



BRIEFING

Telecommunications resilience

Date:	11 June 2021	Priority:	Medium
Security classification:		Tracking number:	2021-4004

Action sought		
	Action sought	Deadline
Hon Dr David Clark Minister for Digital Economy and Communications	Note officials will re-engage with network operators to work through the resilience implications of NEMA's proposed changes to the Civil Defence and Emergency Management Act, and to explore options to increase confidence in the resilience of telecommunication networks.	16 June 2021

Contact for telephone discussion (if required)			
Name	Position	Telephone	1st contact
Susan Hall	Manager, Communications Policy	04 896 5304	✓
Emma Wicks	Senior Policy Advisor	04 901 6184	
Christopher Moses	Policy Advisor	04 897 6386	

The following departments/agencies have been consulted
Commerce Commission

Minister's office to complete:

- | | |
|---|--|
| <input type="checkbox"/> Approved | <input type="checkbox"/> Declined |
| <input type="checkbox"/> Noted | <input type="checkbox"/> Needs change |
| <input type="checkbox"/> Seen | <input type="checkbox"/> Overtaken by Events |
| <input type="checkbox"/> See Minister's Notes | <input type="checkbox"/> Withdrawn |

Comments

Released under the Official Information Act 1982



BRIEFING

Telecommunications resilience

Date:	11 June 2021	Priority:	Medium
Security classification:		Tracking number:	2021-4004

Purpose

This briefing provides an introduction to telecommunications resilience, outlines the potential impact of natural disaster scenarios on telecommunications services, and suggests possible levers for Government to use to enhance resilience.

Recommended action

The Ministry of Business, Innovation and Employment recommends that you:

- a **Note** MBIE has engaged with the telecommunications industry since 2016 on network resilience and emergency response.

Noted

- b **Note** despite this engagement officials consider the Government currently lacks information needed to assess whether the resilience decisions of network operators are reasonable.

Noted

- c **Note** on 9 June 2021, the National Emergency Management Authority (NEMA) sent out a consultation document to government agencies and lifeline utilities (including telecommunications companies) regarding proposed changes to the Civil Defence and Emergency Management (CDEM) Act 2002, which include changes to the responsibilities of lifeline utilities before, during and after an emergency.

Noted

- d **Note** officials will re-engage with network operators on resilience to work through the implications of NEMA's proposed changes to the CDEM Act, and to explore options to increase confidence in the resilience of telecommunication networks.

Noted


Susan Hall
Manager, Communications Policy

Hon Dr David Clark
Minister for Digital Economy and
Communications

11 June 2021

..... / /

Background

1. New Zealand has world-leading telecommunications infrastructure, despite the challenges associated with our narrow and rugged geography. Our networks generally hold up well to natural disasters, and when service interruptions do happen they tend to be localised and short in duration due to the high level of responsiveness by network operators.
2. However, some natural disasters (such as the recent June 2021 floods in Canterbury) have highlighted potential vulnerabilities in the network. These events raise the question of whether more should be done to enhance network resilience.¹
3. Enhancing resilience must always be traded off against the benefits of other network investments, such as technological innovation (e.g. 5G) or expanded coverage (i.e. rural connectivity). Commercial drivers do not typically incentivise network operators to invest in resilience, so any significant changes are likely to require government intervention.
4. This briefing builds on previous advice provided in July and October 2019 to the former Minister of Broadcasting, Communications and Digital Media, which covered:
 - a. outcomes of the Telecommunications Resilience Natural Hazard Risk Assessment completed in 2018, which MBIE commissioned following the Kaikoura earthquake in 2016 [briefing 3853 18-19 refers]
 - b. legislative requirements around resilience to natural disasters [briefing 1346 19-20 refers].

Telecommunications network resilience

5. Telecommunications network infrastructure is made up of two key parts:
 - a. 'nodes' that control communications to and from the regions they service (i.e. central offices or telephone exchanges)
 - b. 'links' that connect nodes and transmit communications across the country (i.e. fibre, digital microwave radio or copper cables).
6. While both links and nodes are essential for a network function, damage to nodes can have more significant consequences for a network. Industry upgrades to service platform technology over the past decade mean that network-based services are delivered from fewer key nodes around the country.
7. Regional voice, mobile and broadband services will not work autonomously in a 'local mode' when key nodes are affected by natural hazards, or when links connecting the region to the centre of the network are affected. This means that an event affecting key nodes in main urban centres such as Wellington or Auckland has the potential to cause major service outages in regions otherwise unaffected by the event.
8. In addition, the resilience of telecommunications services is closely linked to the resilience of other lifeline utilities, such as electricity and transport. Damage to one utility often causes, or occurs simultaneously to, damage to another. For example, an extended power outage at a key node can cause widespread telecommunications outages, even though there is nothing physically wrong with the telecommunications network itself.

¹ This briefing addresses network resilience to natural disasters. While there are many other factors that can disrupt telecommunication services (e.g. faulty software updates, power outages, cyber-attacks, or human error), the controls needed to protect against natural disasters are distinct.

MBIE's work on resilience to date

The 2016 Kaikoura earthquake exposed network vulnerabilities

9. The 2016 earthquake in Kaikoura had significant impacts on local and national telecommunications, including:
 - a. widespread telecommunications outages in the region for several days
 - b. reduced redundancy by leaving only one functioning fibre cable connecting most of the South Island
 - c. loss of the national 111 service for 44 minutes.
10. While network operators responded quickly and effectively to resume services, this event highlighted how large parts of the country are often dependent on specific parts of the network for their services. For example, the disruption of the national 111 service was caused when a Spark call centre in Wellington, which at the time redirected all incoming 111 calls to the relevant emergency service, was evacuated due to earthquake damage and the contingency plan failed to automatically re-direct 111 calls to regional emergency services.
11. After the earthquake, several network operators took steps to add resilience to their networks, including:
 - a. increased route diversity of key links in the South Island to add redundancy to the network
 - b. installing generators at key nodes to ensure service continuity for up to 48 hours in the event of a power outage
 - c. after reviewing their 111 service, Spark established a new 111 call centre in Christchurch.

MBIE undertook a review into network resilience to identify risks posed by natural disasters

12. Following the Kaikoura earthquake, MBIE commenced a review of the resilience of New Zealand's nation-wide telecommunications system, including how it may be impacted by a range of natural hazard risks. The review focused on understanding the resilience of the telecommunications system as a whole (including issues that are not the responsibility of one company alone), and looked at the common risks that the country faces as a result of natural disasters.
13. As part of this review, MBIE commissioned consulting company WSP Opus (now WSP New Zealand) to undertake a risk assessment of our national telecommunications network. The final report, delivered in September 2018, provided a comprehensive overview of the risks posed by natural disasters for telecommunications. It recommended that MBIE further engage with the network operators to analyse the potential exposure of networks against the risks highlighted in the report [briefing 3853 18-19 refers].

Engagement with network operators on the 2018 report

14. s 9(2)(g)(i) [REDACTED]
The network operators tended to take the view that the impact of natural disasters on their networks is almost impossible to accurately predict, and where clear vulnerabilities exist, they have appropriate measures in place to mitigate risks.
15. However, the risk and impact tolerance of the network operators and government may not always align.

Recent events and scenario modelling have shown that vulnerabilities in the network remain

Rangitata River floods – December 2019

16. In December 2019, flooding of the Rangitata River in Canterbury left thousands of homes and businesses without phone or broadband services. The flooding damaged a fibre optic cable near a road bridge over the river on State Highway One (SH1). Several hours later, another fibre optic cable that crosses the river on SH72 was damaged about 16km south of Methven.
17. The combined disruption to Spark's network due to the outages were:
 - a. 111 calling in lower South Island would not proceed under all calling scenarios
 - b. 22 local nodes were isolated
 - c. 163 cell sites were isolated
 - d. approximately 73,500 broadband customers were left without service
18. Spark managed to partially restore the network by using undamaged fibres in the SH1 cable. However, it took two days for Spark to fully restore telecommunications by using spare fibre pairs on the Vodafone link that crossed the Rangitata River on an unaffected parallel bridge.

Canterbury floods – June 2021

19. The recent Canterbury floods have also highlighted vulnerabilities in the network. Similarly to the 2019 floods, network operators' key concerns were about the damage to fibre links across several bridges in the South Island.
20. The 2018 Opus report had highlighted the Canterbury plains as a particularly vulnerable part of the telecommunications network in the case of flooding, as key links running through the plains cross a number of the same river networks. It recommended that a bridge analysis should be undertaken, or verified by network operators, to identify vulnerable bridges on the network. We shared this finding with network operators at the time. Network operators took the view that transport infrastructure vulnerabilities are the responsibility of Government, and not private telecommunications providers who use transport routes for their network.

Wellington earthquake scenario modelling

21. In addition to the real events mentioned above, scientists at GNS Science and lifelines groups have modelled the potential impact of natural disasters on telecommunications networks.
22. In 2019, Wellington Lifelines Group released its report on how a 7.5 magnitude earthquake would impact the Wellington region and suggested a number of infrastructure investments that could enhance the resilience of lifeline utilities. The Group also acknowledged that the ability of some lifeline organisations to invest is restricted.
23. One of the suggested investments was for telecommunications providers to procure back-up power generators at each of the key cell sites in Wellington. In the event of an earthquake, these generators would provide approximately two weeks of power before requiring re-fuelling. The report estimated this project would cost \$11.65 million to implement and recommended that it be undertaken within the next seven years.
24. However, network operators had limited engagement with Wellington Lifelines Group in the preparation of the report and, when the report was released, they expressed doubt that the suggested investment would significantly increase network resilience. Some network operators offered to discuss this with the Minister responsible at the time.

Alpine Fault magnitude 8 earthquake (AF8) scenario modelling

25. The Alpine Fault is the active boundary between the Pacific and Australian tectonic plates. Experts expect that a large earthquake in the Southern Alps will lead to a “cascade” of hazards including aftershocks, landslides, tsunamis, floods, debris flows and more.
26. An AF8 scenario is likely to damage telecommunications equipment and networks across the South Island. Compounding this will be damage to electricity infrastructure, roads, and emergency response management facilities.
27. In preparation for the AF8 scenario, all South Island CDEM Groups have satellite voice and data communications capabilities, and some have high-frequency (HF) radio telecommunications available as alternative means of communication within their CDEM Groups and across the South Island.
28. Ultra-high frequency (UHF) and very-high frequency (VHF) voice telecommunications would be available for land, water and air telecommunications at a local level only. This is because most repeaters (which enable long-distance wireless communications) are vulnerable to quake damage and electricity interruption.

Government currently lacks information needed to assess whether the resilience decisions of network operators are reasonable

29. Due to continued natural disasters exposing vulnerabilities and ^{s 9(2)(g)(i)} [REDACTED], officials consider we do not have enough information to make an informed judgement on network operators’ resilience decisions.
30. Specifically, we lack information on:
 - a. the relative net benefit of resilience over a focus on emergency response
 - b. the costs and benefits of different resilience investments (either within the telecommunications network or between different lifeline utilities)
 - c. how network operators balance competing priorities (enhancing resilience must always be traded off against the benefits of other network investments, such as technological innovation).
31. However, in spite of these uncertainties the government has still made notable investments in telecommunications resilience. For example, the new regional fibre link being built in the West Coast and Otago, funded via the Provincial Growth Fund and announced in August 2020, will provide an alternative connection path in a region which is particularly prone to disruption in an Alpine Fault or similar seismic event.
32. Network operators themselves have also on occasion approached government with proposals that would enhance network resilience. ^{s 9(2)(b)(ii)} [REDACTED] This suggests that network operators have planned resilience initiatives that are feasible, but which they do not consider are commercially viable without government assistance.

Possible ways to enhance network resilience

33. Given the uncertainties and information shortages noted above, we consider there is scope for more work to be done on telecommunication resilience. At the very least, we consider it necessary to seek assurance from network operators that network vulnerabilities are being sufficiently managed. ^{s 9(2)(f)(iv)} [REDACTED]

34. If needed, we consider that there are three potential levers the government could use to enhance resilience that merit further analysis:

1) Use existing regulatory tools to increase transparency of network resilience

35. Obtaining better information from network operators would enable better targeting of policies to enhance resilience. The only piece of legislation that currently provides a clear mechanism to obtain relevant information from network operators is the Civil Defence and Emergency Management (CDEM) Act.
36. The CDEM Act contains two sections that enable the Director of Civil Defence and Emergency Management (the Director) to obtain information from lifeline utilities (which include telecommunications) relating to emergency management:
- a. Section 60 requires lifeline utilities to make available to the Director their plan for functioning during and after an emergency. This power can be exercised at any time.
 - b. Section 76 gives the Director power to require a lifeline utility to provide information that is reasonably necessary for the exercise of civil defence emergency management. To our knowledge, this power has not been exercised.

2) New regulatory powers that set clear resilience obligations on network operators

37. The National Emergency Management Authority (NEMA) is currently reviewing the Government's civil defence and emergency response. The intent of the review is to make improvements to emergency preparedness and response primarily by making responsibilities, both nationally and regionally, clearer. Amendments to the CDEM Act will be required to implement any resulting changes.
38. On 9 June 2021, NEMA sent out a consultation document to government agencies and lifeline utilities (including telecommunications companies) that sets out proposed amendments to the CDEM Act. These changes include setting clearer resilience standards and information-sharing obligations for lifeline utilities.
39. While MBIE has not yet submitted a response to NEMA on their specific proposals, we consider that the CDEM Act review is an appropriate avenue to make changes to the resilience obligations of network operators. We will engage with the network operators and NEMA in the coming weeks to work through the implications of NEMA's proposed changes to the CDEM Act, and to explore options to increase confidence in the resilience of telecommunication networks.
40. Another regulatory lever that could be used to create clear resilience obligations, which was raised at your meeting with officials on 31 May 2021, is to introduce Retail Service Quality (RSQ) codes for telecommunications resilience. The Telecommunications Act (2001) gives the Commerce Commission (the Commission) powers to improve RSQ, including customer service, faults, installation, contracts, product disclosure, billing, switching, service performance, speed and availability. Late last year, the Commission undertook a consultation on pain points faced by consumers to identify where retail quality standards could be improved.
41. MBIE officials spoke to the Commission to see if there was a potential to use the work on RSQ, and in particular RSQ codes, to develop resilience standards. The Commission's initial perspective is that resilience standards do not naturally fit with the ongoing work on RSQ codes. This is partly due to consumers' lack of feedback on this issue and the fact that resilience crosses both retail and wholesale services.
42. At this stage, MBIE does *not* view RSQ codes as an effective lever to enhance resilience, as it does not take into account the interdependencies between different lifeline utilities.

3) Additional funding for government-approved projects

43. Another mechanism is for Government to offer funding (i.e. grants) to network operators for resilience projects. This would ensure the decisions around which network vulnerabilities should be prioritised are in the hands of the network operators, who know their networks best. It would also remove the commercial barrier to making resilience decisions in the public interest.

Next steps

44. MBIE officials will engage with network operators in the coming weeks on the proposed changes to the CDEM Act, and discuss ways to enhance confidence in New Zealand's telecommunications resilience.
45. We understand you may wish to raise the issue of network resilience directly with network operators. To support these conversations, we have attached suggested talking points at **Annex One**.
46. Other than ongoing oversight and reactive response, there is no dedicated telecommunications resilience project currently on the communications policy work programme. Resilience will necessarily form a part of the future of connectivity programme of work, which we are currently scoping. Officials will be briefing you in Q3 this year on this work programme once scoping has been completed. Through that briefing process, we will be seeking your feedback on relative priorities and resource allocation within that work programme.

Annexes

Annex One: Suggested talking points

Annex One: Suggested talking points

These talking points are intended to support conversations with network operators, should you wish to reach out to them and discuss network resilience.

Talking points

s 9(2)(g)(i)



Released under the Official Information Act 1982



AIDE MEMOIRE

Telecommunications resilience: background information for your meeting with the Network Resilience Group

Date:	12 October 2021	Priority:	High
Security classification:		Tracking number:	2122-1332

Information for Minister(s)
Hon Dr David Clark Minister for the Digital Economy and Communications

Contact for telephone discussion (if required)			
Name	Position	Telephone	1st contact
Susan Hall	Manager, Communications Policy	04 896 5304	✓
Christopher Moses	Senior Policy Advisor, Communications Policy	04 897 6386	

The following departments/agencies have been consulted

Minister's office to complete:

Approved

Declined

Noted

Needs change

Seen

Overtaken by Events

See Minister's Notes

Withdrawn

Comments

Released under the Official Information Act 1982



AIDE MEMOIRE

Telecommunications resilience: background information for your meeting with Network Resilience Group

Date:	12 October 2021	Priority:	High
Security classification:		Tracking number:	2122-1332

Purpose

To provide background information about the resilience of telecommunications services in New Zealand and suggested talking points for your meeting with the Network Resilience Group, chaired by Dame Fran Wilde.

Susan Hall
Manager, Communications Policy
Building, Resources and Markets, MBIE

12 / 10 / 21

Background

1. Your office has requested background information on the current state of resilience of telecommunications in New Zealand, and suggested topics for discussion, before your meeting with the Network Resilience Group.
2. Officials understand the meeting will focus on the economics of building resilient networks to reduce the impact on telecommunications following a natural hazard event.

What do we mean by 'resilience'?

3. Ensuring resilient telecommunications services requires a combination of four areas of activity, known as the '4 Rs' of civil defence and emergency management:
 - a. **Reduction** – pre-emptively identifying, mitigating and / or eliminating risks
 - b. **Readiness** – developing operational systems and capabilities before a civil defence emergency happens
 - c. **Response** – actions and resources deployed in the immediate aftermath of an emergency
 - d. **Recovery** – coordinated efforts and processes to bring about the immediate, medium-term and long-term regeneration of a community (including the infrastructure it relies on) following a civil defence emergency.

4. It is impossible to completely eliminate natural hazard risks and there will always be a critical role for readiness, response and recovery. However, it is important for telecommunications companies to do all that they reasonably can to pre-emptively reduce risk in the way they build, maintain and operate their network infrastructure.

Current state of resilience in the telecommunications sector

5. As set out in previous advice [briefing 2021-4004 refers], New Zealand has world-leading telecommunications infrastructure, despite the challenges associated with our narrow and rugged geography. Our networks generally hold up well to natural disasters, and when service interruptions do happen they tend to be localised and short in duration due to the high level of responsiveness by network operators.
6. However, some recent events, such as the floods in Canterbury in June and the recent lightning strike on the West Coast, raise the question of whether more should be done to enhance network resilience.
7. It is important to note that the telecommunications sector has several attributes that distinguish it from most other lifeline utilities (transport, electricity, water etc), most notably that:
 - a. Multiple private companies, not the government, own and operate the network infrastructure
 - b. mobile network operators (MNOs), who provide mobile and fixed wireless broadband services, operate with little regulatory oversight of their service resilience unlike the copper and fibre based access providers. MNOs rely on market competition, commercial and reputational incentives to build resilient networks.
8. Government's role to date has typically been to ensure that there are sufficient incentives on private operators to take resilience decisions in the public interest. This has been done by:
 - a. working with operators to understand their approaches to networks resilience
 - b. implementing resilience requirements through contractual arrangements with private companies (e.g. current contracts with the local fibre companies (LFCs) and Chorus require that fibre access networks (UFB) cannot have a single point of failure likely to impact more than 4,000 connections)
 - c. funding resilience initiatives that would otherwise not be commercially viable for individual private telecommunications companies to provide (even though they may still receive significant indirect economic benefits)
 - d. limited regulation through the Civil Defence and Emergency Management (CDEM) Act, which requires all lifeline utilities (including network operators) to ensure that they are "able to function to the fullest possible extent, even though this may be at a reduced level, during and after an emergency".

How could network operators reduce the risk of disasters impacting telecommunications services?

9. In order to improve resilience by reducing the likely impact of a natural hazard event on telecommunications, network operators would need to build, maintain and operate:
 - a. more robust infrastructure (i.e. less likely to break), although it is impossible to protect against some significant natural hazard events
 - b. more redundant infrastructure (e.g. multiple and diverse connection routes or establishing back-up infrastructure, in case something in the network breaks).

10. Building robust infrastructure is a more manageable and easy-to-implement solution for telecommunications companies, as there are certain standards and quality controls they can follow to ensure their infrastructure meets an agreed threshold (i.e. it is easier to measure). For example, key telephone exchanges and data centres can be built to specific earthquake-resistant standards. However, even the most robust infrastructure is still susceptible in significant natural hazard events.
11. Building redundant and relocating at-risk infrastructure is a far more complex issue. This is because:
 - a. it is difficult (even impossible) to accurately predict where a natural hazard event will take place and what the impact will be, making it difficult to know where redundancies should be built into the system
 - b. network operators are generally not liable for indirect losses, and so are less likely to understand or factor the wider economic impacts into their assessments
 - c. it is extremely expensive to build and maintain new infrastructure that provides no additional service quality for end users (i.e. people pay for the service, not the resilience)
 - d. asset owners (service providers in many cases) are often not the ones to suffer the full economic cost of disruptions, so they are less incentivised to build adequate redundancies (particularly in more remote or sparsely populated regions).
12. Nevertheless, the diversity of network connections available has often been a determining factor in whether previous natural hazard events have caused service disruptions, whether these are redundancies or just alternative connections to reach the same end users. For example, during several flooding events in South Canterbury in recent years, network operators have been able to redirect network traffic from broken or damaged fibre links (caused by bridge washouts) onto other links to ensure service continuity.

What are the key challenges to improving network resilience?

13. The main challenges we are aware of to improving the resilience of telecommunications in New Zealand are:
 - a. The broad range of unpredictable threats and hazards with the potential to cause service disruptions, and increased frequency of these events due to climate change, makes it difficult to prioritise specific resilience initiatives. Private companies will tend to prioritise addressing immediate threats with more certain implications, rather than target risks with far less likelihood and predictability but which have the potential to be catastrophic, such as a major alpine fault earthquake.
 - b. Investing in resilient infrastructure is expensive and not typically commercially viable for private network operators. Resilient networks do not improve day-to-day service quality, and so customers are not usually willing to pay for it (i.e. resilience is only valuable when it's needed, and by then it may be too late).
 - c. There are no consistent or clear resilience standards that network operators – particularly the MNOs – are required to follow regarding the resilience of their networks and / or services. It is difficult to develop these standards in a way that is logical, fair and commercially viable for operators without considerable government funding.
 - d. Enhancing resilience must be traded off against the benefits of other network investments, such as technological innovation (e.g. 5G) or expanded coverage (i.e. rural connectivity). Commercial drivers do not typically incentivise network operators

to invest in resilience, so any significant changes are likely to require government intervention.

- e. There are *growing interdependencies* within and across critical infrastructure sectors, which makes coordination across sectors increasingly important when planning how to improve resilience. Improving the resilience of one sector in isolation from the others will result in fewer benefits as this trend continues (i.e. building more redundant telecommunications infrastructure will not help if the power goes out).

14. s 9(2)(g)(i)

Despite the challenges, there are work programmes underway that will improve telecommunications resilience

15. The main programmes of work currently underway that will have resilience benefits include:
- a. various rural connectivity upgrades commissioned by Crown Infrastructure Partners (CIP) have resilience benefits, such as the new fibre cable from Fox Glacier via Haast to Lake Hawea (however, this still ultimately depends on network operators deciding to maximise use of the available connection as there may be few service quality improvements in doing so in some cases)
 - b. the National Emergency Management Agency's (NEMA's) ongoing review of the CDEM Act, s 9(2)(f)(iv)
16. Furthermore, telecommunications network and service resilience is identified as one of the six main connectivity challenge areas under the proposed Future of Connectivity work programme [briefing 2122-0939 refers].
17. Under the proposed Future of Connectivity work programme, s 9(2)(f)(iv)
- The theme of network and service resilience is also seen as being a key part of a future New Zealand telecommunications connectivity strategy.

Annexes

Annex One: Suggested questions for discussion at your meeting with the Network Resilience Group

Annex One: Suggested questions for discussion at your meeting with the Network Resilience Group

s 9(2)(g)(i)



Released under the Official Information Act 1982



BRIEFING

Telecommunications resilience: advancing your objectives through broader critical infrastructure reforms

Date:	21 June 2022	Priority:	High
Security classification:	Restricted	Tracking number:	2122-4378

Action sought		
	Action sought	Deadline
Hon Dr David Clark Minister for the Digital Economy and Communications	<ul style="list-style-type: none"> Note the talking points at Annex One for the ERS meeting on 28 June 2022, where Ministers will discuss the sequencing and prioritisation of the various ongoing critical infrastructure reforms. Agree that MBIE will report back to you by 27 July 2022 with a plan for advancing telecommunications resilience objectives across the broader critical infrastructure reforms, and how this will align with the Future of Connectivity work programme. 	28 June 2022

Contact for telephone discussion (if required)				
Name	Position	Telephone		1st contact
Deborah Salter	Manager, Communications Policy	04 901 0786		
Christopher Moses	Senior Policy Advisor, Communications Policy	04 897 6386		✓
Jack Weston	Graduate Advisor, Communications Policy	04 896 5654		

The following departments/agencies have been consulted

Minister's office to complete:

Approved

Declined

Noted

Needs change

Seen

Overtaken by Events

See Minister's Notes

Withdrawn

Comments



BRIEFING

Telecommunications resilience: advancing your objectives through broader critical infrastructure reforms

Date:	21 June 2022	Priority:	High
Security classification:	Restricted	Tracking number:	2122-4378

Purpose

This briefing:

- summarises responses from the telecommunications sector to your letter requesting information about network and service resilience
- outlines how the broader critical infrastructure reforms being progressed across government provide the best opportunity to advance your telecommunications resilience objectives
- provides you with suggested talking points for the Cabinet External Relations and Security Committee (ERS) meeting on 28 June 2022, where the sequencing and prioritisation of ongoing critical infrastructure reforms will be discussed.


Executive summary

The Telecommunications Forum (TCF), on behalf of its members, has responded to your letter requesting information about telecommunications network and service resilience, which you sent to national network operators and the TCF in November 2021. Vodafone and Chorus also responded individually.

The TCF report provides a good general overview of how the sector approaches the issue of resilience. However, it does not provide enough detail to determine what the greatest risks are to network resilience, nor whether government intervention may be necessary to lift sector resilience to a more appropriate standard. While Vodafone and Chorus provided more specific details in their responses, follow-up conversations would still be needed to identify the most significant risks and vulnerabilities (and hence identify priority initiatives).

Critical infrastructure reforms

The challenges of enhancing resilience are not unique to the telecommunications sector, and there are already significant programmes of work approved by Cabinet that aim to address – in whole or in part – the resilience of all critical infrastructure in New Zealand:

- Critical National Infrastructure (CNI) resilience – The Department of the Prime Minister and Cabinet (DPMC), overseen by the Minister for National Security and Intelligence, has been directed to explore options to enhance the resilience of critical national infrastructure in New Zealand [ERS-21-MIN-0042 refers]
- s 9(2)(f)(iv)

- Emergency management – The Minister for Emergency Management is overseeing a comprehensive review of the Civil Defence and Emergency Management (CDEM) Act,

and Cabinet has already approved several legislative changes focused on critical infrastructure resilience [GOV-21-MIN-0043 refers], with a final tranche of proposed changes to be considered in the coming weeks.

