatory requirements for critical infrastructure. As noted in the section on potential minimum standards, regulatory confusion would result if both a central agency and sectoral regulators could set resilience requirements. Te Waihanga could potentially take on the coordination function.

    b. Clear lines need to be drawn on the responsibility of a new agency, NEMA and the agencies that currently have regulatory responsibilities for particular sectors (e.g. Commerce Commission regulating for competition in telecommunications). It would need to be very clear who we report or talk to about what, with no duplication or overlap. See above our points around reporting and providing information.

    c. The coordinating function of a new agency (or existing agency given the new functions) should not be limited to regulatory policy. It should also serve a practical purpose of bringing critical infrastructure sectors together to identify interdependencies and co-design practical solutions. At the moment there is no agency serving this function. Having an agency that undertakes this role could do more to identify and address interdependencies, and create a systems-approach, than the introduction of regulation could achieve.

    d. The new agency should be responsible for working with critical infrastructures to develop a resilience strategy that would set a vision and

signal resilience objectives and targets. We have provided examples above of strategies developed by the UK and Canadian governments.

53. We are also conscious that government would be both an owner operator of critical infrastructure (e.g. roads and power supply) and a regulator of resilience for critical infrastructure if new regulation was introduced. How would government resolve this potential conflict and ensure that there is genuine consistency of any minimum standards and enforcement across publicly and privately operated critical infrastructure assets?

The resource management system as a barrier to resilience

54. The discussion document asks if there are additional barriers to resilience of critical infrastructure. For the telecommunications sector (and other sectors such as electricity) the resource management regulatory system is a barrier.

55. The National Environmental Standards for Telecommunications Facilities (NESTF - secondary legislation under the Resource Management Act (RMA)) sets key standards for us in terms of where we can locate our infrastructure, and its size and height. These standards are critical to what we can do in building, maintaining, extending and strengthening our networks. Unfortunately the NESTF has not kept pace with changes in technology that support enhanced resilience, and changes in the built environment.

56. The Ministry for the Environment has informed us that it does not currently have time or resources to update NESTF under the RMA. This is despite TCF, Te Waihanga and MBIE offering to help resource the work. Updates to telecommunications standards are likely to be years away (7-9 years), post introduction of new resource management legislation and the proposed National Planning Framework. Without the NESTF updates, our members need to undertake time consuming and costly engagements with individual councils to seek resource consents and designations, make submissions on plans and seek plan changes. This either slows down infrastructure build or stops it in its tracks. It can also lead to differing resilience outcomes across regions.

57. A government decision to not update the NESTF under the resource management regulatory system will make it extremely difficult for the telecommunications sector to meet requirements under a potential new critical infrastructure regulatory system. We submit that the NESTF needs to be updated before the telecommunications industry can take on any new resilience obligations. Work on the NESTF updates could be done in time for new resilience regulation if government chooses to prioritise it.

Land access issues are also a barrier

58. Providing greater resilience in telecommunications networks through initiatives such as duplicate routes in and out of towns will require us to address land access issues. Network cables will usually follow a road, as an existing infrastructure corridor. Alternative routes may need to be across private land or conservation estate, which requires negotiation of land access agreements. If land owners are not keen then we cannot proceed.

59. We mention this as a potential barrier, and an issue that could make it difficult for the sector to comply with very specific resilience requirements if they were imposed. This is an example of why any resilience standards (if the government decides to pursue it) need to be principles based.

We are happy to discuss further

60. If you have any questions arising from this submission please contact kim.connolly-stone@tcf.org.nz in the first instance.