The Ministry of Business, Innovation and Employment (**MBIE**) is actively engaged in these existing work programmes, which have the potential to advance telecommunications resilience objectives while ensuring a consistent regulatory approach to resilience across all critical infrastructure sectors. ^{s 9(2)(g)(i)}

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

This is not to say the broader reforms will be without their own challenges. ^{s 9(2)(g)(i)}

[Redacted]

Meeting of the Cabinet External Relations and Security Committee (ERS) on 28 June

Given the intersections between the critical infrastructure reforms, the Minister for National Security and Intelligence (**NSI**) has agreed to discuss their sequencing and prioritisation with relevant Ministers at ERS on 28 June 2022 [DPMC-2021/22-1583 refers].

We understand the Minister for NSI's preference is to finalise the emergency management reforms quickly, before embarking on the holistic CNI regulatory changes (as opposed to combining the reforms in a single package). ^{s 9(2)(g)(i)}

[Redacted]

- [Redacted]
- [Redacted]

[Redacted]

- highlight the challenges you and previous Ministers have faced obtaining actionable information from the telecommunications sector to better understand risks and develop initiatives to enhance resilience

- ^{s 9(2)(g)(i)} [Redacted]

Once Ministers have agreed a way forward for the critical infrastructure reforms (post-ERS on 28 June), s 9(2)(g)(i), officials will develop a plan for how to advance telecommunications resilience objectives through the critical infrastructure reforms and provide this to you by 27 July 2022.

Recommended action

The Ministry of Business, Innovation and Employment recommends that you:

a **Note** the talking points attached at **Annex One** for ERS on 28 June 2022, where Ministers will discuss the sequencing and prioritisation of the critical infrastructure reforms underway across government.

Noted

b **Agree** that, following the ERS meeting, MBIE report back to you with a plan for advancing telecommunications resilience objectives through the broader critical infrastructure reforms, and how this will align with the Future of Connectivity work programme, by 27 July 2022.

Agree / Disagree



Deborah Salter
Manager, Communications Policy
Building, Resources and Markets, MBIE

21 June 2022

Hon Dr David Clark
Minister for the Digital Economy and Communications

..... / /

Released under the Official Information Act 1982

Background

1. On 11 November 2021, you sent a letter to national telecommunications network operators and the telecommunications forum (TCF) to ask for information about the resilience of their networks and services. The aim of this letter was to obtain specific information about different resilience risks and how companies assess these risks when investing in their network and service infrastructure.
2. On 24 May 2022, the TCF responded to your letter on behalf of all its member organisations, which include Chorus and the local fibre companies (LFCs), the mobile network operators (MNOs), internet service providers (ISPs) and regional wireless internet service providers (WISPs). Vodafone and Chorus had also previously submitted individual responses.
3. At your meeting with officials on 1 June 2022, you expressed concern about the lack of detailed information in the TCF report. Officials advised you that, in our view, the best opportunity to advance this work is to engage in the broader critical infrastructure reforms underway across government. In response, you asked for more information about how these broader reforms could help to deliver resilience objectives for the telecommunications sector.
4. This briefing provides our advice on these topics and talking points for you to take to ERS on 28 June 2022 (attached at **Annex One**), where Ministers will discuss sequencing and prioritisation of the Government's ongoing critical infrastructure reforms.

Industry responses to your resilience letter

Overview of the responses

5. Overall, the three responses to your letter provide a good general overview about the sector's approach to resilience, but often fall short on the level detail you requested (in particular the TCF report).
6. In line with previous discussions on resilience, the sector responses emphasise the effectiveness of emergency preparedness and response (i.e. dealing with emergency situations by working collaboratively and having resources readily available to deploy at short notice *after* an event occurs).
7. While the sector highlights some areas where further investment and improvements in pre-emptive mitigations could enhance resilience, little detail was provided about the relative priority or urgency of specific risks and vulnerabilities. In addition, where pre-emptive interventions are suggested, the sector tends to fall short of stating how these might be practically implemented.
8. We have identified several areas where more detail would be useful, particularly in forming a policy position on the relative merits of different resilience interventions. Once we have clarity on next steps for the critical infrastructure reforms currently being progressed across government (more advice on this in the sections below), we will be in a position to advise if / when it would be appropriate to hold targeted conversations with individual operators on these topics.
9. We have attached each response to your letter at **Annex Two** (TCF), **Annex Three** (Chorus) and **Annex Four** (Vodafone).

Response from the New Zealand Telecommunications Forum (TCF)

High level summary

10. The TCF report provides an overview of the general approach to resilience issues in the telecommunications sector, including:

- a. the TCF's view on how resilience is currently achieved through industry investment, government interventions (ie funding non-commercial projects), competition between companies and collaboration after an emergency event
 - b. trade-offs that are made between resilience and other customer needs
 - c. how a range of external shocks tend to impact networks and services, and how the sector responds when this happens
 - d. potential areas for improvement
 - e. detailed background information about case studies, network architecture and the Telecommunications Emergency Forum (TEF) that assembles to coordinate the sector's response in emergency scenarios.
11. The report tends to avoid getting into specific details about investment in resilient infrastructure or where the burden of responsibility should lie within the sector for delivering resilient services to consumers. ^{s 9(2)(g)(i)}
12. For example, the TCF states that industry investment in resilience "needs to be balanced with the acceptable level of risk the industry is willing to take", but no further information about what this level of acceptable risk is, or what the greatest risks are that the sector does not invest in mitigating due to commercial factors.
13. Key themes consistently presented in the report include:
- a. Networks are designed and built with resilience in mind (ie it is a core part of the business), but this can only go so far – either because consumers are not willing to pay for greater resilience or because of the unpredictability of events, particularly natural disasters.
 - b. The sector has shown excellent responsiveness and collaboration in previous events, but there are still areas the TCF knows could improve (e.g. better planning for how to respond in advance of emergency events, priority access to telecommunications sites during emergencies, better engagement and information-sharing with local and regional lifeline utility groups and government).
 - c. Market trends have led to more centralised service delivery models (i.e. telecommunications services are increasingly controlled from a few central locations, even though they are delivered to end users across the broader network). This provides more choice and flexibility for consumers but can result in new risks and greater impacts when outages do occur.
 - d. Telecommunications services to end users rely on complex interdependencies between network operators, service providers and other critical inputs (e.g. electricity), not all of which can be controlled by the primary service provider. For example, Chorus is responsible for much of the physical infrastructure over which services are delivered, but do not themselves provide internet services to end users (i.e. Chorus' network is necessary but not sufficient for service continuity).¹

¹ This means that where a fault occurs in the Chorus or LFC access network, there may be service impacts for ISP customers, but the ISPs are not responsible for fixing the underlying issue. Equally, where an ISP has a service platform issue, the local or national impact will only be felt by its customers and the physical network infrastructure will still be operating normally.

Potential follow-up topics for discussion

14. Based on the information provided, we have identified several key areas where targeted follow-up conversations with individual operators could provide useful information to feed into the broader critical infrastructure reforms, including:
 - a. Collaboration pre-emergency – It would be useful to understand exactly how operators work together after an emergency, and whether there is room for more collaboration pre-emergency (e.g. do operators share information with each other about known risks and vulnerabilities?).
 - b. How would better information improve resilience outcomes? The TCF report frequently mentions it would be useful to improve information-sharing and access to coordinated, targeted research about resilience risks, so we would be interested to know how this could be practically done in a way that would drive better outcomes. It would also be good to understand how the sector uses information that is already available (e.g. do operators use this information only when building new infrastructure, or do they reassess existing infrastructure based on new research about risks, such as climate change, flooding, earthquake risk etc).
 - c. Cost of living – We would be interested to understand how expensive resilient services currently on offer are for those who pay for them, and how a more resilient service offering to all consumers would impact pricing.
 - d. Understanding service delivery risks – The TCF report notes the interconnected nature of networks and the complexity of services delivered over the networks, and suggests that it would be useful to study how different network outages would impact services to end users in different regions. We would be interested to discuss how this study should be done (e.g. is this something the TCF could lead) and learn how it would practically improve resilience outcomes.

Response from Chorus

15. Chorus provided a detailed response to your letter, directly addressing many of the questions you raised. This includes a risk assessment table breaking down failure scenarios that result from known risks, including their likelihood, impact and overall risk rating.
16. Key points that Chorus highlights throughout its response include:
 - a. Chorus has unique risk and resilience considerations to work through because, unlike the ISPs and MNOs, it is a wholesale operator subject to utility-style regulation under the Telecommunications Act. Furthermore, Chorus' network architecture agreed with the Crown is designed to limit the impact of any particular network failure (e.g. under the original UFB contract, Chorus and LFCs could not build access networks with a single point of failure that would impact more than 3,000 end users).
 - b. Proposals to increase network resilience may require government funding, as was the case with the new West Coast fibre link completed earlier this year.
 - c. While Chorus may build network infrastructure that provides multiple physical links between the same locations (i.e. physical redundancies) – and is required to do so in many cases – there is no requirement for ISPs to use redundant links when delivering services to end users. That is, just because there may be diverse fibre links available to a particular community, in some cases it may not be commercially viable for ISPs to pay for access to them (this may be because it would raise the cost of services to the community to a level where consumers are not willing or able to pay).
17. Particular topics that we could look to explore further with Chorus include:

- a. how Chorus ensures the ongoing maintenance of network resilience based on new information, in particular regarding long-return period risks (e.g. climate change, increased flooding, earthquakes etc)
- b. how improved information-sharing and collaboration with other operators and Government could mitigate known risks before an emergency (e.g. whether Chorus would share relevant findings from the climate change assessment it commissioned in 2019 with other operators)
- c. whether Chorus will maintain redundant network infrastructure that ISPs and MNOs do not use.

Response from Vodafone New Zealand

18. On 1 February 2022, Vodafone responded to your letter with concise answers to each of your specific questions. Although the response does not provide much detail, it is a useful summary of how the different risks you raised impact Vodafone's network and services, and how it addresses each risk.
19. Some of the key points in Vodafone's response where further conversations would be useful include:
 - a. Investment opportunities – Vodafone states that there are potential network 'choke points' in specific locations around the country, such as the Bombay Hills south of Auckland, which could benefit from further network investment. Individual operators are unlikely do this without government funding due to the relatively low level of risk in these areas compared to other network risks. It would be worth asking Vodafone what initiatives would have the greatest impact and how operators would use the infrastructure if it were built.
 - b. Competition rules – Vodafone states it would be helpful for competition rules to explicitly recognise the limits of network-based competition in certain (rural) areas of New Zealand (i.e. how collaborative investment models such as the Rural Connectivity Group enable deployment of rural infrastructure). In addition, Vodafone asserts that competition rules result in network operators making independent decisions as to the placement and configuration of assets without any discussion or agreement (regardless of whether this is actually legally required). It would be good to clarify with Vodafone exactly how competition rules limit what can be shared by operators and whether there are still useful conversations that could be had without breaching these rules.

Alignment with broader critical infrastructure reforms

20. There are currently several significant programmes of work underway across government that seek to address – in whole or in part – the resilience of critical infrastructure in New Zealand including telecommunications. Three critical infrastructure reforms in particular are of direct relevance to the telecommunications sector, which we have set out below.
21. While MBIE views these work programmes as the best avenue to advance telecommunications resilience objectives, ^{s 9(2)(g)(i)}

Enhancing the resilience of critical national infrastructure (DPMC) [RESTRICTED]

22. On 16 November 2021, Cabinet directed DPMC, working with MBIE and other relevant agencies, to report back to ERS with "options for changing the regulatory structures and responsibilities for critical national infrastructure (CNI) resilience and security in order to take a more dynamic, coordinated and planned approach to strengthening CNI against all hazards and risks".

23. DPMC has conducted a significant amount of scoping work on what a comprehensive, fit-for-purpose regulatory system would look like for critical infrastructure in New Zealand (similar to the reforms recently passed in Australia). This also aligns with the recommendation in Te Waihangā's recently published Infrastructure Strategy to move away from a sector-by-sector approach to infrastructure regulation in New Zealand.
24. DPMC has advised Ministers [DPMC-2021/22-1583] that the reform package would likely require a combination of:
- a. an **agency/agencies with clear policy and regulatory responsibility** for the critical infrastructure system, to create greater accountabilities for system resilience
 - b. a **principles-based definition of critical infrastructures**, to ensure the perimeter can be readily expanded to capture emerging categories
 - c. **new platforms for information collection and sharing** between critical infrastructures and government, to create a shared understanding of risks and vulnerabilities and identify investment priorities
 - d. **enforceable minimum standards**, to reduce vulnerabilities associated with one asset owner underinvesting in their own resilience (focusing on lifting performance in sectors that have underinvested, rather than new requirements across all sectors)
 - e. **backstop intervention powers** to manage significant national security risks.
25. Cabinet has not yet considered whether to proceed with these reforms and there would still need to be a lot more policy work, sector engagement and legislative process before the reforms could be implemented. Given the time it would take to progress this work, DPMC's indicative timeline aims to have the new regulatory system enacted ^{s 9(2)(f)(iv)} [REDACTED] (subject to Cabinet approval and resourcing).

s 9(2)(f)(iv)

26.

27.

Emergency management reforms (NEMA)

28. The Minister for Emergency Management is overseeing a comprehensive review of the Civil Defence and Emergency Management (CDEM) Act. Cabinet has already approved several legislative changes focused on critical infrastructure resilience [GOV-21-MIN-0043 refers], with a final tranche of proposed changes to be considered in the coming weeks.

29. Key proposals relevant to the telecommunications sector include:

a. introducing obligations for sector-specific response plans

b. s 9(2)(f)(iv)

c.

d.

30. s 9(2)(f)(iv)

31. We understand the former Minister for Emergency Management (Hon Kiritapu Allan) intended for the Emergency Management Bill to be introduced to the House later this year, with the new Act to be implemented by July 2023 (subject to further Cabinet approval).

Leveraging broader critical infrastructure reforms is the best opportunity to advance your resilience objectives...

32. There are significant benefits to leveraging the broader reforms to advance telecommunications resilience objectives, in particular that it would:

a. ensure any requirements on telecommunications operators are consistent with those placed on other sectors

b. use limited government resources more efficiently (ie reduce the number of similar or overlapping work programmes, and ensure existing priorities do not need to be deferred)

c. simplify engagement with critical infrastructure entities, particularly given the range of reforms already underway that they have been (and will be) engaged on

d. likely be implemented in a timely manner, given these work programmes have already been agreed to by Cabinet and will require regulatory changes to be implemented (though the CNI resilience reforms are still only at a 'scoping' stage).

33. Based on our current understanding of the reforms, they have the potential to advance telecommunications resilience objectives as follows (noting that these are all proposed legislative changes that have not been confirmed and are at various stages of policy development):

Enhancing critical national infrastructure resilience (DPMC) [RESTRICTED]

- New information-gathering powers for the detailed and commercially sensitive information required to understand resilience risks in the sector, which in turn could help to establish practical and enforceable minimum resilience standards

- Improved government and sector understanding of the CNI system interdependencies
- Improved information-sharing on threats and vulnerabilities between critical infrastructure entities and government.

s 9(2)(f)(iv)

Emergency management (NEMA)

- A new sector emergency response plan could improve access to timely information after an event, sector coordination and preparation for optimising surviving network capacity, and access to sites for telecommunications technicians after an event.

34. This is not to say the broader reforms will be without their own challenges. s 9(2)(g)(i)

[Redacted text block]

35.

[Redacted text block]

36. We would not recommend pursuing standalone telecommunications resilience regulatory reforms at this stage, as it would risk duplicating work that is already underway and detract from MBIE’s ability to meaningfully contribute to the broader reforms.

...while still incorporating resilience as a key objective in your Government Statement of Intent

37. While the regulatory reforms noted above could all contribute to raising the resilience ‘floor’ in the telecommunications sector, s 9(2)(f)(iv)

[Redacted text block]

38. As part of your Future of Connectivity work programme, MBIE continues to develop the Government Statement of Intent (GSI) [2122-3332 refers]. You recently agreed to a series of objectives for the GSI, including that “by 2032 New Zealand has a telecommunications network that is able to respond to the nation’s unique resiliency challenges”.

39. For the GSI, it will be important to consider how resilience benefits are traded off against other connectivity objectives, such as coverage or capacity. In addition, ^{s 9(2)(f)(iv)} [REDACTED]

Meeting of the Cabinet External Relations and Security Committee on 28 June 2022

40. The Minister for National Security and Intelligence (NSI) has agreed to lead an oral item at ERS on 28 June 2022 to discuss the intersections between the critical infrastructure reforms noted in this briefing. The Minister for NSI has been advised on the following three options for how to progress the reforms:

- a. Option 1 – finalise the emergency management reforms quickly, before embarking on the holistic CNI regulatory changes (DPMC and NEMA preference)
- b. Option 2 – combine the critical infrastructure components of all three reforms into a single reform package (^{s 9(2)(g)(i)} [REDACTED])
- c. Option 3 – abandon the full CNI resilience regulatory reform work, and instead supplement emergency management and cyber resilience reforms with new tools to enhance our understanding of vulnerabilities (e.g. new information-gathering powers and information-sharing platforms).

41. We understand the Minister for NSI's preference is Option 1 (progressing the reforms sequentially). ^{s 9(2)(g)(i)} [REDACTED]

42. [REDACTED]

43. [REDACTED]

- b. highlight the challenges you and previous Ministers have faced obtaining actionable information from the telecommunications sector to better understand risks and develop initiatives to enhance resilience

c. s 9(2)(g)(i)

[Redacted]

44. We have attached talking points for you to take to ERS at **Annex One**.

Next steps

45. Once Ministers have agreed a way forward for the critical infrastructure reforms (post-ERS on 28 June), s 9(2)(g)(i), officials will develop a plan for how to advance telecommunications resilience objectives through the reforms and provide this to you by 27 July 2022.

Annexes

Annex One: Talking points for ERS on 28 June 2022

Annex Two: Response from the Telecommunications Forum

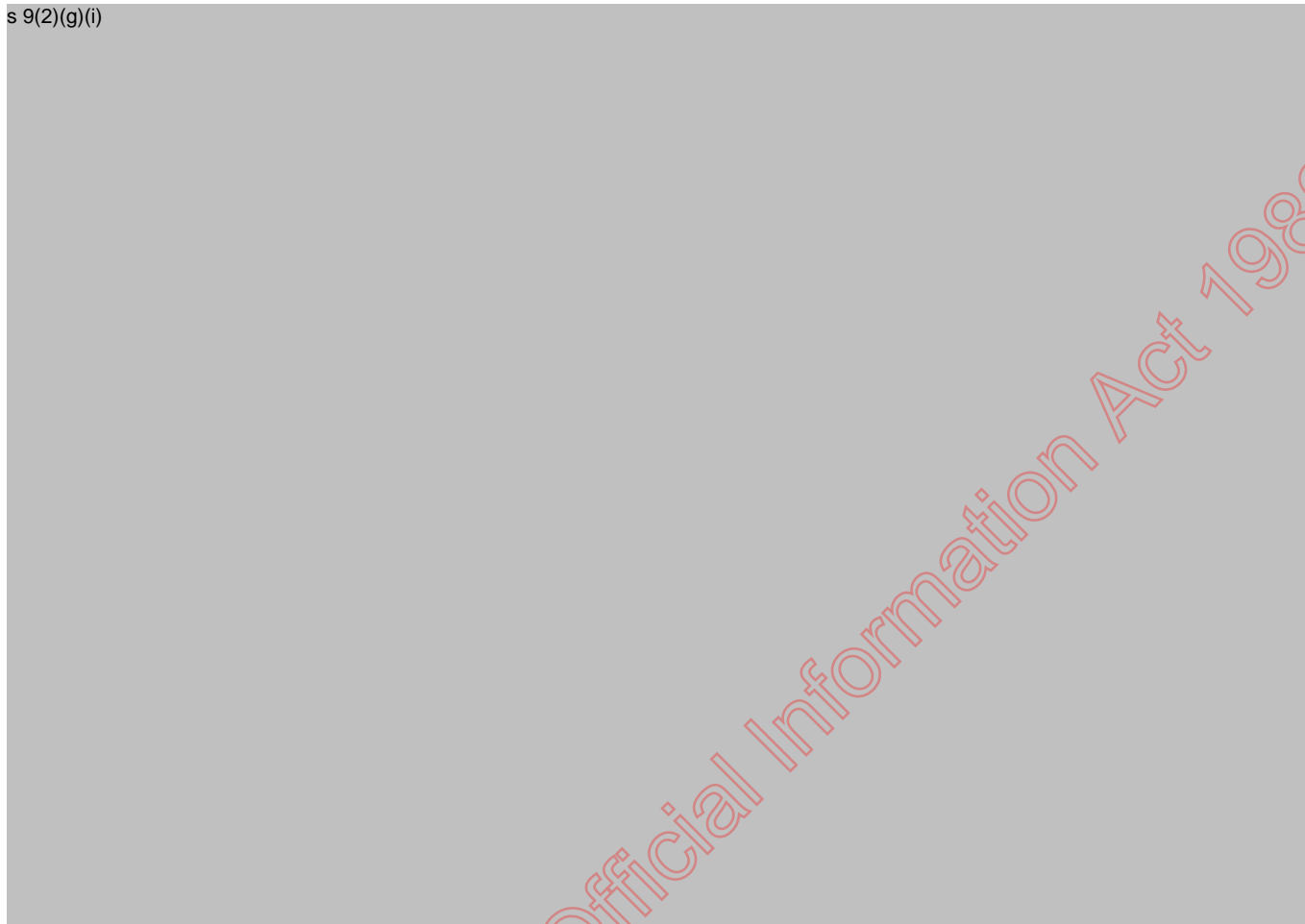
Annex Three: Response from Chorus

Annex Four: Response from Vodafone

Released under the Official Information Act 1982

Annex One: Talking points for ERS on 28 June 2022

s 9(2)(g)(i)



Released under the Official Information Act 1982

Annex Two: Response from the Telecommunications Forum

Released under the Official Information Act 1982

24 May 2022

Hon Dr. David Clark
Minister for the Digital Economy and Communications
Wellington

By email:



Dear Minister

The New Zealand Telecommunications Forum (TCF) has considered your request to provide information on the resiliency of the telecommunications sector in New Zealand, set out in your letter, 11 November 2021. We want to ensure that the government has the information it requires from the sector, and be assured that telecommunications infrastructure is resilient and network operators are able to respond effectively to emergency events.

1. Current State

The TCF has commissioned a 'current state' review of the telecommunications sector with the goal that this will inform the Minister and other officials regarding the resilience of New Zealand's telecommunication services. The report is attached to this letter.

Further discussion may be required with officials at the Ministry for Business Innovation and Employment (MBIE) to agree a pathway for further work to close out any information gaps identified. It is also essential to fold our programme into the wider policy framework being developed through the Minister's Future of Connectivity initiative.

1.1. Resilient networks are our core business

Ensuring our industry operates in a way that is resilient and enables the swift restoration of services following incidents and emergency events is a core part of TCF members' businesses. Telecommunications network operators have strong commercial and regulatory incentives to provide high-quality, resilient networks and services that meet growing consumer expectations about the essential nature of their communications services.

We are conscious that consumers rely on us more today than ever before, and ensuring our network is resilient in the face of rapidly increasing data usage and unexpected events – such as extreme weather events and Covid-19 lockdowns – is crucial to delivering our products and services and keeping New Zealand connected.

In 2018, the Government asked WSP Opus to review industry resiliencies, and they concluded that resiliencies in the telecommunications industry are generally good without extensive vulnerabilities to natural hazard events¹. The attached report provides further detail on how network operators prepare for and collaborate after natural emergency events, as well as other events, to ensure resiliency.

¹ WSP OPUS Telecommunications Resilience Review, Natural Hazards Risk Assessment October 2018

New Zealand Telecommunications Forum Incorporated (TCF)

PO Box 65503, North Shore, Auckland

Tel: + 64 9 475 0203 Fax: + 64 9 479 4530

Email: info@tcf.org.nz Web: www.tcf.org.nz

1.2. Risk assessment and vulnerabilities

Risks, vulnerabilities and system constraints must still be continuously assessed as part of any organisation's ongoing business continuity plans and resiliency planning.

The TCF has identified that damage to cabling and core services nodes due to an emergency event like a natural disaster is a serious risk and can cause long-term service outage to a particular region. Similarly, supply chain disruption can also have an adverse impact on restoration of networks during an emergency event but also during a pandemic, such as that we are currently experiencing.

We can provide assurance that the telecommunications networks are designed and built to be resilient with a "self-healing" transport network and redundant core nodes to reduce significant risk to the network itself. However, planning for these types of risks is ongoing, and the TCF is working with NEMA to develop a sector view through the TCF's Telecommunications Emergency Forum.

1.3. Assess and Monitor

It is not the role of the TCF to actively monitor telecommunications networks. Each network company has their own compliance obligations and regulatory requirements to complete risk assessments and ensure resilience and business continuity plans are in place to minimise any vulnerabilities.

Network operators' platforms and networks are monitored by their individual network operation centres, which hold major incident management processes that also feed into the Telecommunications Emergency Forum as appropriate. Whilst we cannot accurately predict how and when natural disasters will affect the network, the most important thing is to ensure the sector retains the ability to respond quickly when natural disasters do strike, or can collaborate on a response through the TCF.

The TCF is able to quickly bring together the industry and ensure there is appropriate alignment of resilience and business continuity planning so that the sector is able to respond appropriately during a natural hazard event and also during other scenarios such as a pandemic or the recent flubot attack.

1.4. Collaboration is essential

The industry has a demonstrable track record of providing resilient infrastructure and working together in response to natural disasters, emergencies and other significant events.

Telecommunications networks performed well during emergencies such as the Christchurch and Kaikoura earthquakes and systems proved to be resilient when called upon during the Covid-19 pandemic, allowing businesses and communities to do their best in difficult circumstances.

The TCF continues to develop the TEF, working with industry and engaging with other key stakeholders to ensure this forum best supports government, the sector and consumers.

1.5. Responding to new technology and resiliency demands

The TCF is confident that telecommunications network operators are responding to new technology and resiliency demands that are occurring across the market. For example, providers continue to invest in diverse core network elements and data centres and extending self-healing transport networks to additional regions.

1.6. Cyber-attacks and Cybercrime

The TCF supports the industry by acting as a conduit to other agencies when dealing with cyberattacks and cybercrime and sits on a number of inter-agency groups looking at cross-sector responses.

TCF members have well planned resilience programmes for mitigating cyberattacks, which we recognise are becoming an increasing risk to the security of companies, communities and individuals. The specifics of these programmes are better explained bilaterally between the Minister's office and the individual organisations.

2. What are our areas of focus over the next period?

While our Report indicates the current state of the sector is in good shape, there is always room for improvement and we have identified some specific actions that we aim to progress in partnership with our key stakeholders.

2.1. Industry emergency response planning

To date, the telecommunications industry has a proven track record of working together providing a robust collaborative response to restore services as soon as possible following unexpected events. The challenge is in pre-emptively mitigating potential scenarios and it is in this space that we believe efforts to improve resiliency could achieve the greatest impact for consumers.

In our response to NEMA's consultation on the changes to the civil defence legislation we have indicated a willingness to engage in sector planning via the TEF to ensure our response as an industry is optimised and as effective as possible. We propose to get ahead of the game and, working with your officials, develop an industry emergency response plan and codify our TEF processes.

We also propose direct engagement and input into Emergency Management Agencies on a national and regional level to improve our sector's preparedness to support communities directly. This would include consideration of:

- Provisioning of dormant network handovers reserved for emergency use (as part of an industry BCP arrangement)
- Priority access to telecommunications sites during emergencies is essential. This will require not just Waka Kotahi and the Ministry of Transport prioritising land transport access, but also assistance in accessing helicopters for situation assessment and transportation of Cell-sites on Wheels (CoWs), where land transport options are limited;
- A nation-wide fuel plan that includes priority supply to telecommunications providers. There are fuel plans across different Emergency Management Agencies across the country, but not all, and they are not uniform.
- Provision of risk assessment reports (natural hazards, climate change impacts, etc.) across the country. Currently, this information is being provided only where regional or local Lifeline Utilities Groups are conducting projects, for which funding is not necessarily provided by Government but by some of our members.

- Agreed plan and process for what sites and services to be restored to support communities across regions. This will support our approach of working together to get telecommunications services up and running as soon as possible after emergency events.

2.2. Supporting investment in resilient regional networks

We are seeing significant investment in new resilient infrastructure in response to customer demand.

However, New Zealand's geography and population density across parts of the country creates resiliency challenges, and in some cases addressing these may not be possible for network operators to fund on their own.

While providers face strong commercial drivers to provide resilient services, there are inevitably gaps where providing additional resiliency has very high costs, and in some cases, where few consumers benefit, making the commercial business case difficult. In these cases, investment in resilience needs to be balanced with the acceptable level of risk the industry is willing to take. This is determined, among other factors, by the existing level of resilience and the likelihood and impact of an event occurring that would present a significant risk to resilience in those areas.

It is commercially challenging to add further resiliency to transport regions due to, for example, low end user numbers or incremental nature of resiliency benefits of the investment. If there is a desire for additional investment in those areas, the Government should consider targeted investment to support resiliency improvements.

We propose to work with officials, as part of MBIE's Future of Connectivity project, on a robust assessment of regional connectivity to identify opportunities where the government and sector could partner to improve resiliency for those regions.

2.3. Legislative frameworks

You asked if there were any competition rules impeding planning for a more resilient network. The TCF is not aware of any specific competition rules that are preventing that type of planning. However, we will note any constraints or proposals for change if they are encountered as part of the TCF's work on resiliency planning through the TEF.

The TCF will continue to represent the sector where telecommunications resiliency is affected by legislation. Currently, there is a focus on the Resource Management Act (RMA) reforms that are being considered. The sector relies on being able to flexibly deploy capacity to respond to unexpected demand and events. It is important that legislation, in particular the RMA, enables rather than prevents providers doing this. We rely on MBIE to ensure that our interests are represented at the table and look forward to further engagement with officials as the reforms are defined.

3. Conclusion

The TCF is keen to work with government to promote confidence in the sector and ensure consumers continue to have access to reliable services. It is important that our approach recognises the role of existing infrastructure providers and other initiatives such as the Minister's future of connectivity programme, CDEM Act amendments and RMA reforms.

The TCF looks forward to working closely with your officials to keep you informed on the resiliency of telecommunications networks and discuss any proposals to further strengthen resiliency. Engagement and feedback on our areas of focus would be welcomed.

If you have any further questions relating to the telecommunications resiliency that have not be answered in enough detail, please do not hesitate to table these for discussion.

Yours sincerely



Paul Brislen
Chief Executive Officer
New Zealand Telecommunications Forum (TCF)

Released under the Official Information Act 1982



Telecommunications Resilience Study

May 2022

© 2022 The New Zealand Telecommunications Forum Inc. Except as provided by the Copyright Act 1994, no part of this material may be reproduced or stored in a retrieval system in any form or by any means without the prior written permission of the New Zealand Telecommunications Forum Inc.

1. Introduction

This report aims to provide an overview on how New Zealand's telecommunications sector operates, responds to different hazardous events and what measures are in place to manage these events and to mitigate risks.

The telecommunications sector is one of the most complex utility frameworks in New Zealand. It encompasses a blend of commercial and competitive interests. When there is a serious threat to the network, the industry comes together to deliver operational unity where barriers are lowered and a collaborative approach is taken to protect the telecommunication imperatives of New Zealanders

The telecommunication sector is a Lifeline Utility under the Civil Defence Emergency Management Act 2002 and the importance of sustaining assets and the services for consumers cannot be overstated. The reliance and expectations of New Zealanders to stay connected in today's economic and social climate cannot be underestimated.

Although the focus of this study is principally on the physical resilience of the networks and services, it will also briefly mention how the industry responds to significant disruptive events. The report looks at the overall resiliency of the telecommunications sector and the factors that build towards a balanced and considered level of resiliency through mechanisms such as investment, regulation, competition and collaboration.

We would like to acknowledge and thank representatives from a wide range of telecommunication providers who have provided input and feedback in developing this study.

Released under the Official Information Act 1982

Contents

1.	Introduction	1
2.	Defined Terms	3
3.	Overview of telecommunications resiliency	5
3.1.	Investment	5
3.2.	Regulation and the role of Government	6
3.3.	Competition	7
3.4.	Collaboration.....	7
4.	Balancing resilience with customer needs	8
4.1.	Impact of market trends on resilience.....	8
5.	Events that impact telecommunications	8
5.1.	Natural hazards	8
5.2.	Telecommunication network damage by third parties	12
5.3.	Supply chain risks.....	12
5.4.	Pandemic risks	12
6.	Telecommunications sector response to emergency events	13
6.1.	Incident response framework	13
6.2.	Restoring services during an Emergency and a Crisis	14
7.	Focus areas for improving sector resiliency	15
7.1.	Emergency response	15
7.2.	Additional network investment	16
8.	Conclusion	16
	APPENDIX A: Case Studies.....	17
	APPENDIX B: The Telecommunications Emergency Forum	20
	APPENDIX C: Overview of Networks	22
	APPENDIX D: Resiliency Properties of the Networks	32
	APPENDIX E: The TCF	37

2. Defined Terms

These terms are found in this paper and describe the elements that are present in telecommunication networks.

Access Network	An access network provider is responsible for providing connectivity between an exchange / data centre to a local customer base. Historically that was done predominantly over copper cable but is increasingly being supplanted by Fibre and Fixed Wireless delivery - Chorus, Northpower, Tuatahi Fibre, Unison Fibre, Enable Networks (Fibre) and Spark, Vodafone, 2degrees and WISPA NZ (Fixed wireless).
Cell Site	An installation that provides the radio equipment that communicates with cellular handsets and other mobile devices.
Central Office	An interchangeable term for Telephone Exchange – usually a larger purpose-built structure that houses electronic equipment.
Customer	Means a Person who has a billing relationship with an RSP in respect of the relevant Telecommunications Service. The Customer may also be referred to as an End User.
Core Networks	Also known as a “transport” network providing inter-city/town linking, principally buried fibre links, but also some microwave radio – Chorus, Spark, Vodafone, Vocus, Transpower and Kordia
Data Centre	A highly robust and secure facility established mainly to allow telecommunication and digital services providers to house their equipment in a controlled and monitored environment.
DMR	Digital Mobile Radio (can also be used for Digital Microwave Radio as used in fixed networks)
International Networks	Principally delivered over submarine cable network operators, Southern Cross, TGA (Tasman Global Access) and Hawaiki. A small residual number of New Zealand originated satellite services are delivered through the Warkworth Satellite Earth Station, and those are provided mainly to locations such as the Chatham Islands, Scott Base Antarctica and some Pacific Islands.
Latency	The time in milliseconds that it takes a digital signal to travel from the originating to the receiving device.
Lifelines Utility	An entity that provides essential infrastructure services to the community. These services support communities, enable business and underpin the provision of public services.
Link	Term for a connection between nodes.
Mobile Networks	Often referred to as cellular, this service accesses its customer base using radio propagation in the form of “cells” that have overlapping coverage and allow a user’s handset to travel between cells using handoff technology to maintain the call. Spark, Vodafone and 2degrees. Other mobile options are LMR (Land Mobile Radio) and DMR (Digital Mobile Radio) services offered by Vital, who have a comprehensive network throughout the country.

Node	Term for a network element that provides inter-connectivity for one or more Links within a network.
Optical Splitter	A passive device that splits the optical signal into multiple branches to serve UFB customers – it allows light to travel in both directions.
POI	Point of Interconnect – between and RSP and network carrier
POTS	Plain Old Telephone Service (also referred to as PSTN)
Route	Refers to a geographical path between Telecommunication Central Offices or Sites.
Satellite Networks	Used to deliver Internet and voice services generally to remote / rural locations that cannot access those services using land-based options, or that the existing land-based options are unable to provide the level of service that the customer requires. Global Star, Starlink and Kacific are examples of high-capacity providers. Telephony / SMS / low speed Internet services delivered over Inmarsat and Iridium are also used for personal remote and emergency communication.
Sector	A specific part of a route.
Site	A smaller version of a Central Office usually involved with aggregating access network technologies and linking back to a Central Office. A site could be an electronic cabinet.
VHF / UHF	Very High Frequency / Ultra High Frequency
WISPA	Wireless Internet Service Providers Association of New Zealand.

Released under the Official Information Act 1982

3. Overview of telecommunications resiliency

This report provides a snapshot of the current level of resilience of New Zealand’s telecommunication services and some insight into how the industry works during times of crisis. The goal of the industry is always to ensure any disruption to a customer’s telecommunication service is minimised and that outages are repaired as quickly as the situation allows.

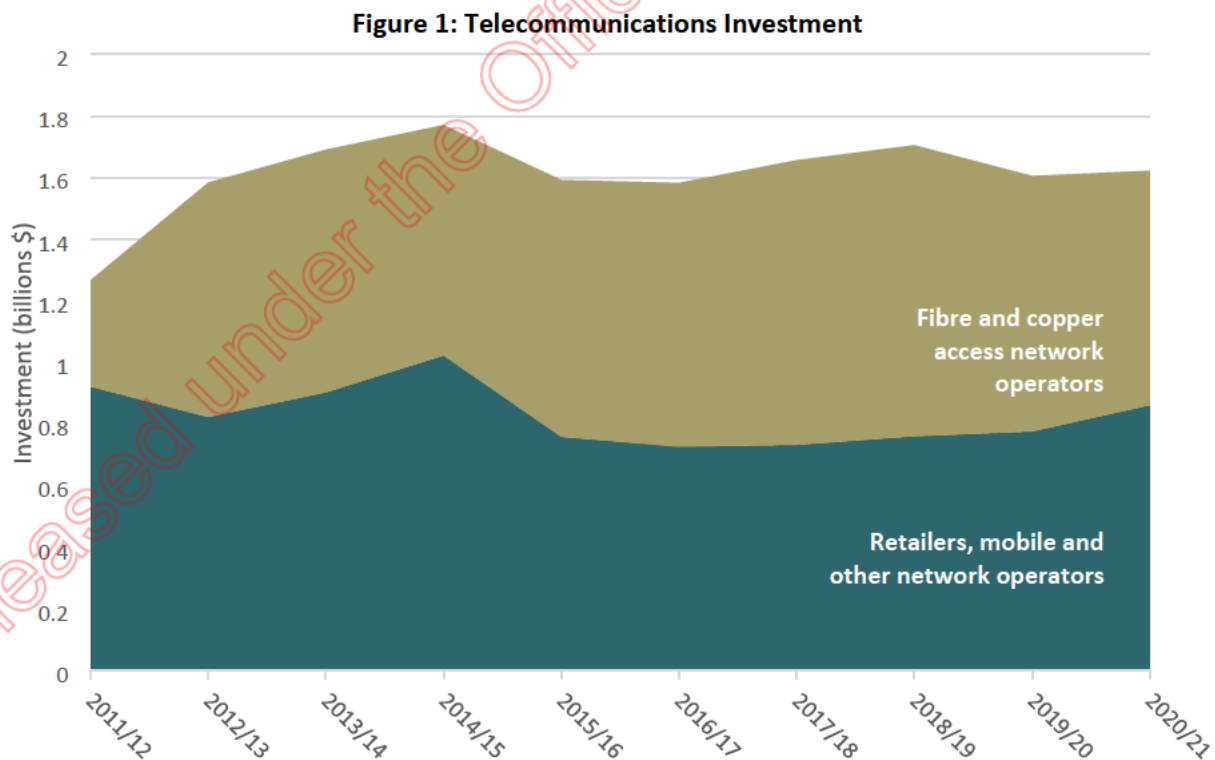
Telecommunications has become as much an essential service as electricity or water. There is an expectation that telecommunication services are always available and although network uptime is generally discussed as being “five nines” (that is, 99.999% reliable) like any key infrastructure it can and is affected during an emergency event. Building resiliency into the network to minimise the impact and maximise the ability to restore and repair is an important part of the sector’s business operations and strategy.

There are various factors that contribute to the telecommunications sector’s resiliency, including investment models, regulatory mechanisms, competition and collaboration that underlies network operations.

Although these factors are never static it is important to ensure they remain in balance to ensure the best response and outcomes during an emergency event. The challenge for the industry is in pre-emptively mitigating emergency events, particularly when it comes to natural disasters.

3.1. Investment

Investment in the sector continues, with overall investment in 2021 at \$1.62 billion¹, with investment in core and backhaul network at \$190million².



¹ Annual Telecommunications Monitoring Report 2021

² Annual Telecommunications Monitoring Report 2021

Where is this investment being made?

'Self-healing networks' are becoming increasingly important to network operators because they provide for networks which repair themselves without requiring human intervention.

These self-healing networks require all of the major network and service providers to manage disaster recovery by having at least two geographically diverse installations (network nodes) that can fully or partially duplicate the nationally centralised service levels provided by that operator.

Investment is also being made to upgrade primary Central Office facilities in the main centres so that they can become highly resilient data centres in their own right. This type of investment must consider geographical and hazardous risks, relying on other data and assessments from Councils and government.

3.2. Regulation and the role of Government

While providers face strong commercial drivers to provide resilient services, there are inevitably gaps where providing resiliency has very high costs and where few consumers benefit. This makes the commercial business case for increased investment in some areas difficult if not impossible. New Zealand's geography and population density across parts of the country create resiliency and investment challenges in this regard.

Despite these challenges, there is a good track record of private partnership with government, which has resulted in meeting those investment challenges. The building of the Ultra-Fast Fibre (UFB) network is a good example of this and more recently the government's funding of the West Coast fibre cable. There are likely further opportunities for partnership which could be considered as part of the Government's Future of Connectivity programme.

Council and government research into resiliency and emergency response across different regions is a valuable source of information for the sector's future investment and resiliency planning. For example, the Massey University is currently carrying out research on infrastructure planning and minimum levels of service for the Wellington region during an emergency event. This research could result in informing Wellington Council and regionally-based providers when developing their future emergency event management planning.

Any work underway by central or local government on post-event planning in various regions importantly must be communicated back to the sector to ensure that at a company level and also a sector level there is robust emergency planning to support a collaborative response arrangement.

Government policy initiatives also determine resiliency for many users. For example, as part of delivering the UFB programme, which will provide fibre-to-the-home connectivity to 87% of New Zealanders by end 2022³, participating UFB partners had to meet resiliency requirements in the agreed network architecture with Crown Infrastructure Partners. The purpose of these requirements was designed to limit the impact of service outages with duplication of key elements that serve larger numbers of customers.

The Telecommunications (New Regulatory Framework) Amendment Act 2018 determined Chorus is subject to Price Quality Regulation whereby the Commerce Commission approves expenditure plans

³ Crown Infrastructure Partners (2021), *Annual Report 2021: for the year ended 30 June 2021*.

ahead of any investment. The availability and other quality standards for Chorus's fibre network are set by the Commerce Commission. In setting those standards, the Commerce Commission seeks to balance the desire for certain levels of network performance against the costs of maintaining that performance given that the investment required is ultimately paid for by end users. Additionally, information disclosure regulation applies to all LFCs, including Chorus, in respect of their regulated fibre services.

The Government's Rural Broadband Initiatives (RBI and RBI2) also made improvements to resiliency by increasing some of the existing connectivity capabilities and extending broadband coverage further via a range of technologies over the past decade.

3.3. Competition

Telecommunications services are delivered by competing operators who provide services to meet market demands. Therefore, commercial pressures and competition drive resilience improvements to meet customer needs and growing expectations.

This will vary from customer to customer and depends on the customer's requirements, their location and which service is available to them.

For some, a basic service with minimal service guarantee (the consumer-grade offering) is adequate. Others will require a back-up capability (typically a mobile service to support a fixed-line connection). Larger corporate customers may require a bespoke, guaranteed level of service and will pay more for that resilience.

3.4. Collaboration

The Telecommunications Emergency Forum (TEF) is a well-established group of 21 members and provides an intra-industry forum that is convened when the industry needs to collaborate and have a unified focus on restoring Telecommunication services during times of disruption. From a Civil Defence perspective, the TEF is identified as the Telecommunications Sector Coordinating Entity (SCE) and links into NEMA through the Senior Emergency Management Advisor (National Lifelines Utility Coordinator) based in the NEMC Wellington. For more information on the TEF refer to Appendix B.

The Sector has demonstrated not only that it is able to work collaboratively but is also able to foster links with allied utilities, such as power companies, and coordinate with them during a crisis. The Sector's physical presence in the NEMC (Beehive Bunker) adds a new dimension in the inter-sector cooperation as the decision making is done at a level that authorises a greater immediacy of actions on the ground and it enables more than one sector e.g. (power, telecommunications, transport) to coordinate a mutually beneficial response.

Fostering a close ongoing relationship with NEMA, both regionally and nationally, ensures protocols and response plans can continue to be fine-tuned and any response via the coordination channels are quickly established during an emergency event.

4. Balancing resilience with customer needs

The Sector must also continue to respond to technology and market changes, to invest in diverse core network elements and data centres, and continue to extend the self-healing transport networks to additional regions.

4.1. Impact of market trends on resilience

Over the last three decades, the telecommunications environment has undergone significant change to reflect market changes. As a result, centralisation of telecommunication networks has occurred and consumers are able to access new services delivered over new network architecture.

Traditionally, each town or district had its own telephone exchange network delivering voice services. National connectivity (intercity calling and low-capacity digital service) was achieved using inter-exchange links of limited capacity. In contrast, the current digital service environment relies on absolute centralisation where the retail service providers' (RSP) services can only be accessed at handover points that are connected to a Core Transport or Regional Network. To cite a common example, a South Westland customer may get their internet and telephony services from an Auckland-based service provider.

While this has improved choice for consumers, it no longer enables the local "fallback" service delivery as was the case in the switched telephony world where customers could still make local calls within the telecommunication's "island" (exchange or group of exchanges) that remained.

Modern cellular services are equally impacted by the loss of a local or regional fibre link as their backhaul connectivity to the IMS (cellular switch) is likely to be over the same physical cable as that delivering Internet derived services.

To mitigate these risks telecommunication services are increasingly provided from centralised self-healing locations. Subsequently, it is important to identify those population centres that currently do not have service diversity as delivered over fibre (failure of the dominant delivery method). By studying the coverage and service types delivered by alternative providers in an area it is then possible to make a call on what level of outage risk would be acceptable to those communities – and examine options to overcome this risk if deemed not acceptable.

5. Events that impact telecommunications

5.1. Natural hazards

The natural hazards that have historically had the greatest impact on telecommunications are severe storms and earthquakes. These are followed by tsunami and volcanic eruptions.

It is important to emphasise that in the majority of cases, natural disasters affect a limited area of the country at any one time. Telecommunications networks are designed to cope with such cases. Close cooperation between all network operators in emergency events also provides for additional resilience.

Storms

The principal impacts of global climate change can be felt by the increasing number and intensity of severe weather events. Disruption to telecommunications by storms is caused in a number of ways.

Due to the largely unpredictable nature of natural disaster events, the resilience focus is on post-event risk planning. The industry's efforts focus on preparedness to respond to a situation by having resources (such as cell sites on wheels) available at short notice, which has to date been an effective approach.

Flooding

The main impact of flooding on the network is the physical erosion and exposure of underground services often accompanied by land movement placing tensile stress on buried fibre cables. Network providers take care to design their networks to avoid any obvious areas where specific geotechnical features are seen to be a problem and take special measures over river and culvert crossings to protect the network from the erosive effects of flooding. While there has been recent instances where resilience was impacted by the magnitude of an event (e.g. bridge washouts South of Franz Josef), these have been localised events.

There are also instances where the network is damaged by unforeseen impacts of flooding. For example, the instance of high rainfall in South Canterbury in 2019, which caused the Rangitata to burst its banks, take an entirely different route and disrupt both sides of a protected Core Transport network⁴, discussed in Case Study 1, Appendix A.

Widespread loss of power

By far the most likely impact of a natural hazard is the loss of commercial mains power. Major telecommunications Central Offices are furnished with emergency generation and can continue to function. Core Transport cabinets and Mobile sites that rely on power do have battery backup facilities but will require attention if the power outage is prolonged. The services delivered from these sites are usually sustained by the connection of a portable generator.

Damage to aerial plant

Telecommunications towers such as cellular installations, antenna-bearing lattice towers (microwave linking) and stayed masts can all be subject to the impacts of natural hazards such as high winds causing antenna misalignment and damage by flying debris, and lightning strikes. These are typically localised events and connectivity can in most cases be provided by other nearby towers if one is damaged and service is disrupted.

Damage to structures

Although telecommunications Central Offices and other sites are generally well founded structurally and are unlikely to be damaged by wind and rain, they can be at risk of flooding and in those instances, flood protection measures have been integrated into the overall fabric of the installation.

Earthquakes

Damage to structures

Telecommunication Central Offices have historically been designed to a high standard not only to support the weight of early electro-mechanical switching equipment but also in consideration of New Zealand's known seismic activity. Some legacy sites have had additional seismic strengthening work done to reflect their (evolving) importance in the modern network.

⁴ Reported through the TEF

Central Offices and Data Centres built in recent years are designed to a high standard with almost “bunker-style” resilience, where protection against the potential for seismic impacts are integral to the design.

External network structures such as masts and towers, although designed to withstand moderate seismic events, are not immune to the impacts of a severe earthquake where network disruption can be caused either by antenna misalignment or damage to the conductors and feeders that connect the tower to the associated equipment structure. However, it is important to emphasise that in most cases earthquakes affect a specific part of the country, meaning connectivity wouldn't be lost across the entire country.

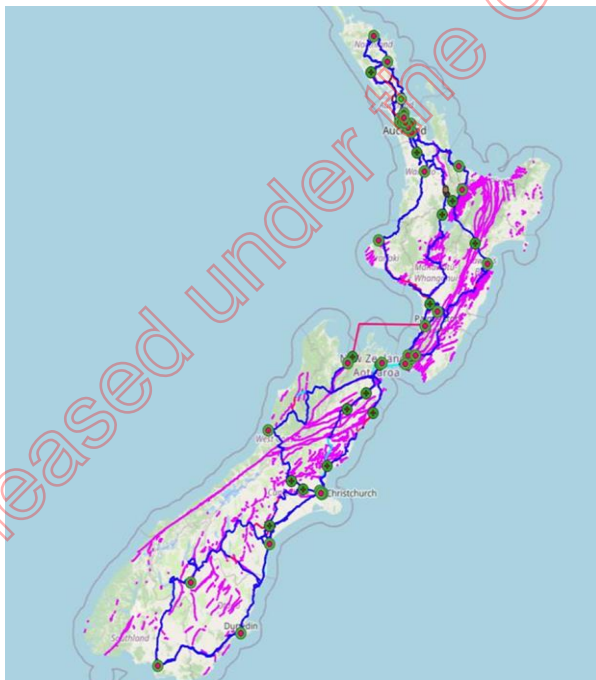
The buried network

The buried fibre network has proven to be very resilient against the impact of moderate earthquakes especially in metropolitan areas where the fibre sheaths are carried in ducts. During the Christchurch earthquake sequence of 2010/11, no fibre links were lost between local exchanges and all core networks out of Christchurch remained operational, however some direct buried (not ducted) links required remedial work to restore cable routes to normal reliability.

In the case of the 2016 Kaikoura earthquake, the degree of movement of the terrain in which the fibre cable was laid severed the cable in over 60 locations on the East coast road between Oaro and Ward⁵. Where roading remediation works occurred on that route, the replacement fibre cable(s) are now placed in ducts. This is expected to help in any future earthquakes.

The figure below shows the geographical disposition of a Core Transport network (in green) overlaid against New Zealand's known major fault lines (in pink). Apart from Auckland and the Far North, no other regions are immune to this hazard.

Figure 2: Geographical Disposition



⁵ Reported through TEF

Tsunami

With the recent transition to UFB services, the telecommunication network architecture is becoming more resilient to inundation as a fibre reticulation is passive and water immersion does not have an immediate effect on service delivery. Also, with the move to passive optical networks, the network's electronics become more centralised into larger sites whose physical construction and location can be selected to be remote from the potentially affected areas to provide protection against inundation.

This is important, because telecommunication networks by necessity track population concentrations and as a consequence there will be instances where an existing Central Office or site will share a potential tsunami inundation exposure with the customer base that it serves. Sites are established geographically to optimise the service delivery to a particular customer grouping and network delivery method.

The worst impacts to the network would be the inrush and outrush scouring effects exposing and dislodging buried and above ground plant, and the restoration of telecommunications would likely be by means other than the restoration of landlines.

Other than a distant tsunami – such as that originating in South America or Japan, providers have little opportunity to provide any reactive protection (such as sandbagging) to low lying sites. Where there is notice, it would be of use for NEMA to make scenario specific inundation maps available to the telecommunications sector and other utilities immediately upon notification of a tsunami.

Volcanic Eruption

The Central North Island does present a potential hazard mainly in the form of a windborne ashfall plume. Tongariro has been active and more recently Mt Ruapehu volcanic unrest continues. It is not possible to plan for such a sporadic event, and at best a potentially impacted telecommunications company can only develop high level operational guidelines to manage the impact.

In addition to considering the health and safety of personnel, the impact of a heavy ash plume landing on a telecommunication installation such as a Central Office or Site with electronics could be catastrophic. All sites of this nature require equipment cooling and this is done mostly using split system air-conditioners (heat pumps) or fresh air fans for the smaller sites.

Significant ashfall would render these systems inoperative and as a consequence the temperature in the equipment room would rise to the point where the equipment would likely shut down (by thermal cut-off) or be irreparably damaged. It is likely also that the national or local power grids would be offline during a volcanic incident, impacting the customer's ability to consume telecommunication services.

Ash clouds also pose a problem for satellite communications as the user's dish needs clear visibility of the sky, and the satellite, in order to connect to the service.

In an ashfall event, health and safety considerations would govern a telecommunications company's ability to attend a site for restoration.

Figure 3: Location of New Zealand Volcanoes



5.2. Telecommunication network damage by third parties

A key and frequent risk to underground high-capacity networks is damage from third parties. This can be from individuals digging a fence post to major civil contractors. Network operators frequently engage with stakeholders to try to mitigate and reduce this damage occurring via education, and encourage the use of services like, BeforeUdig. Monitoring of infrastructure and information sharing across other sectors like construction are also ways to minimise network damage occurring in the first instance.

5.3. Supply chain risks

The recent pandemic has outlined issues around supply chains, which can be out of the control of telecommunications companies but cause a real threat to telecommunication services. While not as direct as a natural disaster, being unable to source parts or devices does cause problems for New Zealand-based telecommunication providers. There is no local supply of high-end electronics deployed by providers, most are manufactured offshore. This is not an issue isolated to the telecommunications sector and nor is it an issue we can resolve in isolation. Like in many industries, Covid-19 contributed to significant supply chain issues, which in some cases meant increased costs of key telecommunications network components.

5.4. Pandemic risks

The COVID-19 outbreak highlighted the importance of good quality connectivity to keep families, communities, schools and workplaces connected. To support this connectivity telecommunications providers must keep the networks running. While automation has been the driving force behind much of the industry's development over the past 30 years or so, the industry still needs people to manage and maintain networks.

Ensuring the telecommunications sector is treated as an essential service by the Ministry of Health and other associated agencies during a pandemic is one learning the sector has taken away from recent events and the key to ensuring the networks can remain operational for the future. Restrictions on the movement of people meant that in some cases technicians were not able to access key equipment, plants or move between regional border crossings because telecommunication technicians weren't categorised as "critical" staff.⁶ This can impact on a network operators' ability to repair parts of their network. International border closures also reduced the sector's ability to access critical labour from overseas, an issue that was widespread across New Zealand's industries.

6. Telecommunications sector response to emergency events

The level of investment into resilience by individual operators and cross-industry collaboration during emergency events has to date ensured a robust response from the telecommunications sector during emergency events.

Investment, assessment and then coordinated collaboration creates a strong foundation for the Sector to respond to events, restore services and support communities. Sector preparation and planning is an area which will continue to develop and for the sector to make improvements. It is this area which can achieve the greatest impact in response to an event and assist central and local government in their own emergency event management and resiliency planning.

6.1. Incident response framework

Broadly, we have three types of incidents, illustrated in the table below. Each provider will have its own process, but for the purposes of this report they are identified as:

- business as usual (BAU)
- emergency
- crisis.

	FEWER CUSTOMERS AFFECTED			MORE CUSTOMERS AFFECTED
HIGH IMPACT	GREEN	YELLOW	RED	RED
	GREEN	YELLOW	YELLOW	RED
LOW IMPACT	GREEN	GREEN	GREEN	YELLOW

*BAU = GREEN Emergency = YELLOW Crisis = RED

BAU

At an operational level, providers routinely manage outages and issues, largely without customers ever seeing any impact. This is BAU event handling and each provider manages such activity within its own parameters. During normal BAU operations, providers are continuously responding to minor faults in their Core and Access networks affecting normal reactive restoration of services.

⁶ Citation needed

Emergency

An emergency event requires inter-operator coordination, or support from external parties; scenarios cover localised flooding or a weather event. In an emergency, providers may engage via the TEF, or depending on the number of impacted customers directly with each other and other essential services within the particular area.

Customers within the affected area will be impacted, communication on restoration of services will be directly managed by their providers and more generally by Civil Defence and emergency services working in the area.

Examples of emergency level activation would be the Rangitata flood caused by a severe localised weather event, refer to Appendix A.

Crisis

For an incident to be deemed a 'crisis' it will typically have an impact on a broader scale – either an entire region will be affected, or the impact will be felt over a longer than normal duration. The TEF will be activated with direct engagement with NEMA. In an extreme situation the "Beehive Bunker" will likely be activated. Events such as the Canterbury earthquake would require a Crisis level of activation.

Customers will be impacted across one or multiple regions over a longer period of time. Restoration of services will require a multi-provider effort working closely with NEMA, emergency services and other utilities. Prioritisation of customers may be required such as community hubs, medical and emergency centres.

This type of incident for the telecommunications sector, could result in a specific critical network element catastrophically failing in an otherwise intact Central Office environment, or it could describe the physical destruction of a Central Office rendering it unable to support any remaining infrastructure.

The highly interconnected nature of New Zealand telecommunications networks makes it difficult to predict a pan-telecommunications impact of a specific asset outage, such as loss of a major Central Office.

Critical network elements contained within these sites are designed to "fail over" to a pre-determined standby condition which may involve transferring its service capacity to an alternative site having network elements that are dimensioned to be able to replicate the full traffic handling capability of the failed site.

6.2 Restoring services during an Emergency and a Crisis

Restoration of services will be determined by a number of factors, such as the extent of the damage, location, access and prioritisation of services to particular locations to support other services as required.

When a more serious network impacting event occurs, individual providers will have equipment that can be used to quickly restore services to impacted areas, such as Central Office / electronic cabinets / cell-sites on wheels and portable generators. However, network operators may require support to get technicians to a site and/or access to a cabinet or cell site and in some cases, helicopters will be required to deliver generators or replenish batteries in order to maintain operation.

7. Focus areas for improving sector resiliency

There are a number of opportunities identified by the sector that will improve its preparedness and provide assurance to government and consumers.

7.1. Emergency response

Developing a pan-industry emergency management plan through the existing TEF forum will set out the telecommunications sector's response will provide assurance to central and local government about the level of preparedness and resiliency across the sector. This plan will consider further opportunities such as:

- a. Priority access to telecommunications sites during emergencies. This will require agencies such as Waka Kotahi and the Ministry of Transport to prioritise land transport access and access to helicopters for situational assessment and transportation of essential telecommunications equipment and personnel.
- b. A nation-wide fuel plan that includes priority supply to telecommunication providers. There are fuel plans across different Emergency Management Agencies across the country, but not all, and they are not uniform.
- c. Optimising how we enable sharing of surviving network capacity to normalise services into an impacted region of New Zealand. This approach was used successfully following the 2016 Kaikoura earthquake and again after the 2019 Rangitata flooding.
- d. A sector-wide crisis exercise programme focused on various probable natural disasters. Some examples might be:
 - i. Hikurangi subduction fault
 - ii. AF8 - South Island Alpine Fault
 - iii. Wellington - one of the likely earthquake scenarios
- e. Establish principles for engaging with local and regional Lifeline Utility Groups, to consider how we might ensure a consistent approach that improves public outcomes and more efficient engagement. For example, there are different approaches to risk assessment reports (natural hazards, climate change impacts, etc) across the country. Currently, this information is being provided only where regional or local Lifeline Utility Groups are conducting projects, for which funding is not necessarily provided by the government but by some of the members. A consistent and full assessment of local risks, by local groups, would improve planning outcomes.
- f. Establish a communication plan with local and central government to keep informed on research work being commissioned and seek consultation and engagement.

7.2. Additional network investment

This is a dynamic sector and the technologies and infrastructure deployed by operators – and services demanded by customers – are evolving. These new services that are important for public safety, social inclusion and the digital economy increasingly rely on infrastructure such as resilient transport networks and data centres. As set out in this report, we are seeing significant industry investment in new resilient infrastructure such as new access fibre robust handovers, national transport fibre routes, highly resilient data centres and service “cores”, and international connectivity. The sector is responding to customer demands for resilient services, ensuring modern technologies and services are available to our markets.

However, New Zealand’s geography and population density across parts of the country creates resiliency challenges, and in some cases addressing these may not be possible for network operators to fund on their own.

While providers face strong commercial drivers to provide resilient services, there are inevitably gaps where providing additional resiliency has very high costs, and in some cases, where few consumers benefit, making the commercial business case difficult. In these cases, investment in resilience needs to be balanced with the acceptable level of risk the industry is willing to take. This is determined, among other factors, by the existing level of resilience and the likelihood and impact of an event occurring that would present a significant risk to resilience in those areas.

There is an economic challenge to add further resiliency to transport routes into some regions due to, for example, low end user numbers or incremental nature of resiliency benefits of the investment. Accordingly, a robust assessment of regional connectivity would be useful to identify opportunities where the government and sector could partner to improve resiliency for those regions. We recommend the sector engaging with Government further on regional resiliency options in the context of the Future of Connectivity review.

8. Conclusion

This report provides an overview of telecommunications resiliency in New Zealand and sets out the future challenges.

The sector will continue to work with government to promote confidence in the sector and ensure consumers continue to have access to reliable services.

To date, the telecommunications industry has a proven track record of working together providing a robust collaborative response to restore services as soon as possible following events. The challenge is in pre-emptively mitigating these scenarios and it is in this space that the TCF believe efforts to improve resiliency could achieve the greatest impact for consumers.

APPENDIX A: Case Studies

Case study 1: Climate change – failure of a geo-diverse fibre link

In early December 2019, South Canterbury experienced a severe rainfall event resulting in extensive flooding and causing rivers to become swollen.

Chorus maintains a geographically diverse network between Christchurch and Timaru which is part of a ladder network that extends from the top to the bottom of the South Island. The principal other user of this network is Spark.

s 9(2)(b)(ii)

In this case the Rangitata river flow was so high that it deviated from its normal channel and burst its banks upstream of the bridges that had the fibre cable attached. The bridges remained undamaged by the flood but the diverted flow caused severe scouring of the road corridor immediately South of both bridges breaking the fibre laid in the roadway berm. The impact of this was to severely impair telecommunication from Timaru South.

One cable – s 9(2)(b)(ii) – remained intact and continued to provide limited services (including cellular 111) to the lower South Island. Spark did manage to transfer some services to this cable by optical patching.

Telecommunication operators take special care with bridge mounted cable crossings. The cable is usually securely mounted on the downstream side of the bridge to protect it from debris that may be washing down a swollen river. If the river had remained within its normal channel, the cable would have been protected but the river's wide deviation was an unforeseen event. It's also possible that with the volume of water encountered in this instance, scouring of the bridge abutments may also have damaged the cable, causing service loss.

Events such as this provide an opportunity to focus on what engineering good practice should be used for buried cable reticulation in the future especially if located near braided rivers or crossing culverts that have potential for scouring due to increased heavy rainfall.



Case Study: Climate change – flooded culvert Buller



A recent example, refer to images above, of very heavy rain occurring in Buller caused this normally dry culvert to deliver a torrent of water from the adjoining steep hill into a river alongside the road.

The bright blue cable is the fibre link between Westport and Karamea. Remarkably the service remained operational in spite of the tensile force exerted on the cable.

Released under the Official Information Act 1982

APPENDIX B: The Telecommunications Emergency Forum

The TEF is administered by the TCF. Its members include: 2degrees, AWACs, Chorus, DTSANZ, Enable Networks, Internet NZ, Kordia, Northpower Fibre, NOWNZ, Spark, Symbio, Vital, Transpower, Trustpower, Tuatahi Fast Fibre, Unison Fibre, Vector, Vocus, Vodafone, NEMA.

The Forum is convened if it is agreed that the scale of a local (or national) telecommunication disruption is well beyond the BAU capabilities of individual companies and it provides a platform not only for resource sharing, but also allows for the development of Sector based priority driven service restoration strategies. NEMA's Local or National Lifelines coordinators are usually invited to provide their input to these sessions.

The Forum is looking to establish quarterly or twice-yearly operational meetings, at the request of its members, and look at developing readiness planning in partnership with NEMA.

The National Emergency Management Centre (Beehive Bunker)

Part of the TEF is to be able to respond to the activation of the National Emergency Management Centre (NEMC) during a major National or Regional event. NEMC is located in the basement of the Beehive and is also referred to as the MCDEM Bunker.

As an outcome of the 2016 Kaikoura Earthquake post event review, it became clear that the telecommunication industry would benefit greatly from having a "voice" right in the Bunker's operations centre. As a consequence, the TCF has established a roster of local Wellington telecommunications representatives who will physically domicile themselves in the Bunker's operations room during a crisis. The sector representative becomes the TEF's conduit directly into the centre of the MCDEM operational environment) allowing them not only to represent logistical requirements but also facilitating real time tactical information exchange.

TEF in action

The November 2016 earthquake and the resultant damage to the Eastern fibre route effectively isolated Kaikoura from outside communications and the failure removed the Eastern side of the diversity ladder bestowing critical importance on the remaining Western arm of the ladder. It is worth noting that because the Kaikoura area had a 'POTS' switch, people within the township were able to contact each other.

The only intact fibre link in the Kaikoura area was offshore - the Vodafone 'Aqualink' cable which provides express capacity from Christchurch to Wellington. As the result of industry collaboration, the Aqualink was able to be intercepted at the Kaikoura landing point and equipment installed to provide (within four days) almost normalised service into Kaikoura and also restore some diversity into the core network.

The temporary restoration of the eastern core fibre route occurred through cable overlays where the fault was inaccessible, some slung from helicopters for hundreds of metres. Chorus and Spark also brought forward plans for an inland fibre route to increase diversity.

The event highlighted how important it is for the sector to have a collaborative forum such as the TEF to develop those initial restoration strategies which can then be physically implemented by the most appropriate participants. It was useful also to be able to provide a unified response to NEMA and bring their personnel into the discussion.



Released under the Official Information Act 1982

APPENDIX C: Overview of Networks

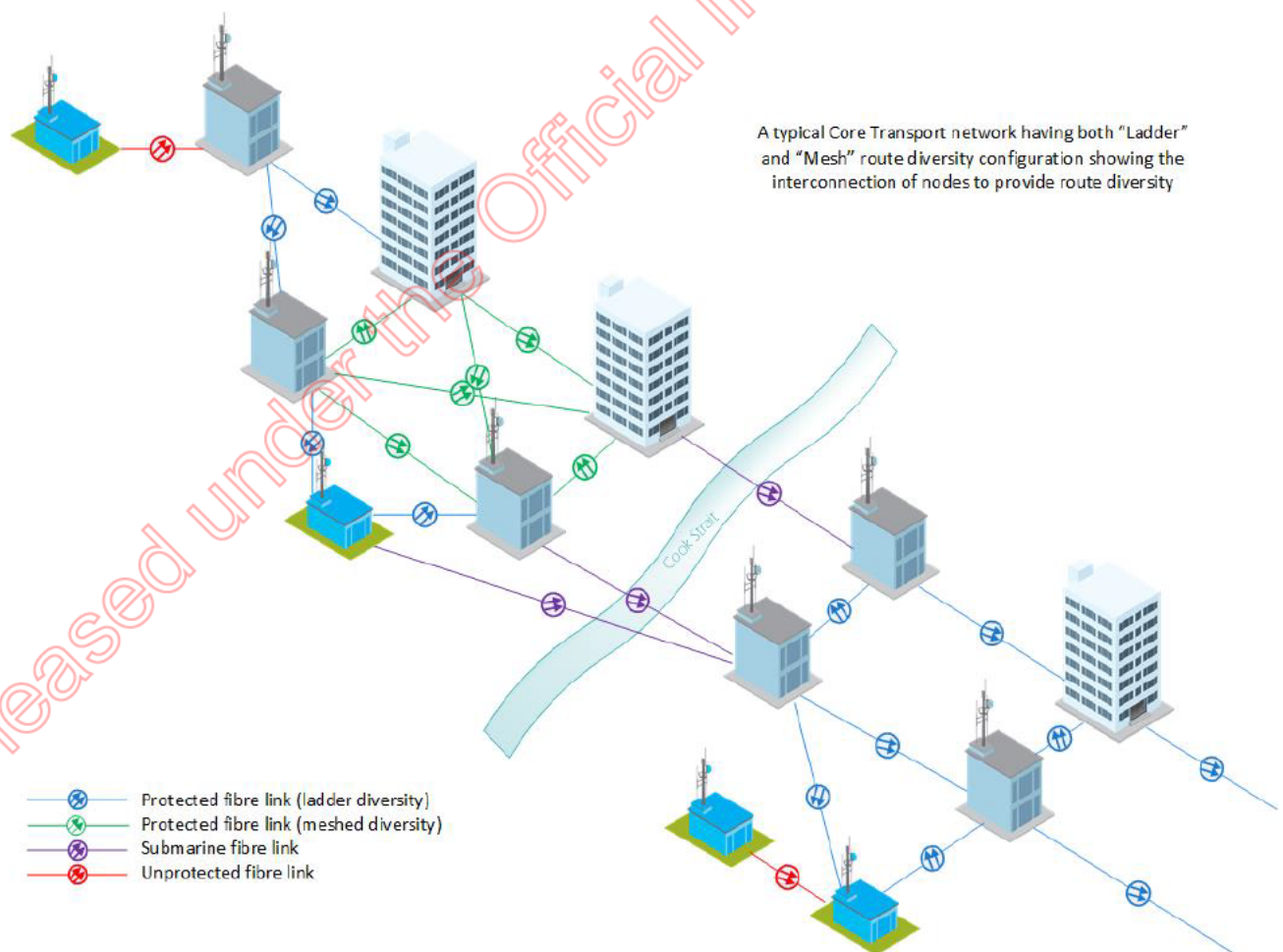
This section sets out the different types of networks operating in the New Zealand telecommunications environment.

Core Networks

Forming the backbone of an operator’s national network, their purpose is to serve the entire country with inter – region communications. There are multiple Core Network operators who collectively use a combination of land-based fibre and radio systems, each having varying degrees of geographic penetration throughout New Zealand. In an Internet service delivery context, the Core Network provides a highly resilient facility (like a network cloud) that permits national interconnectivity between the customers in a local access network and their respective service providers, irrespective of their national location.

Core Network operators generally run a meshed / ladder network using a combination of geographical fibre route diversity and geo-redundancy of equipment sites. This means that equipment nodes (exchanges / data centres) can affect a “self-healing” function by redirecting digital traffic away from a failed link into those that are still operational.

Figure 4: A Typical Core Transport Network



A typical Core Transport network having both “Ladder” and “Mesh” route diversity configuration showing the interconnection of nodes to provide route diversity

Aggregation and regional transport networks

The aggregation and backhaul networks connect access networks from concentrated points of demand at, say, the local exchange or mobile site to highly resilient and high-capacity Core Networks. These networks are important in that they connect regions to the core networks.

Access Networks

Access networks are responsible for delivering services to a local customer base.

Historically this was done using copper cable reticulated from a local exchange to the customer and although Copper-based services are still available, it is increasingly being supplanted by the UFB fibre and 5G mobile network-based access networks, overlaying the existing copper plant.

Fixed wireless is also an option that is being increasingly taken up by consumers across New Zealand. Radio based solutions for this include cellular service (as in RBI), WISP (Wireless Internet Service Providers) and a range of Satellite services.

Access networks are generally the most vulnerable components of the overall telecommunications environment as they generally cannot be furnished with redundancy features such as those found in self-healing regional and core networks. Customers can choose to improve their overall service's reliability by implementing a fallback service. For example, a UFB customer having an additional connection using an alternative technology (such as wireless).

Fixed Access Networks

Cable fed access networks

Cable fed access networks are by far the most prevalent service delivery method used by the Telecommunications sector. Service to the "last mile" has undergone significant evolution not only to future proof the network for future service delivery but also to meet the ever-changing needs of consumers. Historically, access network cables were Copper paired cables but services are rapidly moving to becoming fibre optic such as the UFB (Ultrafast Broadband) networks in use today.

FTTN (Fibre to the Node)

As recently as the early 2000s, due to the demand for faster Internet speeds, fibre fed electronic cabinets were installed nationally to effectively shorten the copper cable distances to the customer's premises allowing the use of a range of DSL (Digital Customer Line) technologies. This culminated in the use of VDSL (Very high-speed Digital Customer Line) and these services are still available where Fibre delivered services are not yet installed.

Alongside this service there were early instances of FTTH (Fibre to the Home) before the advent of UFB, that was reticulated in a similar way to the copper network.

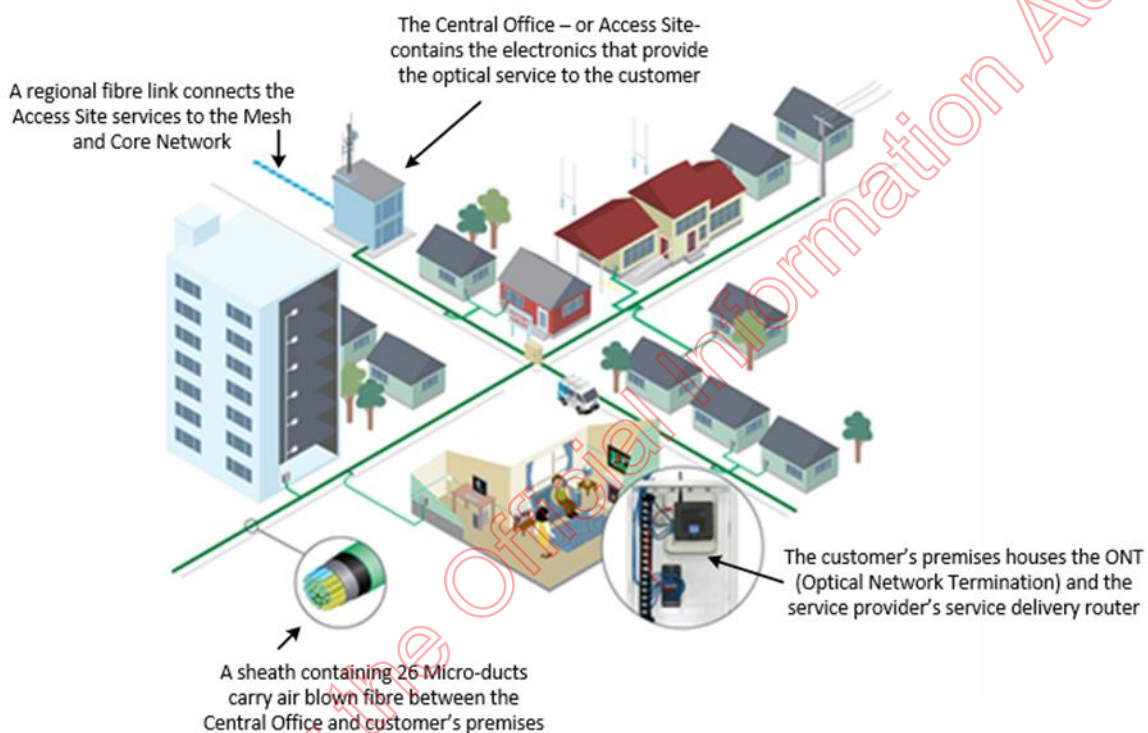
UFB (Ultra-Fast Broadband)

UFB is the new standard for fibre based Broadband service delivery in New Zealand. In areas where it is available, it delivers fast and uncongested internet speeds that allows the customer to access a

myriad of digital services and applications. Over 1.8 million homes and businesses (87% of New Zealanders) will have access to UFB by the end of 2022.⁷

The service is provided using a passive optical network (abbreviated as PON) – meaning that between the customer premises and the Central Office (exchange) there are no intermediate electronics. The physical streetside buried network reticulation is in the form of a sheath of bundled micro-ducts that carry individual air blown fibre units from a POLT (Passive Optical Line Terminal) in the Central Office to the customer’s ONT (Optical Network Termination).

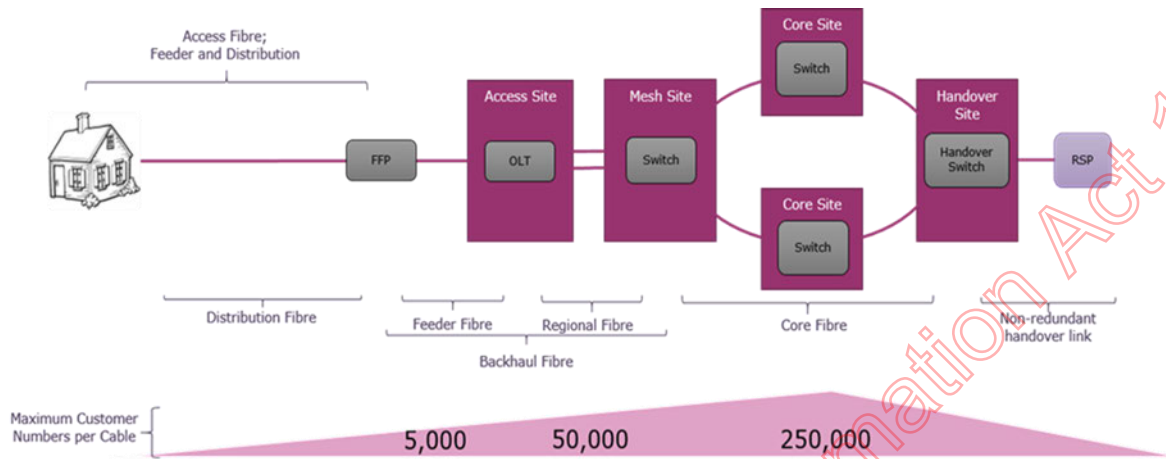
Figure 5: Fibre Network



The UFB underground plant is physically more robust than the copper reticulation that it replaces but if the network is damaged by a third party (like a civil contractor’s digger bucket) the time required to restore services to the impacted customers is greater than it would have taken to fix a copper reticulation of the same capacity. This is because the service is delivered using a bundle (sheath) containing 25 Micro-ducts into each of which has an air-blown fibre unit that serves one customer’s premises. Each tube needs to be repaired and then a new fibre unit blown from the cabinet / exchange to the premises. By comparison, a Copper cable can be repaired at the site of the break without needing to replace end to end service reticulation.

⁷ Crown Infrastructure Partners (2021), Annual Report 2021: for the year ended 30 June 2021.

Figure 6: Illustrative Customer to Service Provider linking elements



Access Site - The far left of the diagram depicts the customer’s premises with a fibre link into an “Access” site, where an electronic network element called a POLT (Passive Optical Line Terminal) aggregates a large number of customers. This equipment is usually located inside a Central Office but some operators also install the equipment into streetside cabinets

Mesh Site - Most Access sites have a protected (geographically diverse) fibre link to the Mesh site. The Mesh site aggregates the digital traffic from a number of Access sites and provides protected connectivity into the Core Transport network.

Core Site(s) – This diagram shows only two Core Sites, but in actual fact there may be many Core Sites that are responsible for providing the protected conduit that is required to reach a Handover Site.

Handover Site – this is where the customer’s digital connection is accessed by the Internet Service Provider. In fact, the services originating from a single Access Site may be delivered to many geographically displaced Handover Sites, depending on where multiple RSPs choose to have their customers’ service delivered.

The most vulnerable part of a UFB service is the section between the customer’s premises and the POLT (within the access site). Although modern Micro-duct sheath is made from very tough HDPE it remains an unprotected path to the end user and is susceptible to third party damage.

Reliance on power to the property

The UFB passive optical network requires that the customer provides a reliable power source at the premises to maintain not only the ONT (Optical Network Termination) but also to any attached service delivery device such as a router. (In contrast to the original POTS service where basic speech power to the phone was provided from the exchange or cabinet).

There are battery backup options available that will sustain a Broadband Modem or ONT for about an hour, but they are not in widespread use.

To protect their network against a widespread power outage, a provider goes to great lengths to make sure that their Central Offices and Cabinets have power backup facilities, but if the customer does not have a power backup facility for their telecommunication, they are unable to consume the service.

Providers of Ultrafast Broadband fibre access networks

In 2011, then Crown Fibre Holdings, now Crown Infrastructure Partners (CIP) triggered a UFB build programme that allocated specific areas to four participants. Chorus had the largest share (75%) of the deployment with the balance being awarded to three other Local Fibre Companies (LFCs) in their allocated regions. In addition, there are now several power companies that also offer competing fibre services.

Chorus

Chorus was formerly part of Telecom New Zealand (now known as Spark) and after demerger from Telecom retained extensive core and access networks throughout New Zealand. In addition to its fibre network Chorus also provides copper-based services throughout New Zealand though has the ability to withdraw these services where fibre is available.

Northpower Fibre

Northpower is based in Whangarei and reticulates an area roughly bounded by Hikurangi, Dargaville and Mangawhai. Their network is roughly a 50/50 mix of underground and aerial fibre. The network has very much a hub and spoke configuration where route diversity is limited to those sites which are approximately 10KM radially distant from the Whangarei CBD. Northpower use a combination of their own buildings and electronic cabinets to deliver their services.

Tuatahi First Fibre (formerly Ultrafast Fibre)

Based in Hamilton, Tuatahi First Fibre reticulates underground UFB fibre networks in selected townships throughout the Waikato, Taranaki, Bay of Plenty and Whanganui. Tuatahi's Central Offices are co-located in Chorus and Spark exchange buildings and their external network reticulation is passive optical fibre using optical splitters inside above ground cabinets.

Enable Networks

Enable Networks are based in Christchurch and reticulate Christchurch city and the areas roughly bounded by Rangiora and Kaiapoi in the North and Rolleston and Halswell to the South. Enable have laid their own backhaul network that interconnects 12 Central Offices, two of which are their network's POI (Points of Interconnect). Enable's UFB customer network reticulation is entirely passive.

Other UFB Providers

Throughout the country other operators such as Unison and Network Tasman also reticulate fibre-based Internet services alongside their core business (Power Supply) – in selected pockets of their service areas, they operate in direct competition with the incumbent UFB network providers.

Wireless Access Networks

Wireless Internet Service Providers (WISPs)

There are ~37 wireless internet service providers nationally affiliated with WISPA NZ and an additional small number who operate independently of this. WISP networks originated in response to a demand for better internet service principally in rural NZ.

Traditionally WISPs have been focused on radio-only delivery, but recently larger WISPs have started to provide buried fibre access to larger rural community clusters that are distant from but in some instances over-build the local fibre company's reticulation.

Fixed Wireless access (Cell Site derived)

The three national Cellular mobile providers in New Zealand (Vodafone, Spark and 2degrees) offer a Fixed Wireless service. This service can be delivered from any Cell Site to any residence that is within coverage and is available in both Urban and Rural environments.

Fixed wireless service is used as a component of the RBI (Rural Broadband Initiative) to deliver services to customers where the installation of fibre to their premises was considered too expensive.

Mobile Access Networks

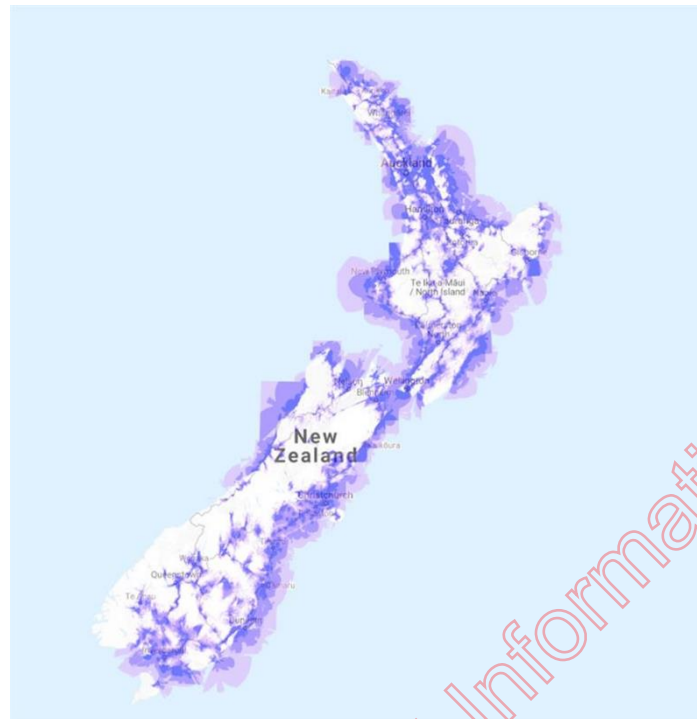
Cellular networks

Spark, Vodafone and 2degrees, and RCG operate Cellular radio networks in New Zealand. The general principle of their operation is one of radio coverage "cells" that integrate to form a coverage zone.

The Cell Site provides the local coverage, and a mobile handset will connect to the cell site with the strongest signal, usually, but not always the nearest cell site.

The figure below shows typical cellular service coverage throughout New Zealand

Figure 7: Typical Cellular Service Coverage



Transmission links connect the local Cell site to an aggregation node and then enters the Core Transport network to be transported to the Cellular service provider’s IMS (IP Multimedia Subsystem). The IMS hosts the mobile switching exchange function that connects the calling mobile handset to the requested service – telephony or data.

In addition, the IMS (or Cellular exchange) function is georedundant and each Cellular network operator has at least two IMS nodes distributed amongst the main centres. The IMS also integrates the mobile operator’s fixed wireless access services.

Individual cell sites cannot operate independently of the IMS, that is to say that they are unable to provide stand-alone local service if the Fibre or Radio link to the Cell site is broken. Connectivity into the IMS environment via the core transport platform is essential for all services to operate.

The principal cellular technologies delivery throughout NZ are 3G, 4G (3rd and 4th Generation) and recently 5G has begun to make its appearance sporadically in some main centres. Each advance of generation is able to provide – in addition to voice – greater data speeds and lower latency. The topology for 5G requires a higher density of cell sites to provide the same geographical coverage area

Digital Mobile Radio (DMR) land mobile networks (Vital)

Vital (ex Teamtalk) is the major provider of analogue and digital mobile radio in the country (used for handheld VHF and UHF communication devices) and in addition to their commercial user, base provides services to a number of lifeline utilities and emergency services in the region including Ambulance Services and CDEM communities.

Vital’s land mobile radio networks are interconnected by a combination of Fibre and their own National Digital Microwave radio network. This provides a level of resilience during national

disasters as the service is not reliant on underground fibre networks and reticulated power. Many Vital sites are built for customers to operate for up to 72 hours without power/fuel top ups and key sites are interconnected by dual microwave radio installations for robustness.

Radio based Transport Networks (Kordia)

Kordia owns and manages the broadcasting network in New Zealand, which includes FM radio.

Kordia has invested significantly in resiliency by way of geographical and technological diversity (Fibre and Radio) into their sites and centres. Kordia's sites, network and power backup systems are provisioned to a high level of robustness and the infrastructure is dimensioned to match the role of a specific installation especially high sites such as those that house the high elevation Digital Microwave repeater sites.

s 9(2)(b)(ii) [Redacted]

International Networks

Submarine cable providers

New Zealand is served by three submarine cable operators that land five individual cable ends in the upper North Island. These provide service to numerous international points of presence located predominantly in Australia and the USA. The more recently installed cables (s 9(2)(b)(ii) [Redacted])

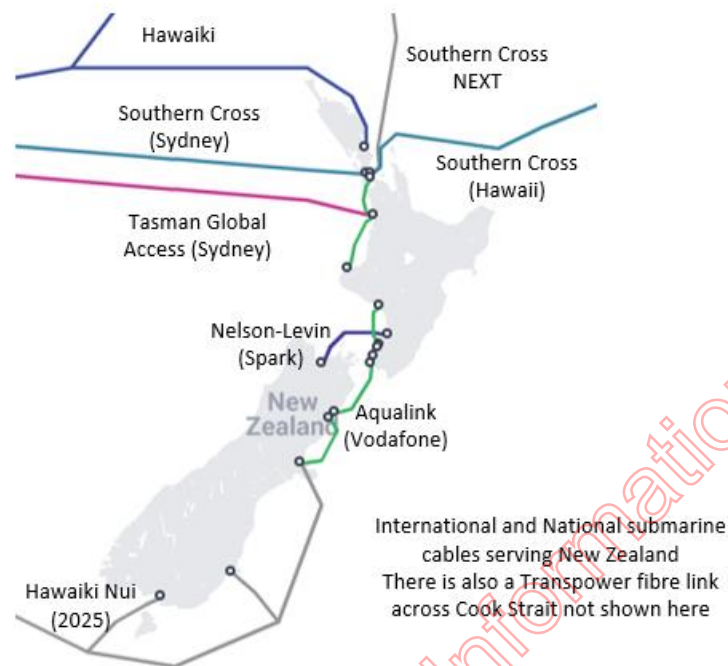
[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

Released under the Official Information Act 1982

Figure 8: International and National Submarine Cables



Satellite Networks

Geostationary satellite with fixed satellite earth installations

There remain very few services from New Zealand being delivered by this means. The remaining Satellite Earth Station (SES) is located at Warkworth and owned by Spark International.

The permanent services still delivered by this installation to New Zealand interests are -

1. **Chatham Islands** – principally to provide backhaul for the Island’s NEAX POTS telephone exchange. The island’s telecommunications, upgraded as part of the RCG and RBI – 2 programme providing satellite derived island wide 4G Cellular coverage from 5 Cell sites.
2. **Scott Base Antarctica** – a satellite Earth station positioned at Arrival Heights feeds a limited digital capacity to Antarctica NZ’s Scott Base via a 4KM surface laid fibre link. Due to Scott Base’s proximity to the USA McMurdo base – their fallback option is to utilise their satellite capacity – and vice versa.
3. **Pacific Island nations** - a number of Pacific Island destinations.

Satellite for the provision of consumer Internet

This section has been included to indicate that satellite-based services are available to provide services that support terrestrial telecommunication in New Zealand. Satellite services can either be a customer’s main connectivity with the rest of the world (as in the case of a remote rural environment), or it can be installed as a backup to protect their normal terrestrial services.



There are increasing options for New Zealand customers to connect to satellite systems that promise consistently fast internet and include a corresponding array of retail service providers that sell these services. Some satellite operators are -

Globalstar

Globalstar is LEO (Low Earth Orbit) satellite system that uses 48 satellites in six polar orbits with each orbit hosting eight satellites. The orbits are located at an altitude of almost 1400km.

Starlink

Another service that uses multiple “shells” of LEO satellites, Starlink enables video calls, online gaming, streaming, and other high data rate activities that historically have not been possible with satellite internet. Users can expect to see download speeds between 100 Mb/s and 200 Mb/s and latency as low as 20ms in most locations.

Kacific

Kacific Broadband Satellites Group (Kacific) is a satellite operator providing a high-speed broadband internet service for the South East Asia and Pacific Islands regions. It is a Ka-band HTS (High Throughput Satellite) satellite. This service is derived from a geostationary satellite, achieves up to 30Mb/s but has a high latency as a consequence of being geostationary.

OneWeb

This is another LEO service that has a New Zealand footprint. This service is capable of delivering 400Mb/s Internet download speeds with a latency of 32ms.

Other satellite communication providers that have New Zealand service footprints include Inmarsat, Iridium, Intelsat and Global Express. Apart from Global Express, these systems generally use frequency bands that do not deliver high speed Internet access.

APPENDIX D: Resiliency Properties of the Networks

Core Transport Networks

All Core Network operators configure their networks to have dynamic self-healing properties. If you consider a mesh or ladder network, then the failure of any single route or rung of the ladder will usually not impact the traffic carried by that operator as it automatically switches to a redundant available path. In most cases for a single route failure, it's possible to fully restore services “round the other way” even if those services take a longer route than they are normally programmed to take.

The figure below shows the geographical disposition of a typical “Core Transport” network showing the geographically diverse routes that contribute to its robustness.

s 9(2)(b)(ii)



UFB Network

Physical streetside UFB Fibre delivery

A buried optical fibre cable is inherently more robust physically than its copper counterpart. In the case of UFB, either the fibre bundle or sheath containing the air-blown Micro-ducts is made of HDPE (High Density Poly-Ethylene).

UFB networks also consist of aerial networks, where fibre cable is suspended on (for example) power poles. Aerial fibre is rated for different conditions than ducted fibre, taking into account the different exposure conditions that apply. Although ducted fibre is typically more resilient to, for example, earthquakes, aerial fibre is easier to access and repair (reducing reinstatement times).

Optical fibre is also immune to the electrical interference and induction that was always an issue to be managed with Copper cable reticulation as cables that accumulated moisture due to sheath cracks and nicks were susceptible to inducing noise into the individual cable pairs. This impacted the customer's service performance – especially that of high-speed DSL services.

By comparison to a copper network, the UFB network and its associated blown fibre units are immune to the effects of water.

One of the best features of the UFB service delivery is that, as opposed to the FTTN (Fibre to the Node) which delivered a fibre connection into an electronically active cabinet (needing a mains power feed), the majority of the UFB network between the Central Office and the customer's premises is entirely a passive optical fibre. The only intervening cabinet or fibre flexibility point that may be part of the service delivery is an optical splitter which is also passive.

There are areas in New Zealand that are fed using a single buried fibre high speed digital link. Those communities are found mainly at the periphery of the network where the difficulty and cost of providing a diverse fibre link was / is prohibitive.

Cellular Fixed Wireless

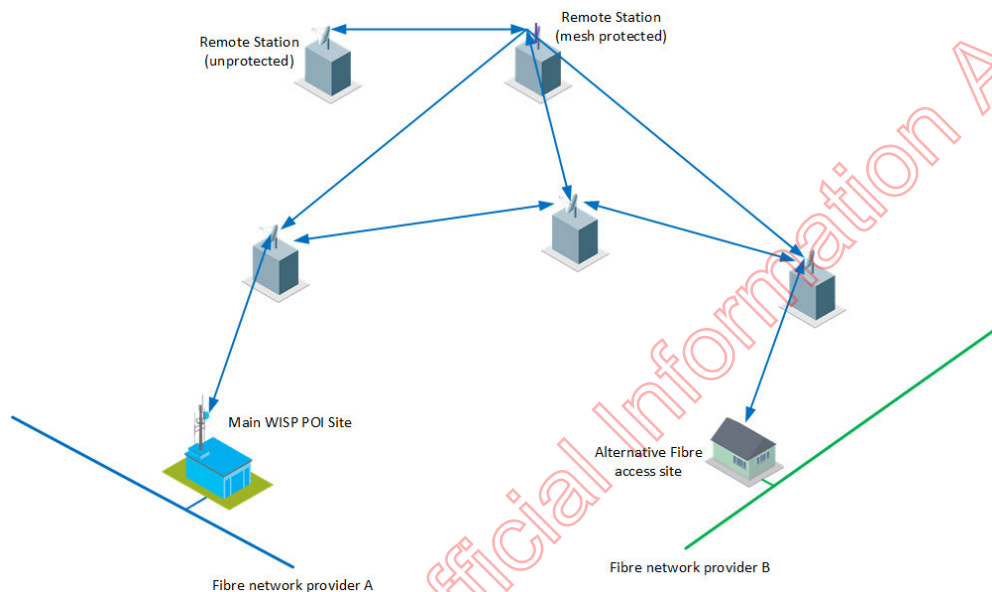
Cellular derived fixed wireless services have a similar or slightly better reliability than mobile services delivered from the same cell site(s), because the fixed services use a different network platform – and greater reliability because of physically static equipment. Reliability of the radio link component (such as may be encountered in some rural situations) can be improved by the addition of an external antenna on the premises.

Due to the service using shared radio linking frequencies and the technology employed at the cell site, there may be some service level reduction (Internet connection speed) during busy times of the day, usually in the evening, where multiple users are connected to the same cell site.

WISP network

The diagram below shows a typical layout of a WISP network having mesh diversity in between remote sites. Also shown is an additional diversity option using a remote fibre connected premises to complete a ring diverse path back to the main WIPS POI site.

Figure 10: Typical Layout of WISP Network



Networks

Although smaller WISP networks may be comprised of single interconnecting radio hops to remote stations, WISPs with large networks (such as Amirunet) have hilltop nodes with radio path visibility of each other and are provisioned with meshed connectivity. In addition, that connectivity can be bolstered if one of the remote stations is near to a local fibre network – allowing the signal to have a diverse path back to a POI using a normal UFB or other fibre delivered service.

Sites and infrastructure

WISPs, depending on the scale of their operation, generally align with the resilience principles that apply to the rest of the telecommunication industry. Given that their remote stations are usually mounted on the top of hills away from commercial power supplies, most of these are solar powered and are provisioned minimally with generous battery backup (days) and if the site is a key node in their network, may have an engine alternator as well.

Cellular Mobile

For 111 calling, if there is no coverage by a customer's chosen cellular operator, then either of the two other company's cellular service will allow the call to be made to emergency services.

In addition to each cellular installation being provisioned with battery backup, typically between four and 20 hours depending on their location and priority, they may also have either a permanently installed generator or the ability to connect to a rapidly deployed generator.

Cellular operators have (or have access to) sufficient portable generation resources to support a limited number of battery-only sites if there is an extended commercial mains outage. During a widespread telecommunication outage, the restoration of mobile services becomes a priority as it restores widespread service delivery of a service that is predominantly accessed by battery powered handsets and other cellular connected devices.

In recent times – and especially with the advent of new 5G networks and the attendant negative press that is currently circulating – there have been instances of random vandalism of cellular installations. This has included the felling of stayed masts (such as those found in rural areas) and the use of fire in attempts to damage the sites. All cell site installations are inherently physically robust so there's not a lot that the operators can do better – unless the incidence of vandalism escalates – generally or at a specific site – the sites are restored to their original state.

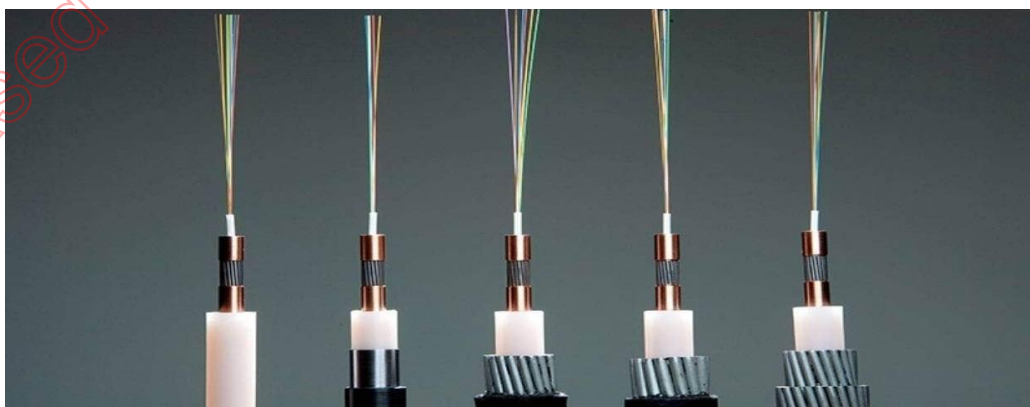
Submarine cables and shore based terminal stations

Cable stations

Following international guidelines, these stations are built to a standard that reflects the importance of the services they provide. Generally, a bunker style of building located away from the public eye and protected by electrified fences and monitored by security cameras. The stations are furnished with battery backup and standby power generators that have several days of run-time before fuel needs to be replenished. Cable stations are located well above any potential inundation zones and have a high level of seismic hardness.

Cables

Reflecting the importance of the services carried and the presence of high voltages (10KV in the case of Southern Cross NEXT) the cables are heavily armoured where they traverse overland and the seaward side to a depth of approximately 1500 metres when in proximity to the shore. The ocean sectors of the cable need less armouring due to the depths encountered but special measures are taken when the cable unavoidably needs to traverse areas of the sea bed that presents greater risk to the cable (including cable crossings of other submarine operators).



Protecting the land-based network (the dry network)

In the case of the Southern Cross and TGA cables, the overland sections are located in populated areas and special measures are taken to protect the cable asset. These include a regular cable survey by driving the route to confirm that there is no civil construction activity occurring near the cable. In addition, the routes are well marked identifying this specific asset and any cable location (to allow civil works near the cable) and works stand-over is provided free of charge.

Protecting the submerged network (the wet network)

Submarine cable network operators have formed a close association with the NZ Fishing industry to bring their attention to the location and criticality of the submerged asset. Although, in proximity to the shore the cable is buried under the sea bed to about one metre, it can be easily damaged both by large vessels' anchors and sea bed trawling. In the Waitemata harbour, regular patrols of the exclusion zones by the Auckland Harbour Board assist with enforcement of protecting the submerged asset.

Satellite services

While satellite-based services are an excellent alternative delivery method especially for those customers that are unable to connect to land-based services, they do have radio propagation issues (signal fading) during times of high rainfall and heavy cloud cover.

Higher speed services use radio frequencies that are higher on the spectrum, but this is more affected by signal fade.

Lower speed services are available, and are less prone to signal fade, but their data speeds are lower.

High speed satellite services are a useful adjunct to those services being delivered over terrestrial networks and can serve those customers who are removed from the existing networks. There are limitations to the quality of the services but for those users who are in remote parts of the country, they may provide exactly the solution that suits their needs.

APPENDIX E: The TCF

The New Zealand Telecommunications Forum (known as the TCF) sets standards and specifications for the way members interact on industry-wide issues, such as facilitating customer switching, blocking scam callers, marketing of broadband services and provides an independent disputes resolution service for the sector.

The TCF interacts, on behalf of the sector, with a wide range of government agencies, Commerce Commission and consumer focussed organisations.

TCF member companies represent over 95% of New Zealand telecommunications customers. The TCF actively fosters co-operation and collaboration amongst the telecommunications industry across regulatory, technical and policy issues in order to get the best outcomes for consumers of telecommunications services. It provides an environment in which its members can create practical, efficient solutions to issues, develop industry self-regulatory codes and educate consumers.

For more information visit our website: www.tcf.org.nz

Members



Released under the Official Information Act 1982

Annex Three: Response from Chorus

Released under the Official Information Act 1982

Hon David Clark
Minister for the Digital Economy and Communications
Executive Wing
Parliament Buildings
WELLINGTON 6011

22 December 2021

Dear Minister

Thank you for your letter of 11 November requesting information about the resilience of Chorus' telecommunications network. Our response focuses on Chorus' specific risk and resilience considerations as a wholesale network operator subject to utility-style regulation. We understand that the TCF will coordinate a response on sector cooperation to support resilience and event preparedness in the new year which we will also participate in.

Managing risk to the network is a core part of our business and our goal of providing a congestion-free network. However, it is worth noting that we only operate the layer 1 and layer 2 aspects of the network, and as such, service interruption can still occur due to issues arising at the layer 3 (RSP) level – for example cybercrime.

Our network architecture agreed with the Crown is designed to limit the impact of a service outage by providing resilience should a single element fail. The greater the customer numbers impacted, the more elements are duplicated, i.e. the core network carrying tens of thousands of connections must be more available than a cabinet or small exchange with two or three hundred connections.

Growing our network's resilience beyond what was agreed with the Crown will be a consideration under the new regulatory regime consultation process which would also add cost to connectivity. While under the new regulatory regime we have the ability to recover costs of this nature over time, the Commerce Commission must approve expenditure allowances for this, partly based on consumer demand and a cost benefit analysis. Our experience is that even where we have resilience and redundancy, our customers still may choose not to take the additional services due to the increased cost.

The geographic challenges of our country create resilience challenges that are costly to overcome as they do not often meet commercial investment thresholds. Where proposals are developed for increased physical resilience these may require government funding, as was the case with the West Coast link due for completion early next year.

Fibre expansion will also improve resilience more generally. Modern fibre networks have a different resiliency profile to that of our much older copper networks in rural New Zealand. Addressing the digital divide would likely improve New Zealand's wider resilience in terms of individuals being able to access connectivity. We have engaged with your officials on how the fibre footprint could continue to be expanded over time.

Under the new fibre regulatory framework we are required to produce expenditure proposals for the Commerce Commission to approve. Although our first regulatory period¹ is just

¹ 1 January 2022 to 31 December 2024.

about to begin we are already starting work on our expenditure proposal for the second regulatory period. We have begun our engagement with key stakeholders and end-users on the proposal. As part of this we will be seeking views about their expectations for resilience and this feedback will support our expenditure proposal to the Commerce Commission. We will keep your officials updated on our progress and the impact on our resilience planning.

Yours sincerely



JB Rousselot
Chief Executive, Chorus Limited

Released under the Official Information Act 1982

COMMERCIAL IN CONFIDENCE

APPENDIX: CHORUS NETWORK RESILIENCE

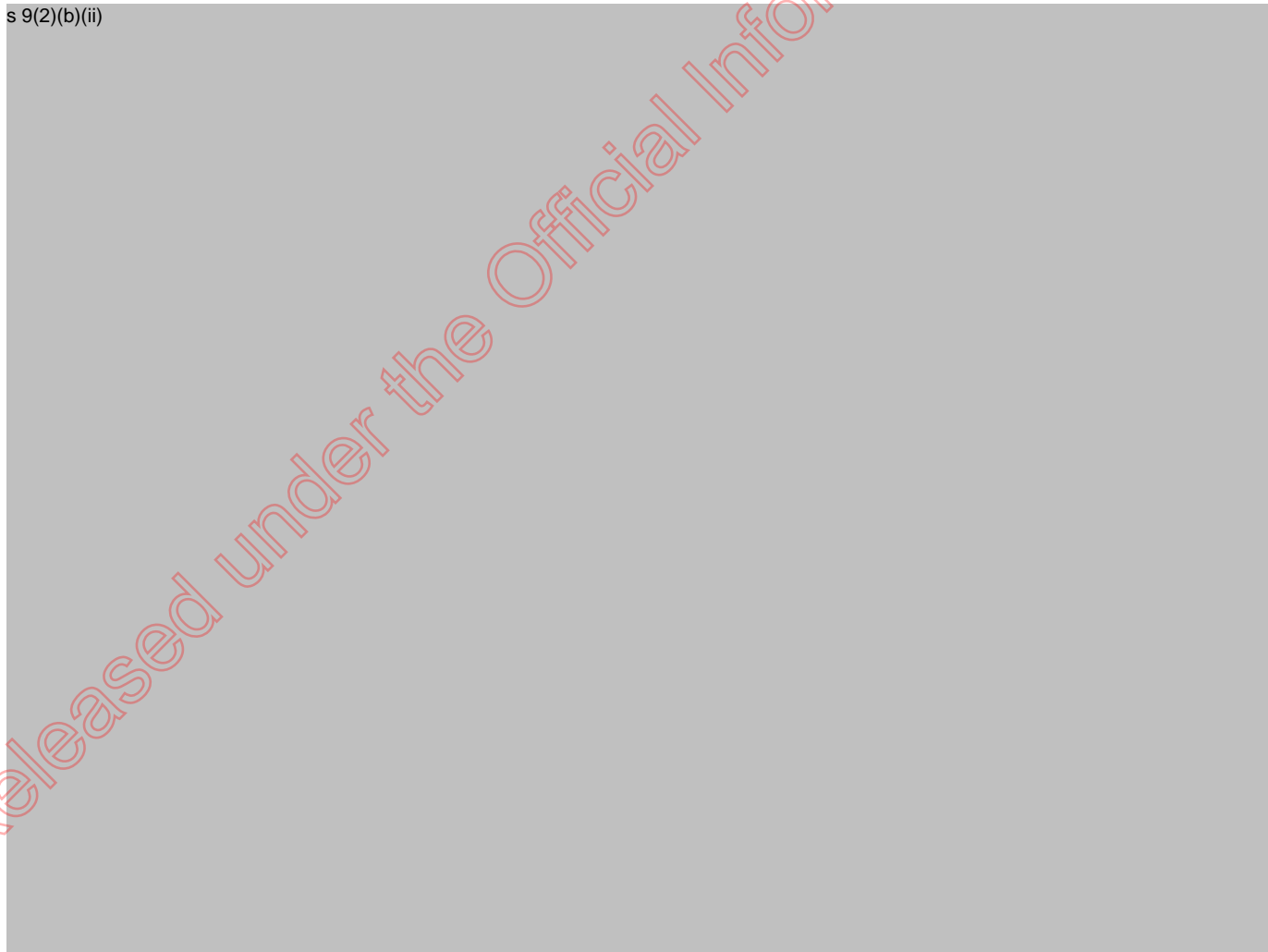
The information we are providing is both sensitive and commercial in confidence to Chorus. We are providing this information on the basis that it will be treated with appropriate controls around its security and the information provided will not be distributed further than necessary. We consider that the contents would be protected from disclosure under the Official Information Act 1982.

Our response contains material which, if disclosed, would be prejudicial to our commercial position including information that would assist our network competitors. It further contains information that, if disclosed, would be detrimental to network security. If you intend to disclose this information to any third party under the Official Information Act, we ask that you notify us so that we can consider our response and take any action as appropriate.

RESPONSES TO QUESTIONS:

- 1. What dominant risks, vulnerabilities, or system constraints you are aware of that could have an adverse impact on your network's ability to keep New Zealanders safe and connected following an event?**

s 9(2)(b)(ii)



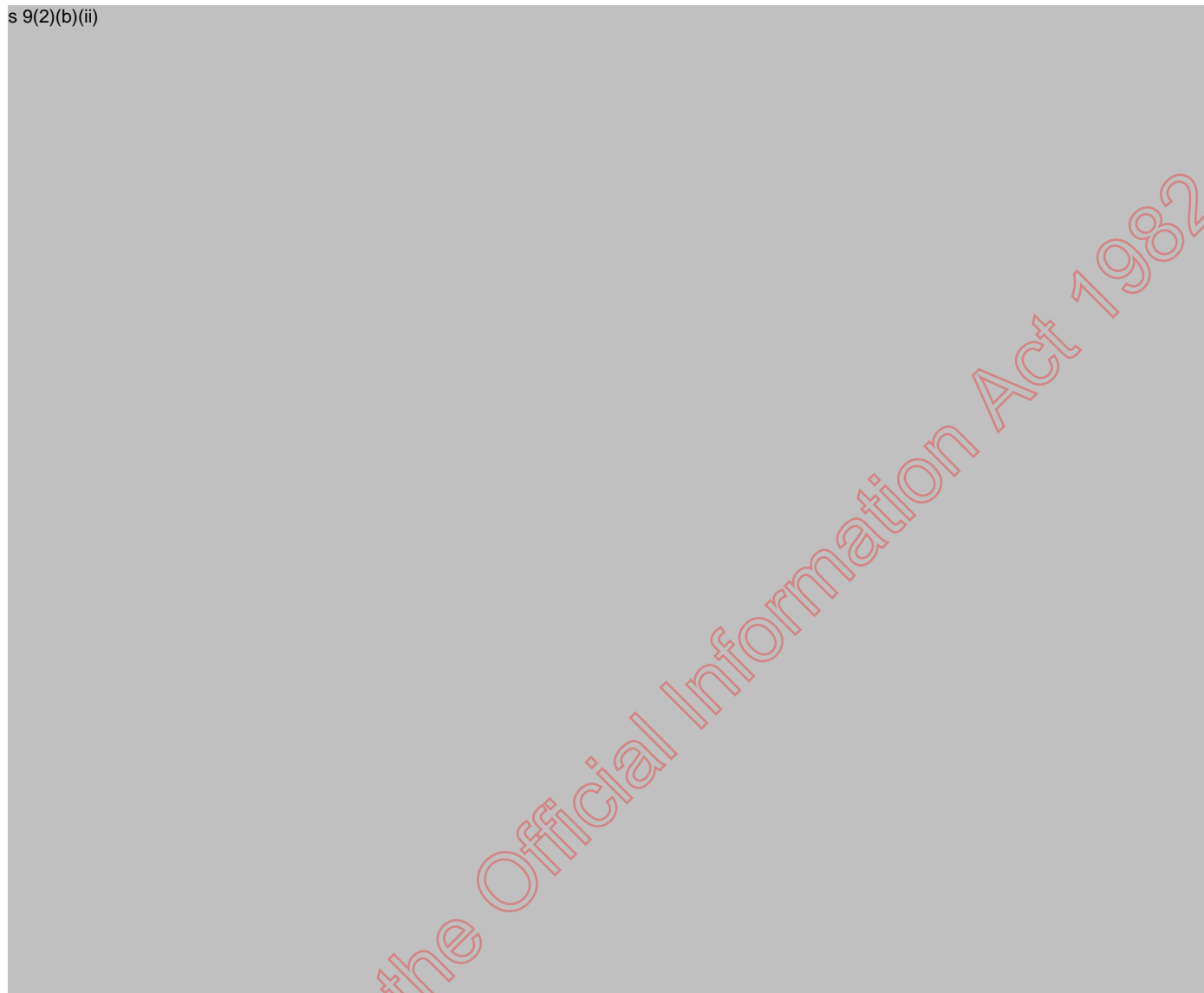
COMMERCIAL IN CONFIDENCE

s 9(2)(b)(ii)

Released under the Official Information Act 1982

COMMERCIAL IN CONFIDENCE

s 9(2)(b)(ii)



2. What dominant risks are Chorus' current network and service architectures designed to mitigate?

s 9(2)(b)(ii)



s 9(2)(b)(ii)

Released under the Official Information Act 1982

COMMERCIAL IN CONFIDENCE

s 9(2)(b)(ii)

3. How Chorus assesses vulnerabilities in its network, including the risks of natural hazards and anticipated climate change impacts?

s 9(2)(b)(ii)

4. How these risk assessments influence Chorus' consideration of investments in new infrastructure, and which risks your planning excludes?

s 9(2)(b)(ii)

COMMERCIAL IN CONFIDENCE

Released under the Official Information Act 1982

5. How Chorus works with relevant authorities, telecommunications, and other companies (for example electricity companies) to mitigate risks and how these relationships could be enhanced?

Operationally, Chorus is a member of the Telecommunications Emergency Forum which collaborates and coordinates activities between network operators and other agencies and organisations (e.g., Civil Defence, the Lifeline Utility Coordinator) in the case of significant service impacting events.

Prior events including the Christchurch and Kaikoura earthquakes showed the high levels of cooperation within the industry when working to restore services. We understand the TCF response to your letter will address sector-wide event response in more detail.

Our framework for contingency planning and disaster recovery leverages the TEF and includes initial response plans, business continuity plans, technology continuity plans, and disaster recovery plans.

6. What future plans Chorus has that will enhance the resilience of the network and services to particular natural hazard and other risks?

s 9(2)(b)(ii)



Released under the Official Information Act 1982

s 9(2)(b)(ii)

7. What Chorus views as the top 3 specific risks to its network based on frequency and severity criteria, and what plans are in place to address them?

s 9(2)(b)(ii)

8. What Chorus views as the top 3 overall system risks to supply consistency and how Chorus would identify they be best resolved?

s 9(2)(b)(ii)

s 9(2)(b)(ii)

9. Which populous locations are most at risk of service disruption, and what future plans, if any, do you have to improve resilience in these regions?

s 9(2)(b)(ii)

10. Are there any competition rules impeding planning for a more resilient network? If so, does Chorus have any suggestions for pragmatic change that government could lead in this regard?

s 9(2)(b)(ii)

COMMERCIAL IN CONFIDENCE

s 9(2)(b)(ii)

11. How does Chorus work with other security providers to prepare for cyber-attacks, and mitigate cybercrime?

s 9(2)(b)(ii)

12. How does Chorus prepare for and support its customers during denial-of-service attacks and other disruptive cyber incidents? In particular how do you ensure that your network and services can effectively mitigate disruptions in an evolving environment, in order to provide continuity of service?

s 9(2)(b)(ii)

Annex Four: Response from Vodafone

Released under the Official Information Act 1982



1 February 2022

Susan Hall
Manager, Communications Policy
Ministry of Business, Innovation and Employment
15 Stout Street
Wellington

By email: Susan.Hall@mbie.govt.nz

Re: Resilience of Vodafone's telecommunications network

Dear Susan,

I refer to Minister David Clark's letter sent on 11 November 2021 to Jason Paris, CEO of Vodafone New Zealand, regarding the resilience of Vodafone's telecommunications network.

This letter addresses the key broader themes and issues recently discussed with MBIE officials in regard to telecommunications network resilience. In addition, the annex below provides details relating to the specific questions raised in the Minister's letter. We encourage the Government to consider this information, together with information provided by other operators and the Telecommunications Carriers Forum (TCF), when making any policy decisions relating to telecommunications resilience. We will continue to engage with MBIE on these matters.

Distinction between jeopardy and failure

As acknowledged in the Minister's letter, the telecommunications industry has a demonstrable track record of working together in response to natural disasters and emergencies. This was most recently demonstrated by networks remaining resilient in light of multiple floods in the Canterbury and West Coast regions, and the rapid increase in data usage during Covid-19 lockdowns.

When it comes to incidents affecting specific network assets (e.g cell sites, fibre routes), it is important to distinguish between jeopardy and failure. Our network is built in a way that gives us at least double redundancy across the whole country (with increased redundancy in some areas). This means that any one or two elements of the network can fail without impacting overall resilience, because of the way that the network is designed. If a network asset stops working for any reason, it puts the network at jeopardy, but it doesn't necessarily mean the loss of service for customers, as other network assets can be redeployed to provide coverage. For example, we have multiple fibre routes between main centres (see *Figure 1*). If one route is cut, the network is in jeopardy. If two are cut, the network is still in jeopardy, but not at fault as service continues to be provided via alternative routes.

If all routes are cut, then the network fails, meaning a loss of service. Official classification of telecommunications in the highest category of critical infrastructure would help ensure we can access the affected sites and restore connectivity as soon as possible in such cases – particularly where the issue arises from a declared emergency, which currently results in restrictions on the ability of Vodafone and contractors to access affected areas. Situations where the network is in jeopardy are common and unavoidable. However, the network is designed to manage such situations to prevent failure and ensure continued access to services for customers.



s 9(2)(b)(ii)



Released under the Official Information Act 1982



Distinction between network and service resilience

Another distinction that is important to be mindful of is the difference between network and service resilience.

The network layer includes physical infrastructure that provides connectivity to customers, such as cell towers and fibre links. As outlined above, all of these elements can fail and if they do, that is considered a network failure (i.e. one that telecommunications network providers are in control of resolving in most cases).

Meanwhile, the service layer includes third party network elements, such as a Microsoft data centre in Auckland and Netflix data centre in Sydney. These elements can fail for any variety of reasons and have an impact on customers.

Failures in places like data centres, which customers are increasingly dependent on, are not elements that telecommunications network providers control, and we are not in a position to control the restoration of failures in these environments. However, these service elements are becoming increasingly integrated with our network, and the ability for customers to differentiate between network and service failures is becoming increasingly difficult. In other words, network operators like Vodafone are frequently seen as responsible by our customers for service elements that we don't provide or control.

Dependencies on other infrastructure

Our network and services are only as resilient as other services that support them (e.g. electricity networks). Vodafone experiences on average 3 power incidents every day, while 60% of all incidents in the 2020/21 financial year were caused by power failures. Furthermore in a case of major disasters, the telecommunications network resiliency becomes even more vulnerable to external dependencies, including power supply. In other words, telecommunications network resiliency often goes hand in hand with the resiliency of other infrastructure.

For example, Vodafone has two links between North Island and South Island, as well as additional capacity provided by the Spark/Chorus cables located a significant distance away from Vodafone's cables (see *Figure 2*), meaning that if an event such as an Alpine fault rupture were to occur, we would be able to continue providing full internet connectivity to the South Island. This is an example of how redundant parts of our network are designed to be geographically diverse, providing a decent level of resilience.

s 9(2)(b)(ii)





In comparison, the electricity network only has one link across the Cook Strait, making it a single point of failure. Given the importance of power supply for the availability of telecommunications services, including for New Zealanders' ability to connect to these services in their homes, the lack of resilience in this respect is concerning.

More broadly, information sharing is key for ensuring that telecommunications network providers can collaborate effectively with other infrastructure providers (i.e. power, roads, rail). However, the records of national infrastructure networks tend to be of poor quality. One way to enhance the relationship between telecommunications and other infrastructure providers would be to mandate the sharing of information to help ensure we have access to the most up to date records for planning purposes. Improving the quality of infrastructure location information in planning records is also likely to assist in reducing causes of many outages, e.g. cable breaks where construction activity occurs and affects cables that are located elsewhere than where is recorded.

Chorus resilience products

During a meeting with MBIE officials in December 2021, it was expressed that it would be helpful to understand whether Vodafone makes use of resilience products offered by Chorus.

s 9(2)(b)(ii)

Mission critical communications

Enabling resilient networks is central to work currently underway in Vodafone to enable high availability, mission critical communications for emergency services. s 9(2)(b)(ii)

Potential choke points in telecommunications infrastructure

Needless to say, maintaining resilient networks is key for Vodafone's business and this is an important consideration when investment decisions are made. However, investment in resilience needs to be balanced with the acceptable level of risk we are willing to take in specific locations. This is determined, among other factors, by the existing level of resilience, as well as the likelihood and impact of an incident occurring that would present a significant risk to resilience.

While past experience shows that telecommunications networks across New Zealand are resilient as a whole, there are a couple of locations that could benefit from additional investment. Once such area is Bombay Hills. Due to the narrow land in the area, there are a few pinch points coming into South of Auckland (see *Figure 1*). All telecommunications operators go through this corridor and while there are separation abilities, the separation is relatively minimal.

One solution would be to extend Aqualink (see *Figure 2*) into Auckland, landing near Glenbrook, which would give another alternative connection into the city. However, it is not commercially viable for industry to fund this alone due to the relatively low risk level in the area, and government support would be needed if an alternative link is desired.

We expect the TCF's report to provide further details on potential opportunities for enhancing resilience and our response to major events across telecommunications infrastructure as a whole.



I hope this provides a useful overview of Vodafone's network resilience and how we assess and plan for resilience risks. As expressed in our previous conversations, any future Government strategy on telecommunications resilience needs to be mindful of avoiding incorporating costly features or refinements into something unnecessarily. Desire for investment in resilience in parts of the country that are not economically viable for the industry also need to be weighed up against other priorities of MBIE's Future of Connectivity strategy, such as the rollout of 5G and improving rural connectivity.

Confidentiality

Confidentiality is sought in respect of the information provided in this letter. 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 Vodafone; and
- b. disclosure of the Confidential Information would be likely to prejudice unreasonably the commercial position of Vodafone.

We ask that MBIE 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 MBIE seek and consider its views as to whether the Confidential Information remains confidential and commercially sensitive before it responds to such requests.

Please get in touch if you require any further information. We would be happy to provide further detail on specific aspects addressed in this letter in writing or by setting up a call with relevant people in the business.

Kind regards,

A handwritten signature in blue ink, appearing to read 'T. Thursby', is located below the 'Kind regards,' text.

Tom Thursby
Head of Legal and Regulatory
Vodafone New Zealand Limited



Annex

Current resilience landscape and improving the status quo

	MBIE question	Vodafone response
1.	What dominant risks, vulnerabilities, or system constraints you are aware of that could have an adverse impact on your network's ability to keep New Zealanders safe and connected following an event?	<ul style="list-style-type: none"> • s 9(2)(b)(ii) • [Redacted] • Natural disasters (e.g. flood, fire, civil disturbance, tsunami, earthquake, eruption, extreme weather) • Impacts of Covid-19. For example, reduced ability to repair parts of the network due to lockdown restrictions (not everything can be done remotely), increased costs of network components due to Covid impact on supply chains, and reduced ability to access critical labour resources due to border restrictions. The cumulative impact of the pandemic affects areas like network investment and network loading.
2.	What dominant risks Vodafone's current network and service architectures are designed to mitigate?	All of the above
3.	How Vodafone assesses vulnerabilities in its network, including the risks of natural hazards and anticipated climate change impacts?	s 9(2)(b) ii
4.	How these risk assessments influence Vodafone's consideration of investments in new infrastructure, and which risks your planning excludes?	

Released under the Official Information Act 1982



		s 9(2)(b)(ii)
5.	How Vodafone works with relevant authorities, telecommunications or other companies (for example electricity companies) to mitigate risks, and how these relationships could be enhanced?	<p>The telecommunications industry has an excellent track record of working collaboratively in emergencies and we will continue to do so. We work with the following stakeholders on an ongoing basis:</p> <ul style="list-style-type: none">• Lifelines (Local Authority level) – we are active participants.• NEMA – we participate in event of incidents.• Relevant TCF groups – we are active participants (formal process for engaging with industry).• Ad hoc collaboration with other telecommunications providers (backdoor/informal process for engaging with industry). <p>Overall, the telecommunications industry does well to respond to events through collaboration. However, there may be more that could be done at an industry level around proactive preparation and protocols being in place in advance of emergencies. Documenting</p>

Released under the Official Information Act 1982



		<p>these processes may be useful for providing a high level of assurance around industry's responsiveness. The TCF is carrying out a separate piece of work on industry-wide resilience and we expect will look at how industry collaboration could be improved.</p>
<p>6.</p>	<p>What future plans Vodafone has that will enhance the resilience of the network and services to particular natural hazard and other risks?</p>	<ul style="list-style-type: none"> • Ongoing and continual awareness and re-evaluation of potential threats • Geo-redundancy <ul style="list-style-type: none"> ○ Having redundant (backup) equipment doesn't protect against failures that affect an area, such as having a server room burn down. We architect for geo-redundancy, to minimise the effect of a single server, building or link failure. ○ While failure of parts of the network is inevitable, our overall network is designed to survive the loss of any one of the following: link, switch, server, site, city. The principle is that any element - server, application, router, switch or link—can fail, and the Vodafone Core Network will correct for this failure. ○ The network is designed taking into account the consequences of such failure. That means, for instance, not siting two switches in the same machine room where the same set of fire sprinklers can take them both out. ○ We plan for failure by: i) understanding and documenting the likely failure mechanisms; ii) designing the network to survive failure; and iii) minimising the size of failure domains. ○ Redundancy is guided by the following principles: i) since anything can fail, all critical infrastructure requires at least one backup element; ii) since any element can fail, there must be a backup element; and iii) since any link can fail, there must be an alternative link. ○ Geographic redundancy: since some events, such as a fire, flood or earthquake, can affect a large area, critical infrastructure must not be confined to a single city. <p>s 9(2)(b)(ii)</p>

Released under the Official Information Act 1982



		s 9(2)(b)(ii)
--	--	---------------

Information to better inform the government’s understanding on any systemic issues

	MBIE question	Vodafone response
7.	What Vodafone views as the top 3 specific risks to its network based on frequency and severity criteria, and what plans are in place to address them?	<p><u>Top 3 specific risks:</u></p> <div style="background-color: #cccccc; padding: 5px;">s 9(2)(b)(ii)</div> <p>Natural disasters (including Covid-19)</p> <ul style="list-style-type: none"> We expect the number and extensiveness of natural disasters to increase due to climate change. <p>Power supply</p> <ul style="list-style-type: none"> 60% of all incidents in the 2020/21 financial year were caused by power failures. We experience on average 3 power incidents every day. These statistics highlight the extent of our dependency on power grids. Furthermore, in a case of major disasters, the telecommunications network resiliency becomes vulnerable to external dependencies, including availability of power for cell sites, access and POP sites. Cook Strait is a single point of failure for electricity

Released under the Official Information Act 1982



		<p>networks. Customers are also dependent on power supply in their premises – all modern communications equipment rely on constant availability of electricity. Other dependencies include road access to network equipment and availability of fuel for back-up power generation.</p> <p><u>Plans to address them:</u></p> <p>s 9(2)(b)(ii)</p> <p>Power supply</p> <ul style="list-style-type: none">• We have our own power generators and our own supply of diesel, which means that we can deal with power outages at some sites. However, we are dependent on NEMA in terms of our ability to deploy generators and diesel to affected sites.• Meanwhile, we are taking actions to reduce the number of impacting power incidents with investment in longer battery reserves and operational processes to trigger generator deployments as necessary. <p>Natural disasters (including Covid-19)</p> <ul style="list-style-type: none">• Focus in this area is on post-event risk planning (as outlined in more detail above in response to Q3). The industry's efforts currently tend to focus on preparedness to respond to a situation by having resources (such as cell sites on wheels) available at short notice, which has to date been an effective approach.• It is difficult to plan ahead for different eventualities when it comes to natural disasters. It is also important to remember that, in the majority of cases, natural disasters affect a limited area of the country at any one time. Our networks are designed to cope with such cases. For example, while the loss of one or a number of cell sites due to an earthquake would put the network at jeopardy, it would not necessarily mean the entire network fails, as we may have alternative cell sites that can provide coverage in the affected areas. Close co-operation between all network operators in emergency events also provide for additional resilience.
--	--	--

Released under the Official Information Act 1982



8.	What Vodafone views as the top 3 overall system risks to supply consistency, and how Vodafone would identify they be best resolved?	s 9(2)(b)(ii)
		Natural disasters, force majeure <ul style="list-style-type: none">• Focus in this area is on post-event risk planning, which is the best use of the industry's resources. As outlined in response to questions above, natural disasters tend to be localised events and our networks are designed to ensure that we have one or more alternative links to maintain connectivity.
		s 9(2)(b)(ii)
9.	Which populous locations are most at risk of service disruption, and what future plans, if any, do you have to improve resilience in these regions?	All main cities are roughly equally vulnerable. Everything south of the central plateau is at risk of earthquakes. Everything north (and the plateau itself) is at risk of volcanoes (with an essentially identical actuarial risk). All cities except Palmerston North and Hamilton are ports and at risk from tsunamis and climate change. Hamilton and Palmerston North are situated

Released under the Official Information Act 1982



		<p>on rivers and at risk from flooding and climate change. All parts of NZ are subject to extreme weather.</p> <p>However, it is important to remember that natural disaster events affect a limited area of the country at any one time, and our networks have always been designed to cope with such eventualities. We take great care not to place all of our infrastructure in one place and make certain that we have both North Island and South Island covered (we have two links between North and South Island, plus additional capacity). Our network is built in a way that gives us double redundancy across the whole country. Any one or two elements of the network can fail without impacting resilience, because of the way that the network is designed.</p>
<p>10.</p>	<p>Are there any competition rules impeding planning for a more resilient network? If so, does Vodafone have any suggestions for pragmatic change that government could lead in this regard?</p>	<p>Competition analysis continues to assume potential for network-based competition between operators across areas of New Zealand. While this assumption remains correct in areas where there is sufficient population and usage density to support competitive investment, it does not hold true in areas with low density/usage where industry economics do not support overlapping and duplicative investment.</p> <p>In these areas resilience is better served by collaborative investment models that are likely to result in networks that are more highly specified to support colocation, resilience and mission critical communications. For example, collaborative investment models in these areas are more likely to result in more highly engineered sites with back-up power and failover options than sub-economic infrastructure deployed by a single operator. It would be helpful for competition rules to more explicitly recognise limits of network-based competition in certain areas of New Zealand.</p> <p>In terms of overall planning for resilience, competition rules are also likely to reduce scope for operators to coordinate on placement of network assets in those areas where they continue to compete at a network level. Competition rules will require operators to make independent decisions as to the placement and configuration of assets, without discussion and agreement between operators influencing these decisions. Irrespective of whether this actually enhances competition, the restrictions on coordination that are imposed mean operators are unable to take a coordinated approach on resilience issues when deciding on the investment and location of network assets.</p>

Released under the Official Information Act 1982



		As outlined in response to Q7, the most important dependency of telecommunications resilience is power. The quality of power distribution assets in rural areas is therefore material. The Commerce Commission has a key role in ensuring the quality of these power grids.
11.	How does Vodafone work with other security providers to prepare for cyber-attacks, and mitigate cybercrime?	s 9(2)(b)(ii)
12.	How does Vodafone prepare for and support its customers during denial of service attacks and other disruptive cyber incidents? In particular, how do you ensure that your network and services can effectively mitigate disruptions in an evolving environment, on order to provide continuity of service?	s 9(2)(b)(ii)

Released under the Official Information Act 1982



		s 9(2)(b)(ii)
--	--	---------------

Released under the Official Information Act 1982



BRIEFING

Telecommunications resilience during natural disasters

Date:	17 February 2023	Priority:	Medium
Security classification:	Restricted	Tracking number:	2223-2592

Action sought		
	Action sought	Deadline
Hon Ginny Andersen Minister for the Digital Economy and Communications	Discuss this briefing at your weekly meeting with officials on Monday 20 February 2023.	20 February 2023

Contact for telephone discussion (if required)				
Name	Position	Telephone		1st contact
Deborah Salter	Manager, Communications Policy	04 901 0786	s 9(2)(a)	
Christopher Moses	Senior Policy Advisor, Communications Policy	04 897 6386	N/A	✓

The following departments/agencies have been consulted

Minister's office to complete:

Approved

Declined

Noted

Needs change

Seen

Overtaken by Events

See Minister's Notes

Withdrawn

Comments

Released under the Official Information Act 1982



BRIEFING

Telecommunications resilience during natural disasters

Date:	17 February 2023	Priority:	Medium
Security classification:	Restricted	Tracking number:	2223-2592

Purpose

This briefing provides:

- background information about New Zealand telecommunications resilience
- an overview of significant programmes of work already underway across government to enhance the resilience of all critical infrastructure
- further levers that could be considered for specifically improving telecommunications resilience.

Executive summary

New Zealand's telecommunications infrastructure generally holds up well to natural hazard events. However, significant events such as Cyclone Gabrielle highlight vulnerabilities in the network, in particular the high level of interdependency with other critical infrastructure (e.g. energy and transport). These interdependencies make it important to address critical infrastructure vulnerabilities in a coordinated, cross-sector approach.

Telecommunications companies are privately owned and therefore are driven by commercial incentives. While companies do invest considerably in resilience, commercial drivers only go so far. In some cases, a higher level of resilience may involve government intervention through either regulatory changes or funding non-commercial investments.

In terms of regulatory intervention, there are three significant programmes of work across government already underway to enhance the resilience of critical infrastructure. These are:

- a comprehensive review of the emergency management system, including an Emergency Management Bill being considered by the House early this year (led by NEMA)
- a regulatory work programme on enhancing critical national infrastructure resilience, led by the Department of the Prime Minister and Cabinet (DPMC), s 9(2)(f)(iv)

- s 9(2)(f)(iv)

MBIE considers these work programmes are the most appropriate vehicle for driving regulatory changes to telecommunications resilience. s 9(2)(f)(iv)

s 9(2)(f)(iv)

Resilience is one of five key objectives to be delivered, and it is important to balance this with other objectives (e.g. expanding coverage or increasing network capacity).

s 9(2)(f)(iv)

Recommended action

The Ministry of Business, Innovation and Employment (MBIE) recommends that you:

- a **Discuss** this briefing with MBIE officials at your weekly meeting on Monday 20 February 2023.

Agree / Disagree



Deborah Salter
Manager, Communications Policy
Building, Resources and Markets, MBIE

17 / 02 / 2023

Hon Ginny Andersen
**Minister for the Digital Economy and
Communications**

..... / /

Background

1. New Zealand has world-leading telecommunications infrastructure, despite the challenges associated with our narrow and rugged geography. Our networks generally hold up well during natural disasters, and when service interruptions happen, they tend to be localised and short in duration due to the responsiveness of network operators.
2. However, significant, geographically widespread natural hazard events – such as Cyclone Gabrielle and the recent Auckland floods – highlight certain vulnerabilities in the network, in particular the high level of interdependency with other critical infrastructure such as energy and transport networks. These events raise the question of whether there is more the Government, and, in many cases, private owner-operators could do to enhance the resilience of the nation's critical infrastructure.
3. There are already significant government programmes of work underway that aim to enhance critical infrastructure resilience, including but not limited to telecommunications infrastructure. MBIE has been engaging with agencies leading those work programmes to provide input from a telecommunications perspective, and to ensure key risks are incorporated in the broader direction of travel.
4. In addition, there are levers available to the Government that would target specific telecommunications resilience improvements, which are canvassed in this briefing. MBIE recommends that these options should still be considered in parallel to resilience work underway in other critical infrastructure sectors to ensure any decisions make the best use of limited resources to target the most critical vulnerabilities, in turn maximising the benefits for people and communities across Aotearoa.

Resilience of telecommunications infrastructure and services in New Zealand: key issues and challenges

Networks comprising of key nodes and links provide the backbone of our communications infrastructure

5. Telecommunications services are delivered to end users in a number of ways, and the networks that transmit these communications are complex. At a high level, the core of a telecommunications network comprises of two general types of infrastructure:
 - a. central 'nodes' that control communications to and from the regions they serve (e.g. network control centres or telephone exchanges)
 - b. physical and wireless 'links' that connect nodes and transmit communications across the country (e.g. fibre, digital microwave radio or copper cables).
6. While both links and nodes are essential for a network function, loss of functionality at key nodes can often have more significant consequences for a network due to the number of connections that rely on service functions provided by these nodes. Links, while still essential for network functionality, can be duplicated or even triplicated to provide redundancy in the event of damage to one or more links in a given region.
7. In addition to the 'core network' features noted above, the way people access their connection varies as well. The 'access network' (the edge of the network that connects end users to the core network) is made up of either **fibre cables** (UFB network), **copper cables** (ADSL or VDSL broadband, or landline phone services), or **radio waves** emitted from, and received by, cell towers (e.g. fixed wireless broadband, or mobile cellular functions). In addition, the access network includes cell towers and roadside cabinets that aggregate data received from individual connections into a single 'backhaul' link to the core network.

8. Each part of the network can be affected by natural hazard or other damaging events in different ways, and therefore building resilience into the network requires a mix of approaches.

Service outages are caused by many factors, revealing complex interdependencies across critical infrastructures

9. There are many potential causes of a telecommunications service outage, though some of the most common include:
 - a. physical damage to network infrastructure (caused by natural hazards, human error or sabotage etc)
 - b. power outages (exchanges, cell towers, some roadside cabinets and end user broadband equipment all require power to operate)
 - c. software faults or cyber-attacks impacting a service provider, disrupting services provided by or reliant on that company but leaving other services and the physical network itself unharmed
 - d. end user equipment failure.
10. Notably, not all causes of service outages are under the control of telecommunications network operators or service providers. The resilience of telecommunications services is closely linked to the resilience of other critical infrastructure, such as electricity and transport networks. Damage to one often causes, or occurs simultaneously to, damage to another.
11. For example:
 - a. the cutting of electricity feeds to a key node, cabinet or cell tower can cause widespread telecommunications outages, even though there is nothing physically wrong with the telecommunications network itself
 - b. damage to transport infrastructure, in particular damage to roads, bridge washouts and landslides, can damage fibre and copper links that run alongside or across that infrastructure.
12. Interdependencies between telecommunications services and other critical infrastructure mean that decisions about resilience in any given critical infrastructure sector also have significant impacts on the resilience of other critical infrastructures.

Impact of service outages

13. The impact of telecommunications service outages varies on a case-by-case basis, depending on the scale, nature and geographic extent of the damage caused to the network and the commercial arrangements in place between service providers and network operators.
14. One of the trends in the way telecommunications services are delivered to end users is an increased centralisation of service control functions, resulting in fewer key nodes around the country. With older networking technology (such as copper landlines), people living in regions cut off from the rest of the network could still use their landlines to contact neighbours and others connected to the local telephone exchange (provided the local network remained intact). Today, most regional voice, mobile and broadband services will not work when key nodes are affected by natural hazards, or when links connecting the region to the centre of the network are cut.

15. This can be seen in the impact on services in Gisborne over the past few days, where both key fibre links into the region were cut and total service outages occurred across both mobile and fixed networks. This is shown in the map attached at **Annex One**, provided by Chorus on 16 February.

General approach to resilience in the telecommunications sector

16. Telecommunications network operators tend to frame discussions about resilience in terms of the rapidity of their emergency response (i.e. ability for operators to quickly spring into action once an event has occurred). They tend to take the view that the impact of natural disasters on their networks is almost impossible to accurately predict, and where clear vulnerabilities exist, they have appropriate measures in place to mitigate risks.
17. Some of the pre-emptive measures taken by telecommunications network operators include:
- building diverse links to ensure large numbers of customers are not reliant on a single point of failure (e.g. under the original UFB build contracts, Chorus's network had to have no single points of failure servicing more than 4,000 customers)
 - arrangements to ensure 111 calls can be made in areas where any mobile network operator has coverage (so if a Spark customer dials 111 while out of range of the Spark network, their call will still connect if they are in range of either the 2degrees or Vodafone network)
 - power generators and battery back-ups are provided at cell sites, roadside cabinets and exchanges in case of power outages.
18. Enhancing resilience must always be traded off against the benefits of other network investments, such as technological innovation (e.g. 5G, 6G etc) or expanded coverage (i.e. rural connectivity). Commercial drivers do not always incentivise network operators to invest in resilience, as consumers do not tend to be willing to pay the higher associated service costs given as they do not receive tangible benefits (until something goes wrong, by which time it is too late to build increased resilience).
19. This means that government intervention – through either regulatory changes or funding – may be required to increase resilience in the network where the desired level of resilience is not being delivered by commercial operators.

Significant government reforms are already being progressed to enhance critical infrastructure resilience

20. There are currently several significant programmes of work underway across government that seek to address the resilience of critical infrastructure in New Zealand, including telecommunications.
21. Three critical infrastructure reforms in particular are of direct relevance to the telecommunications sector:
- the **emergency management** system review led by NEMA, with a new Emergency Management Bill due to be presented to the House early this year
 - a regulatory work programme on enhancing **critical national infrastructure resilience**, led by the Department of the Prime Minister and Cabinet (DPMC), s 9(2)(f)(iv)
[REDACTED]
 - s 9(2)(f)(iv)
[REDACTED]

22. MBIE views these work programmes as the best regulatory avenue to advance any telecommunications resilience objectives, as they should enable a coordinated approach to be taken across different critical infrastructure sectors. s 9(2)(g)(i)

Leveraging the broader critical infrastructure reforms is the best opportunity to advance any regulatory telecommunications resilience objectives

23. There are significant benefits to leveraging the broader reforms to advance telecommunications resilience objectives, in particular it would:
- a. ensure any requirements on telecommunications operators are consistent with those placed on other sectors,
 - b. use limited government resources more efficiently (i.e. reduce the number of similar or overlapping work programmes, and ensure existing priorities do not need to be deferred),
 - c. simplify engagement with critical infrastructure entities, particularly given the range of reforms already underway that they have been (and will be) engaged on, and
 - d. likely be implemented in a timely manner, given these work programmes have already been agreed to by Cabinet and will require regulatory changes to be implemented (though the CNI resilience reforms are still only at a 'scoping' stage).

24. s 9(2)(f)(iv)
- [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]

Emergency management (NEMA)

- A new sector emergency response plan could improve access to timely information after an event, sector coordination and preparation for optimising surviving network capacity, and access to sites for telecommunications technicians after an event.

25. s 9(2)(g)(i)
- [Redacted]
 - [Redacted]

s 9(2)(g)(i)

26.

27. s 9(2)(f)(iv)

s 9(2)(f)(iv)

28. s 9(2)(f)(iv)

29.

s 9(2)(f)(iv)

30. s 9(2)(f)(iv)

31.

32.

33.

Next steps

34. MBIE officials will discuss this briefing with you at the next weekly meeting on Monday 20 February 2023.

Annexes

Annex One: Map of North Island Chorus fibre outages post-Cyclone Gabrielle

Annex One: Map of North Island Chorus fibre outages post-Cyclone Gabrielle

s 9(2)(b)(ii)



Released under the Official Information Act 1982



Telecommunications networks – impact of cyclone Gabrielle

Purpose

To provide you with background information, talking points and Q&A ahead of your press stand-up on 15 February 2023 about the impact of cyclone Gabrielle on telecommunications networks in New Zealand.

Background

1. Cyclone Gabrielle has had a significant impact on telecommunications networks and services across the upper North Island over the past few days.
2. As the networks are privately owned and operated, private telecommunications companies are ultimately responsible for addressing these impacts. The Telecommunications Forum (TCF), whose members include most telecommunications companies in the country, plays a coordination role in emergency situations by standing up the Telecommunications Emergency Forum (TEF). The TEF coordinates the sector response to emergencies.
3. On Saturday 11 February, the TCF confirmed that the TEF group would be stood up (at the request of the National Emergency Management Agency (NEMA)) in preparation and response to the cyclone over the coming days. The TEF was then stood up on Monday 13 February.
4. The Government response to emergency events, such as Cyclone Gabrielle, is led by the Minister for Emergency Management and NEMA. As Minister for the Digital Economy and Communications, your role is to speak to the Government's view of the networks and to consider whether the appropriate policy settings are in place for future events.
5. This briefing provides:
 - a. An overview of the impacts on telecommunications networks and services
 - b. Industry plans to address these impacts, expected timeframes and prioritisation for restoring services
 - c. Key messages and Q&A responses for your press stand-up at 5:30 pm today.

Impacts of the cyclone on telecommunications networks and services

6. The **most significant cause of network outages is the loss of mains power** at cell sites and some roadside cabinets. While cell sites and cabinets have battery back-up power, these generally only provide power for between 4-8 hours. In addition to the impact on the network infrastructure, loss of power at end user households means that people cannot access their broadband – and in many cases landline phone – connection.
7. There have also been a small number of breaks in key fibre links, however in these cases the impact is much more significant due to the number of connections reliant on these links. While in most cases the network is built to re-route services on alternate links when fibre breaks occur, there are limits to the diversity of routes available. As JB Rousset from

Chorus informed you earlier today, in the case of the fibre into Gisborne, while there are two fibre links for the area, thereby providing resilience, unfortunately both of those cables have been impacted.

Current status

8. Based on the latest situation report from the TCF and information provided to you by the industry at midday. **Paul Brislen from TCF will be providing your office with the most up-to-date figures immediately before your briefing at 3.30pm:**
 - a. Multiple areas of the North Island are isolated from a telecommunications perspective – Gisborne is cut off as is the east coast of the Coromandel Peninsula
 - b. Five fibre outages have occurred impacting customers in Gisborne, Napier, Hastings, Taupō and Far North regions. Chorus expects two of these outages – Coromandel and north of Taupō to be repaired this afternoon.
 - c. Government agencies are helping in deploying generator sets to isolated areas
 - d. The sector is prioritising restoring the most critical sites with a focus in Napier, broader Hawkes Bay and Gisborne. For example Chorus has a helicopter up this afternoon to assess damage to the fibre cables and determine an approach for repair.
 - e. 225,000 people across the country were without power on Tuesday afternoon, meaning they will not be able to access their broadband connection and may begin to run out of battery on their mobile devices
 - f. Service outages across the main providers (as at 9:00 am 15 February) are as follows:
 - i. **Spark** – 152 Spark sites down; total § 3(2)(b)(i) customer broadband service outages due to loss of power at customer premises
 - ii. **Vodafone** - Approximately 183 cell sites are offline
 - iii. **2degrees** - 126 cell sites are offline mostly due to power cuts; Gisborne offline for both fixed and mobile service due to fibre cuts; Taupo has been partially restored.
 - iv. **Rural Connectivity Group** (a consortium of all three mobile network operators operating in more rural/remote areas) – 122 cell towers offline; 12 mobile sites with mains fail (running on battery); 118 cabinets mains fail (these cabinets provide broadband services)
 - v. **Wireless Internet Service Providers (WISPs) - WISPS** (as at 14 Feb 2022):
Gisborne – Gisborne.Net cut off due to fibre access; Napier / Hastings - Several WISPs severely impacted with over 75% of sites down on some networks due to power or fibre outages; Northland - Isolated impacted sites on regional WISPs; Auckland - Isolated sites impacted by fibre cuts and power supply; Waikato - Isolated sites impacted by fibre cuts and power supply; elsewhere, power and wind damage impacting customers but networks are fully operational.
9. In addition, the TCF has advised officials that the Napier exchange only has 48 hours of fuel remaining to power its generator. The TCF urgently needs the fuel plan from NEMA to

ensure priority access is given to refuel this generator as it is the **sole operational node** for all three networks in the area. Officials will discuss this issue with you in more detail shortly.

10. Current restoration activity is being prioritised in the following areas:
 - a. Cell sites undergoing power management where practical (meaning certain capabilities are disabled to preserve power and prioritise critical functions)
 - b. Priority mobile site list provided to TEF to assist with mains power restoration or generator set placement
 - c. Fuel checks / refuel for generator sites
 - d. Spark – 5 Satellite units and additional generators are being flown into Napier today
 - e. Vodafone – equipment and generators being flown into Napier today.

Key challenges / emerging issues

11. We have been advised by the TCF that two key challenges have presented throughout the response to Cyclone Gabrielle:
 - a. **Access to sites**, particularly in rural areas, is a challenge due to transport issues (with limited access to helicopters), s 9(2)(g)(i) [REDACTED] and health and safety hazards caused by the adverse weather. In many cases, service restoration is delayed until technicians conduct on-site assessments and restoration.
 - b. **Mains power outages** continue to be the main issue facing telecommunications operators, who have a limited number of generators available to deploy compared to the number of sites offline. In addition, ongoing outages place a strain on the fuel supply for these generators, which can compound with access challenges noted above to complicate service maintenance.
12. In addition, resources to address faults are also limited. Service companies continue to look to move resources to impacted or possible impacted areas as well as reallocating technicians from different departments to fault remediation work.

MBIE comment

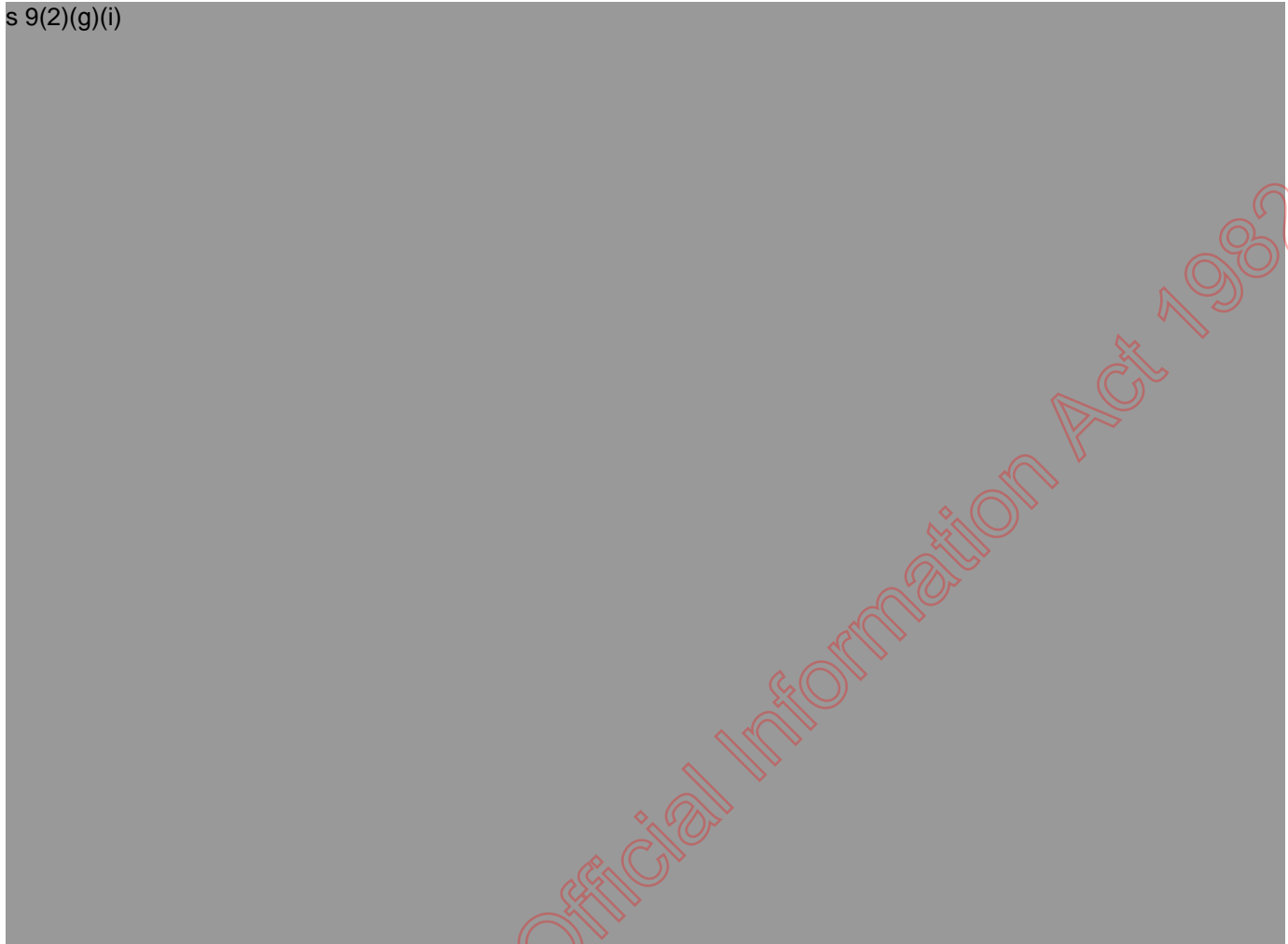
13. We will provide you with more comprehensive advice on resilience in telecommunications networks tomorrow (16 February) as per the request made by your office earlier this week.

Annexes

Annex 1 Material for the press stand-up at 5:30pm, 15 February 2023

Annex 1: Material for your press stand-up at 5:30pm, 15 February 2023

s 9(2)(g)(i)



Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs
Minister for the Digital Economy and Communications
Minister for State Owned Enterprises
Minister of Statistics
Minister Responsible for the Earthquake Commission



11 November 2021

JB Rousselot
Chief Executive Officer
Chorus

Dear JB,

I am writing to you today to request information about the resilience of Chorus' telecommunications network. I understand that other Ministers have previously written to you on this issue, and you will be aware that I have raised it with industry representatives.

I would first like to acknowledge the high level of responsiveness and collaboration that network operators have shown to restore services in recent emergency situations such as the Kaikōura earthquake in 2016, and multiple floods in the Canterbury and West Coast regions. I appreciate your quick actions following these events, and your ongoing cooperation on issues relating to emergency response.

However, as Minister for the Digital Economy and Communications, I consider it important to ensure that the government has the information it needs to be sure that our telecommunications networks can withstand emergency events with limited service interruptions. This is more important than ever due to a number of factors:

- the COVID-19 pandemic has meant that people need to work remotely more frequently, placing greater importance on the reliability of our broadband and mobile networks
- significant natural hazard events are disrupting services more frequently, and this trend will only continue with the impact of climate change
- the increased frequency and impact of cyber-attacks becoming a growing disruptor to New Zealanders' day-to-day lives.

While I acknowledge that we will never be able to make specific, accurate predictions about emergency events, and there will always be a central role for emergency response, it is important that network operators have plans in place to contribute to a robust telecommunications network before an event occurs. This includes implementing appropriate measures to reduce the risk of service outages caused by such events.

I am therefore requesting information from network operators so that the government has a full understanding of the current resilience landscape, and where there might be scope for us to work together to improve the status quo. In particular, I would like to know:

- what dominant risks, vulnerabilities, or system constraints you are aware of that could have an adverse impact on your networks ability keep New Zealanders safe and connected following an event?
- what dominant risks Chorus' current network and service architectures are designed to mitigate;
- how Chorus assesses vulnerabilities in its network, including the risks of natural hazards and anticipated climate change impacts;
- how these risk assessments influence Chorus' consideration of investments in new infrastructure, and which risks your planning excludes;
- how Chorus works with relevant authorities, telecommunications and other companies (for example electricity companies) to mitigate risks, and how these relationships could be enhanced;
- what future plans Chorus has that will enhance the resilience of the network and services to particular natural hazard and other risks.

In addition to the information above, it would be valuable if you could provide the following specific information to better inform the government's understanding on any system issues:

- what Chorus views as the top 3 specific risks to its network based on frequency and severity criteria, and what plans are in place to address them?
- what Chorus views as the top 3 overall system risks to supply consistency, and how Chorus would identify they be best resolved?
- which populous locations are most at risk of service disruption, and what future plans, if any, do you have to improve resilience in these regions?
- are there any competition rules impeding planning for a more resilient network? If so, does Chorus have any suggestions for pragmatic change that government could lead in this regard?
- how does Chorus work with other security providers to prepare for cyber-attacks, and mitigate cybercrime?
- how does Chorus prepare for and support its customers during denial of service attacks and other disruptive cyber incidents? In particular how do you ensure that your network and services can effectively mitigate disruptions in an evolving environment, on order to provide continuity of service?

I have asked my officials at the Ministry of Business, Innovation and Employment (MBIE) to re-assess the government's approach to resilience in the telecommunications sector, and your response to these questions will inform that assessment.

I am also aware that this work coincides with the National Emergency Management Agency's (NEMAs) work on reviewing the Civil Defence and Emergency Management Act, so my officials will work closely with NEMA to ensure work is not duplicated in this space.

I greatly appreciate your cooperation and input into this work going forward.

Yours sincerely

A handwritten signature in blue ink, consisting of a large, stylized 'D' with a horizontal line through it and a vertical line extending downwards from the center.

Hon Dr David Clark
Minister for the Digital Economy and Communications

Released under the Official Information Act 1982

Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs
Minister for the Digital Economy and Communications
Minister for State Owned Enterprises
Minister of Statistics
Minister Responsible for the Earthquake Commission



11 November 2021

Jolie Hodson
Chief Executive Officer
Spark New Zealand Ltd

Dear Jolie,

I am writing to you today to request information about the resilience of Spark's telecommunications network. I understand that other Ministers have previously written to you on this issue, and you will be aware that I have raised it with industry representatives.

I would first like to acknowledge the high level of responsiveness and collaboration that network operators have shown to restore services in recent emergency situations such as the Kaikōura earthquake in 2016, and multiple floods in the Canterbury and West Coast regions. I appreciate your quick actions following these events, and your ongoing cooperation on issues relating to emergency response.

However, as Minister for the Digital Economy and Communications, I consider it important to ensure that the government has the information it needs to be sure that our telecommunications networks can withstand emergency events with limited service interruptions. This is more important than ever due to a number of factors:

- the COVID-19 pandemic has meant that people need to work remotely more frequently, placing greater importance on the reliability of our broadband and mobile networks
- significant natural hazard events are disrupting services more frequently, and this trend will only continue with the impact of climate change
- the increased frequency and impact of cyber-attacks becoming a growing disruptor to New Zealanders' day-to-day lives.

While I acknowledge that we will never be able to make specific, accurate predictions about emergency events, and there will always be a central role for emergency response, it is important that network operators have plans in place to contribute to a robust telecommunications network before an event occurs. This includes implementing appropriate measures to reduce the risk of service outages caused by such events.

I am therefore requesting information from network operators so that the government has a full understanding of the current resilience landscape, and where there might be scope for us to work together to improve the status quo. In particular, I would like to know:

- what dominant risks, vulnerabilities, or system constraints you are aware of that could have an adverse impact on your networks ability keep New Zealanders safe and connected following an event?
- what dominant risks Spark's current network and service architectures are designed to mitigate;
- how Spark assesses vulnerabilities in its network, including the risks of natural hazards and anticipated climate change impacts;
- how these risk assessments influence Spark's consideration of investments in new infrastructure, and which risks your planning excludes;
- how Spark works with relevant authorities, telecommunications and other companies (for example electricity companies) to mitigate risks, and how these relationships could be enhanced;
- what future plans Spark has that will enhance the resilience of the network and services to particular natural hazard and other risks.

In addition to the information above, it would be valuable if you could provide the following specific information to better inform the government's understanding on any system issues:

- what Spark views as the top 3 specific risks to its network based on frequency and severity criteria, and what plans are in place to address them?
- what Spark views as the top 3 overall system risks to supply consistency, and how Spark would identify they be best resolved?
- which populous locations are most at risk of service disruption, and what future plans, if any, do you have to improve resilience in these regions?
- are there any competition rules impeding planning for a more resilient network? If so, does Spark have any suggestions for pragmatic change that government could lead in this regard?
- how does Spark work with other security providers to prepare for cyber-attacks, and mitigate cybercrime?
- how does Spark prepare for and support its customers during denial of service attacks and other disruptive cyber incidents? In particular how do you ensure that your network and services can effectively mitigate disruptions in an evolving environment, on order to provide continuity of service?

I have asked my officials at the Ministry of Business, Innovation and Employment (MBIE) to re-assess the government's approach to resilience in the telecommunications sector, and your response to these questions will inform that assessment.

I am also aware that this work coincides with the National Emergency Management Agency's (NEMAs) work on reviewing the Civil Defence and Emergency Management Act, so my officials will work closely with NEMA to ensure work is not duplicated in this space.

I greatly appreciate your cooperation and input into this work going forward.

Yours sincerely

A handwritten signature in blue ink, appearing to be 'D. Clark', written over a faint yellow circular stamp.

Hon Dr David Clark
Minister for the Digital Economy and Communications

Released under the Official Information Act 1982

Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs
Minister for the Digital Economy and Communications
Minister for State Owned Enterprises
Minister of Statistics
Minister Responsible for the Earthquake Commission



11 November 2021

Mark Aue
Chief Executive Officer
2degrees

Dear Mark,

I am writing to you today to request information about the resilience of 2degrees' telecommunications network. I understand that other Ministers have previously written to you on this issue, and you will be aware that I have raised it with industry representatives.

I would first like to acknowledge the high level of responsiveness and collaboration that network operators have shown to restore services in recent emergency situations such as the Kaikōura earthquake in 2016, and multiple floods in the Canterbury and West Coast regions. I appreciate your quick actions following these events, and your ongoing cooperation on issues relating to emergency response.

However, as Minister for the Digital Economy and Communications, I consider it important to ensure that the government has the information it needs to be sure that our telecommunications networks can withstand emergency events with limited service interruptions. This is more important than ever due to a number of factors:

- the COVID-19 pandemic has meant that people need to work remotely more frequently, placing greater importance on the reliability of our broadband and mobile networks
- significant natural hazard events are disrupting services more frequently, and this trend will only continue with the impact of climate change
- the increased frequency and impact of cyber-attacks becoming a growing disruptor to New Zealanders' day-to-day lives.

While I acknowledge that we will never be able to make specific, accurate predictions about emergency events, and there will always be a central role for emergency response, it is important that network operators have plans in place to contribute to a robust telecommunications network before an event occurs. This includes implementing appropriate measures to reduce the risk of service outages caused by such events.

I am therefore requesting information from network operators so that the government has a full understanding of the current resilience landscape, and where there might be scope for us to work together to improve the status quo. In particular, I would like to know:

- what dominant risks, vulnerabilities, or system constraints you are aware of that could have an adverse impact on your networks ability keep New Zealanders safe and connected following an event?
- what dominant risks 2degrees' current network and service architectures are designed to mitigate;
- how 2degrees assesses vulnerabilities in its network, including the risks of natural hazards and anticipated climate change impacts;
- how these risk assessments influence 2degrees' consideration of investments in new infrastructure, and which risks your planning excludes;
- how 2degrees works with relevant authorities, telecommunications and other companies (for example electricity companies) to mitigate risks, and how these relationships could be enhanced;
- what future plans 2degrees has that will enhance the resilience of the network and services to particular natural hazard and other risks.

In addition to the information above, it would be valuable if you could provide the following specific information to better inform the government's understanding on any system issues:

- what 2degrees views as the top 3 specific risks to its network based on frequency and severity criteria, and what plans are in place to address them?
- what 2degrees views as the top 3 overall system risks to supply consistency, and how 2degrees would identify they be best resolved?
- which populous locations are most at risk of service disruption, and what future plans, if any, do you have to improve resilience in these regions?
- are there any competition rules impeding planning for a more resilient network? If so, does 2degrees have any suggestions for pragmatic change that government could lead in this regard?
- how does 2degrees work with other security providers to prepare for cyber-attacks, and mitigate cybercrime?
- how does 2degrees prepare for and support its customers during denial of service attacks and other disruptive cyber incidents? In particular how do you ensure that your network and services can effectively mitigate disruptions in an evolving environment, on order to provide continuity of service?

I have asked my officials at the Ministry of Business, Innovation and Employment (MBIE) to re-assess the government's approach to resilience in the telecommunications sector, and your response to these questions will inform that assessment.

I am also aware that this work coincides with the National Emergency Management Agency's (NEMAs) work on reviewing the Civil Defence and Emergency Management Act, so my officials will work closely with NEMA to ensure work is not duplicated in this space.

I greatly appreciate your cooperation and input into this work going forward.

Yours sincerely

A handwritten signature in blue ink, appearing to be 'David Clark', enclosed within a large, loopy blue oval.

Hon Dr David Clark
Minister for the Digital Economy and Communications

Released under the Official Information Act 1982

Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs
Minister for the Digital Economy and Communications
Minister for State Owned Enterprises
Minister of Statistics
Minister Responsible for the Earthquake Commission



11 November 2021

Paul Brislen
Chief Executive Officer
New Zealand Telecommunications Forum (TCF)

Dear Paul,

I am writing to you today to request information about the resilience of telecommunications networks in New Zealand. I understand that other Ministers have previously written to the TCF on this issue, and you will be aware that I have raised it with industry representatives.

I would first like to acknowledge the high level of responsiveness and collaboration that network operators have shown to restore services in recent emergency situations such as the Kaikōura earthquake in 2016, and multiple floods in the Canterbury and West Coast regions. I appreciate your quick actions following these events, and your ongoing cooperation on issues relating to emergency response.

However, as Minister for the Digital Economy and Communications, I consider it important to ensure that the government has the information it needs to be sure that our telecommunications networks can withstand emergency events with limited service interruptions. This is more important than ever due to a number of factors:

- the COVID-19 pandemic has meant that people need to work remotely more frequently, placing greater importance on the reliability of our broadband and mobile networks
- significant natural hazard events are disrupting services more frequently, and this trend will only continue with the impact of climate change
- the increased frequency and impact of cyber-attacks becoming a growing disruptor to New Zealanders' day-to-day lives.

While I acknowledge that we will never be able to make specific, accurate predictions about emergency events, and there will always be a central role for emergency response, it is important that network operators have plans in place to contribute to a robust telecommunications network before an event occurs. This includes implementing appropriate measures to reduce the risk of service outages caused by such events.

I am therefore requesting information from network operators so that the government has a full understanding of the current resilience landscape, and where there might be scope for us to work together to improve the status quo. While much of this information will be held by individual operators, it would be valuable to have input from the TCF as you will have a unique perspective on how network operators work together to address these issues. In particular, I would like to know:

- what dominant risks, vulnerabilities, or system constraints you are aware of that could have an adverse impact on the ability of networks to keep New Zealanders safe and connected following an event?
- what dominant risks current network and service architectures are designed to mitigate;
- how or whether TCF assesses vulnerabilities in networks, including the risks of natural hazards and anticipated climate change impacts;
- how TCF works with relevant authorities, telecommunications and other companies (for example electricity companies) to mitigate risks, and how these relationships could be enhanced;
- what future plans TCF has that will enhance the resilience of the networks and services to particular natural hazard and other risks.

In addition to the information above, it would be valuable if you could provide the following specific information to better inform the government's understanding on any system issues:

- which populous locations are most at risk of service disruption, and what future plans, if any, do you have to improve resilience in these regions?
- are there any competition rules impeding planning for a more resilient network? If so, does TCF have any suggestions for pragmatic change that government could lead in this regard?
- how does TCF work with other security providers to prepare for cyber-attacks, and mitigate cybercrime?
- how does TCF prepare for and support customers during denial of service attacks and other disruptive cyber incidents? In particular how do you help to ensure that networks and services can effectively mitigate disruptions in an evolving environment, on order to provide continuity of service?

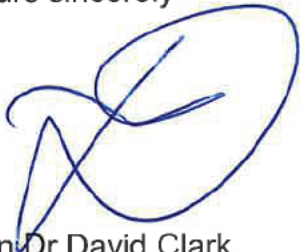
I have asked my officials at the Ministry of Business, Innovation and Employment (MBIE) to re-assess the government's approach to resilience in the telecommunications sector, and your response to these questions will inform that assessment.

I am also aware that this work coincides with the National Emergency Management Agency's (NEMAs) work on reviewing the Civil Defence and Emergency

Management Act, so my officials will work closely with NEMA to ensure work is not duplicated in this space.

I greatly appreciate your cooperation and input into this work going forward.

Yours sincerely

A handwritten signature in blue ink, appearing to be 'D. Clark', written over a faint circular stamp.

Hon. Dr David Clark
Minister for the Digital Economy and Communications

Released under the Official Information Act 1982

Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs
Minister for the Digital Economy and Communications
Minister for State Owned Enterprises
Minister of Statistics
Minister Responsible for the Earthquake Commission



11 November 2021

Mark Callander
Chief Executive Officer
Vocus New Zealand

Dear Mark,

I am writing to you today to request information about the resilience of Vocus' telecommunications network. I understand that other Ministers have previously written to you on this issue, and you will be aware that I have raised it with industry representatives.

I would first like to acknowledge the high level of responsiveness and collaboration that network operators have shown to restore services in recent emergency situations such as the Kaikōura earthquake in 2016, and multiple floods in the Canterbury and West Coast regions. I appreciate your quick actions following these events, and your ongoing cooperation on issues relating to emergency response.

However, as Minister for the Digital Economy and Communications, I consider it important to ensure that the government has the information it needs to be sure that our telecommunications networks can withstand emergency events with limited service interruptions. This is more important than ever due to a number of factors:

- the COVID-19 pandemic has meant that people need to work remotely more frequently, placing greater importance on the reliability of our broadband and mobile networks
- significant natural hazard events are disrupting services more frequently, and this trend will only continue with the impact of climate change
- the increased frequency and impact of cyber-attacks becoming a growing disruptor to New Zealanders' day-to-day lives.

While I acknowledge that we will never be able to make specific, accurate predictions about emergency events, and there will always be a central role for emergency response, it is important that network operators have plans in place to contribute to a robust telecommunications network before an event occurs. This includes implementing appropriate measures to reduce the risk of service outages caused by such events.

I am therefore requesting information from network operators so that the government has a full understanding of the current resilience landscape, and where there might be scope for us to work together to improve the status quo. In particular, I would like to know:

- what dominant risks, vulnerabilities, or system constraints you are aware of that could have an adverse impact on your networks ability keep New Zealanders safe and connected following an event?
- what dominant risks Vocus' current network and service architectures are designed to mitigate;
- how Vocus assesses vulnerabilities in its network, including the risks of natural hazards and anticipated climate change impacts;
- how these risk assessments influence Vocus' consideration of investments in new infrastructure, and which risks your planning excludes;
- how Vocus works with relevant authorities, telecommunications and other companies (for example electricity companies) to mitigate risks, and how these relationships could be enhanced;
- what future plans Vocus has that will enhance the resilience of the network and services to particular natural hazard and other risks.

In addition to the information above, it would be valuable if you could provide the following specific information to better inform the government's understanding on any system issues:

- what Vocus views as the top 3 specific risks to its network based on frequency and severity criteria, and what plans are in place to address them?
- what Vocus views as the top 3 overall system risks to supply consistency, and how Vocus would identify they be best resolved?
- which populous locations are most at risk of service disruption, and what future plans, if any, do you have to improve resilience in these regions?
- are there any competition rules impeding planning for a more resilient network? If so, does Vocus have any suggestions for pragmatic change that government could lead in this regard?
- how does Vocus work with other security providers to prepare for cyber-attacks, and mitigate cybercrime?
- how does Vocus prepare for and support its customers during denial of service attacks and other disruptive cyber incidents? In particular how do you ensure that your network and services can effectively mitigate disruptions in an evolving environment, on order to provide continuity of service?

I have asked my officials at the Ministry of Business, Innovation and Employment (MBIE) to re-assess the government's approach to resilience in the telecommunications sector, and your response to these questions will inform that assessment.

I am also aware that this work coincides with the National Emergency Management Agency's (NEMAs) work on reviewing the Civil Defence and Emergency Management Act, so my officials will work closely with NEMA to ensure work is not duplicated in this space.

I greatly appreciate your cooperation and input into this work going forward.

Yours sincerely

A handwritten signature in blue ink, consisting of a large, stylized 'D' with a horizontal line through it and a vertical line extending downwards from the left side.

Hon Dr David Clark
Minister for the Digital Economy and Communications

Released under the Official Information Act 1982

Hon Dr David Clark

MP for Dunedin

Minister of Commerce and Consumer Affairs
Minister for the Digital Economy and Communications
Minister for State Owned Enterprises
Minister of Statistics
Minister Responsible for the Earthquake Commission



11 November 2021

Jason Paris
Chief Executive Officer
Vodafone New Zealand

Dear Jason,

I am writing to you today to request information about the resilience of Vodafone's telecommunications network. I understand that other Ministers have previously written to you on this issue, and you will be aware that I have raised it with industry representatives.

I would first like to acknowledge the high level of responsiveness and collaboration that network operators have shown to restore services in recent emergency situations such as the Kaikōura earthquake in 2016, and multiple floods in the Canterbury and West Coast regions. I appreciate your quick actions following these events, and your ongoing cooperation on issues relating to emergency response.

However, as Minister for the Digital Economy and Communications, I consider it important to ensure that the government has the information it needs to be sure that our telecommunications networks can withstand emergency events with limited service interruptions. This is more important than ever due to a number of factors:

- the COVID-19 pandemic has meant that people need to work remotely more frequently, placing greater importance on the reliability of our broadband and mobile networks
- significant natural hazard events are disrupting services more frequently, and this trend will only continue with the impact of climate change
- the increased frequency and impact of cyber-attacks becoming a growing disruptor to New Zealanders' day-to-day lives.

While I acknowledge that we will never be able to make specific, accurate predictions about emergency events, and there will always be a central role for emergency response, it is important that network operators have plans in place to contribute to a robust telecommunications network before an event occurs. This includes implementing appropriate measures to reduce the risk of service outages caused by such events.

I am therefore requesting information from network operators so that the government has a full understanding of the current resilience landscape, and where there might be scope for us to work together to improve the status quo. In particular, I would like to know:

- what dominant risks, vulnerabilities, or system constraints you are aware of that could have an adverse impact on your network's ability keep New Zealanders safe and connected following an event?
- what dominant risks Vodafone's current network and service architectures are designed to mitigate;
- how Vodafone assesses vulnerabilities in its network, including the risks of natural hazards and anticipated climate change impacts;
- how these risk assessments influence Vodafone's consideration of investments in new infrastructure, and which risks your planning excludes;
- how Vodafone works with relevant authorities, telecommunications and other companies (for example electricity companies) to mitigate risks, and how these relationships could be enhanced;
- what future plans Vodafone has that will enhance the resilience of the network and services to particular natural hazard and other risks.

In addition to the information above, it would be valuable if you could provide the following specific information to better inform the government's understanding on any system issues:

- what Vodafone views as the top 3 specific risks to its network based on frequency and severity criteria, and what plans are in place to address them?
- what Vodafone views as the top 3 overall system risks to supply consistency, and how Vodafone would identify they be best resolved?
- which populous locations are most at risk of service disruption, and what future plans, if any, do you have to improve resilience in these regions?
- are there any competition rules impeding planning for a more resilient network? If so, does Vodafone have any suggestions for pragmatic change that government could lead in this regard?
- how does Vodafone work with other security providers to prepare for cyber-attacks, and mitigate cybercrime?
- how does Vodafone prepare for and support its customers during denial of service attacks and other disruptive cyber incidents? In particular how do you ensure that your network and services can effectively mitigate disruptions in an evolving environment, on order to provide continuity of service?

I have asked my officials at the Ministry of Business, Innovation and Employment (MBIE) to re-assess the government's approach to resilience in the telecommunications sector, and your response to these questions will inform that assessment.

I am also aware that this work coincides with the National Emergency Management Agency's (NEMAs) work on reviewing the Civil Defence and Emergency Management Act, so my officials will work closely with NEMA to ensure work is not duplicated in this space.

I greatly appreciate your cooperation and input into this work going forward.

Yours sincerely

A handwritten signature in blue ink, appearing to be 'D Clark', written in a cursive style.

Hon Dr David Clark
Minister for the Digital Economy and Communications

Released under the Official Information Act 1982

From: Sam Lord <Sam.Lord@parliament.govt.nz>
Sent: Tuesday, 21 February 2023 2:03 pm
To: Jacqui Robinson (Crown Infrastructure)
Cc: Mark Binns; Graham Mitchell (Crown Infrastructure); James Hartley
Subject: RE: Cyclone Gabrielle Impacts
Attachments: Cyclone Gabrielle Impacts Letter to Ministers.pdf

Hi Jacqui,

Minister Andersen has now noted this letter.

Kind regards,

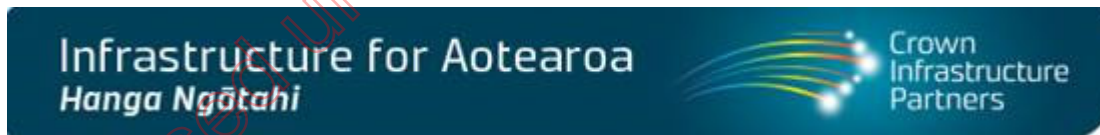
Sam Lord | Private Secretary – Digital Economy and Communications
Office of Hon Ginny Andersen | Mobile: s 9(2)(a)

From: Jacqui Robinson (Crown Infrastructure) [mailto:Jacqui.Robinson@crowninfrastructure.govt.nz]
Sent: Friday, 17 February 2023 5:59 PM
To: Hon Grant Robertson <Grant.Robertson@parliament.govt.nz>; Hon Dr Megan Woods <Megan.Woods@parliament.govt.nz>; Ginny Andersen <ginny.andersen@parliament.govt.nz>
Cc: Amanda Wilson <Amanda.Wilson@parliament.govt.nz>; Sam Lord <Sam.Lord@parliament.govt.nz>; Sandy Grove <Sandy.Grove@parliament.govt.nz>; Mark Binns <mbinns.co@gmail.com>; Graham Mitchell (Crown Infrastructure) <Graham.Mitchell@crowninfrastructure.govt.nz>
Subject: Cyclone Gabrielle Impacts

Please find attached a letter from Mark Binns (Chair of CIP) regarding Cyclone Gabrielle impacts.

Jacqui

Jacqui Robinson
Executive Assistant to Graham Mitchell, CEO
Crown Infrastructure Partners Ltd
L10 HSBC Tower 188 Quay Street | Auckland
PO Box 105321 | Auckland 1143
Phone s 9(2)(a) | Mob s 9(2)(a)



This email and any attachments are confidential to Crown Infrastructure Partners Limited and may be subject to legal privilege or copyright. If you have received this email in error, please advise the sender immediately and delete the email and any attachments from your system. If you are not the intended recipient, you must not use, distribute, amend, copy or rely on this email or any attachments. Emails are not secure. They can be intercepted, amended, lost or destroyed and may contain errors or viruses. If you communicate with Crown Infrastructure Partners Limited by email, you are taken to accept these risks. Any views expressed in this email are those of the individual sender, except where the message states otherwise and the sender is authorised to state them to be the views of Crown Infrastructure Partners Limited.

Released under the Official Information Act 1982



Crown Infrastructure Partners Ltd
L10, HSBC Tower, 188 Quay Street
Auckland Central
PO Box 105 321, Auckland 1143
Telephone: +64 9 912 1970
info@crowinfrasturcture.govt.nz
www.crowninfrastructure.govt.nz

17 February 2023

Hon. Grant Robertson
Minister of Finance

Hon. Megan Woods
Minister for Infrastructure

Hon. Ginny Andersen
Minister for Communications and Digital Economy

Dear Ministers

Re: Cyclone Gabrielle Impacts on Infrastructure

Clearly the impact of Cyclone Gabrielle has been unprecedented in its impact across New Zealand.

The Crown Infrastructure Partners ("CIP") Board met today and agreed that CIP should offer assistance and advice to Government in areas where it has proven competence. There are two areas where we believe we could provide immediate assistance, if required.

You will be aware that CIP is uniquely placed to assist and advise the Government on telecommunications resilience given its role in managing all the Government's telecommunications infrastructure programmes, its commercial relationships with nearly all telecommunication network operators, its oversight of the public safety network and its internal telecommunications engineering capability

Addressing improvement to telecommunications resilience will undoubtedly be required given events and a whole of industry approach will be required to deliver the best results. This will need to be coordinated by someone and given CIP's significant knowledge of the technologies utilised and the approach taken by other countries (e.g. Australia) and independence from the industry, it is well placed to undertake this role. In Australia the Government and the industry agreed what needed to be done in terms of scope from a resilience basis and the contributions to be made by the respective parties. A similar result should be achievable here.

The second area where we could be of assistance is with regard to any urgent repairs in the 3 Waters area. s 9(2)(g)(i)

[Redacted]

As an aside it has been noted how marae can be used as refuge and Civil defence hubs in a number of rural areas. You will be aware that CIP is currently implementing a programme around digital connectivity and safe drinking water for marae around the country. s 9(2)(f)(iv)

[Redacted]

If Ministers have any interest in these initiatives or other queries in terms of relevant infrastructure delivery generally, please feel free to contact either myself or Graham Mitchell at any time.

Yours sincerely



Mark Binns
Chair

c.c. Ben Wells – Treasury
James Hartley - MBIE

Released under the Official Information Act 1982

From: Chris Moses
Sent: Tuesday, 14 September 2021 12:19 pm
To: Jarrod Bryce (Parliament); Charles Jarvie; Susan Hall; James Hartley
Cc: Richard Hills
Subject: RE: West Coast outage update [UNCLASSIFIED]

Hi Jarrod – talking points below.

Let me know if we're missing something 😊

Chris

Talking points following West Coast fibre outage on 13 September

s 9(2)(g)(i)



Released under the Official Information Act 1982

From: Jarrod Bryce <Jarrod.Bryce@parliament.govt.nz>
Sent: Tuesday, 14 September 2021 11:27 am
To: Charles Jarvie <Charles.Jarvie@mbie.govt.nz>; Chris Moses <Chris.Moses@mbie.govt.nz>; Susan Hall <Susan.Hall@mbie.govt.nz>; James Hartley <James.Hartley@mbie.govt.nz>
Cc: Richard Hills <Richard.Hills2@mbie.govt.nz>
Subject: RE: West Coast outage update [UNCLASSIFIED]

Thanks for sending this through Charles – it is helpful context.

Can I confirm that I will still get a few lines from the Minister on this? As well as a few general lines it would be good to have a few specific lines.

Specifically:

- Connectivity: what is being done to improve connectivity (how fast link would have influenced this event)
- Emergency: how do people contact emergency services in such an event
- Resilience: what has been done (should be done) to improve resilience

Jarrod

From: Charles Jarvie [<mailto:Charles.Jarvie@mbie.govt.nz>]
Sent: Tuesday, 14 September 2021 10:32 AM
To: Chris Moses <Chris.Moses@mbie.govt.nz>; Jarrod Bryce <Jarrod.Bryce@parliament.govt.nz>; Susan Hall <Susan.Hall@mbie.govt.nz>; James Hartley <James.Hartley@mbie.govt.nz>; Ajay Makhija <Ajay.Makhija@nema.govt.nz>
Subject: FW: West Coast outage update [UNCLASSIFIED]
Importance: High

Folk,

Note the send time – received here around 10:25am, MBIE email system issue. I have not edited to speed up distribution.

The 111 availability situation is complex as it depends on how service providers implement the landline service for their customers.

If mobile network is unavailable 111 roaming will not occur for RCG based services in South Westland and will only be available from another standalone network if its backhaul is still intact.

Charles

From: s 9(2)(a) <[REDACTED]@chorus.co.nz>
Sent: Tuesday, 14 September 2021 9:50 AM
To: Charles Jarvie <Charles.Jarvie@mbie.govt.nz>
Cc: s 9(2)(a) <[REDACTED]@chorus.co.nz>; s 9(2)(a) <[REDACTED]@chorus.co.nz>
Subject: Re: West Coast outage update [UNCLASSIFIED]

Hi Charles

Below is a summary of where we are at currently, and I'll keep you updated on progress.

Yesterday morning at about 4am multiple lightning strikes on the West Coast just south of Kumara Junction, damaged a Chorus fibre cable with approximately 3,500 broadband services affected and some mobile cell towers that use fibre to move data around the network. The majority of impact was felt in Franz Josef, Fox Glacier, Greymouth, Hokitika, Harihari, Whataroa and Ross.

Initially yesterday, the adverse weather made locating and assessing the damage challenging. When the section of damage cable was located it was discovered to be running under private land in flooded paddocks. To restore services we needed to source a 600m fibre cable overlay (a temporary repair that would leave the fibre on the surface until we were able to do a full repair later). By now it was early evening and the replacement cable needed to come from Christchurch overnight.

Technicians are on the ground now and carrying out the work to bypass the damaged fibre with the overlay. We've expecting this to be completed today, but don't yet have an expected time for restore.

The West Coast fibre in build at the moment will give resilience to the area when it is completed to Lake Hawea.

Kind regards

s 9(2)(a)

| **Regulatory & Policy Affairs Manager**

C H O R U S | T s 9(2)(a) | M s 9(2)(a)

From: Charles Jarvie <Charles.Jarvie@mbie.govt.nz>

Date: Tuesday, 14 September 2021 at 9:23 AM

To: s 9(2)(a) <[s 9\(2\)\(a\)@chorus.co.nz](mailto:s 9(2)(a)@chorus.co.nz)>

Subject: West Coast outage update [UNCLASSIFIED]

s 9(2)(a)

Hi

Does Chorus have an update on the outage impacting locations south of Hokitika? Spark's website indicates still broadband and mobile outages. The Chorus outage page shows "... the system is currently under maintenance".

Minister is talking at the Rural Symposium today and likely to raise the outage in the context of resiliency etc.

Thanks

Charles

www.govt.nz - your guide to finding and using New Zealand government services

Any opinions expressed in this message are not necessarily those of the Ministry of Business, Innovation and Employment. This message and any files transmitted with it are confidential and solely for the use of the intended recipient. If you are not the intended recipient or the person responsible for delivery to the intended recipient, be advised that you have received this message in error and that any use is strictly prohibited. Please contact the sender and delete the message and any attachment from your computer.

The content of this email (including any attachments) is intended for the addressee only, is confidential and may be legally privileged. If you've received this email in error, you shouldn't read it - please contact me immediately, destroy it, and do not copy or use any of the content of this email. No confidentiality or privilege is waived or lost by any mis-transmission or error. This communication does not designate an information system for the purposes of Part 4 of the Contract and Commercial Law Act 2017. Although we have taken reasonable precautions to ensure no viruses are present in this email, we cannot accept responsibility for any loss or damage arising from the use of this email or its attachments.

Any opinions expressed in this message are not necessarily those of the Ministry of Business, Innovation and Employment. This message and any files transmitted with it are confidential and solely for the use of the intended recipient. If you are not the intended recipient or the person responsible for delivery to the intended recipient, be advised that you have received this message in error and that any use is strictly prohibited. Please contact the sender and delete the message and any attachment from your computer.

Released under the Official Information Act 1982