DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Proactive Release

The following documents have been proactively released by the Department of the Prime Minister and Cabinet (DPMC) on behalf of Rt Hon Chris Hipkins, Minister for National Security and Intelligence:

Proactive Release: Enhancing Critical Infrastructure Resilience

The following documents have been included in this release:

Title of Briefing: Enhancing Critical Infrastructure Resilience – Release of Discussion Document

Title of Paper: Acting urgently to strengthen the resilience of New Zealand's critical infrastructure system – Release of Discussion Document (CAB-23-SUB-0226)

Title of Minute: Acting urgently to strengthen the resilience of New Zealand's critical infrastructure system – Release of Discussion Document (ERS-23-MIN-0025)

Title of Minute: Acting urgently to strengthen the resilience of New Zealand's critical infrastructure system – Release of Discussion Document (CAB-23-MIN-0226)

Some parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant section of the Act that would apply has been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Key to redaction codes:

- Section 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand;
- section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials;
- section 9(2)(g)(ii), to prevent improper pressure or harassment.

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Coversheet

Briefing: Enhancing critical infrastructure resilience - Release of Discussion Document

Date:	1 March 2023	**Report No:**	DPMC-2022/23-753
		Security Level:	~~[RESTRICTED]~~
		Priority level:	[High]

	Action sought	Deadline
Rt Hon Chris Hipkins **Prime Minister and Minister for National Security and Intelligence** Hon Andrew Little **Minister Responsible for the GCSB** Hon Ginny Andersen **Minister for the Digital Economy and Communications**	**Agree** to commence Ministerial consultation on a Cabinet paper (Attachment A) seeking agreement - to progress the urgent work on critical infrastructure resilience through a single legislative package and - commence public consultation on the limits of our current regulatory settings. Or **agree,** if Ministers would prefer to continue to prioritise work on the critical infrastructures' cyber resilience, to commence consultation on an alternative draft Cabinet paper (Attachment E).	7/3/2023
Hon Grant Robertson **Minister for Cyclone Recovery** Hon Dr Megan Woods **Minister for Infrastructure**	**Note** the contents of this report.	N/A

Name	Position	Telephone		1st Contact
Tony Lynch	Deputy Chief Executive National Security Group	s9(2)(g)(ii)	s9(2)(g)(ii)	✓
s9(2)(g)(ii)	Principal Policy Advisor	s9(2)(g)(ii)	s9(2)(g)(ii)	

Departments/agencies consulted on Briefing
These agencies were consulted on the discussion document and Cabinet paper: Ministry of Foreign Affairs and Trade, Treasury, Ministry of Business, Innovation and Employment, Ministry of Transport, Department of Internal Affairs, Ministry for the Environment, National Emergency Management Agency, Te Waihanga (the Infrastructure Commission), New Zealand Security Intelligence Service, the Government Communications Security Bureau, Commerce Commission, Electricity Authority, Reserve Bank of New Zealand, and LINZ.

Minister's Office

Status:

☐ Signed ☐ Withdrawn

Comment for agency:

Attachments:

Attachments:	Title	Security classification
Attachments relevant to delivering on the recommended single Bill approach to enhancing infrastructure resilience (RECOMMENDED)		
Attachment A:	Alternative draft Cabinet paper (seeking approval for taking measures forward as one Bill)	IN-CONFIDENCE
Attachment B:	Draft Discussion Document	IN-CONFIDENCE
Attachment C:	Draft Summary Discussion Document	IN-CONFIDENCE
Attachments relevant to delivering on Cabinet's previously agreed two Bill approach to enhancing infrastructure resilience		
Attachment D:	Proposed approach to delivering on two Bill approach	IN-CONFIDENCE
Attachment E:	Draft Cabinet paper to deliver on two Bill approach	IN-CONFIDENCE

Briefing

Enhancing critical infrastructure resilience - Release of Discussion Document

To: Rt Hon Chris Hipkins
Prime Minister and Minister for National Security and Intelligence
Hon Grant Robertson
Minister for Cyclone Recovery
Hon Dr Megan Woods
Minister for Infrastructure
Hon Andrew Little
Minister Responsible for the GCSB
Hon Ginny Andersen
Minister for the Digital Economy and Communications

Date	1/03/2023	**Security Level**	~~[RESTRICTED]~~

Purpose

1. In late-2022, Cabinet agreed to progress two pieces of legislation to enhance critical infrastructure resilience – one focussed on cyber resilience in 2024 and a second focussed on broader resilience (including against natural hazards) in 2025.
2. However, in light of pronounced critical infrastructure failures caused by Cyclone Gabrielle and the Prime Minister's concern that reform to enhance infrastructure resilience to natural hazards be completed prior to 2025, we propose that the decision to develop two separate Bills and prioritise work on cyber resilience be revisited. Given this changed context, we instead recommend taking forward all work to enhance infrastructure resilience as a single Bill for introduction in 2024.
3. To ensure that Cabinet's December aspiration for a Bill to be introduced in 2024 can be met, regardless of Ministers' preferred approach to taking this work forward, this briefing also provides:
   - two alternative Cabinet papers for Ministerial consultation, one that continues to prioritise work on cyber resilience and one that seeks to combine and accelerate the entire work programme; and
   - a discussion document setting out the limitations of New Zealand's current regulatory approach to delivering critical infrastructure resilient to cyber and other hazards and threats, which can be released under either option.

The Prime Minister has overall responsibility for this work as part of his National Security and Intelligence portfolio (it is part of the Foreign Interference Work Programme).

The Minister Responsible for the Government Communications Security Bureau and the Minister for the Digital Economy and Communications are jointly responsible for work to enhance cyber resilience.

The Minister for Infrastructure is responsible for monitoring the Government's response to the Infrastructure Strategy.

The Minister for Cyclone Recovery is copied in given this work's interaction with this portfolio's interests.

Executive Summary

Background and context

4. Critical infrastructures – like electricity, water, transport and telecommunications networks – underpin almost all of New Zealand's economic activity and are essential to New Zealanders' health and wellbeing.
5. As most recently illustrated through the Auckland floods and Cyclone Gabrielle, the loss, damage, disruption, and immobilisation of critical infrastructure can severely prejudice the provision of essential services, undermine public safety, and pose national security threats. New Zealand's regulatory settings are demonstrably not fit for purpose in managing these hazards and threats.
6. Recognising this, in late-2022 Cabinet agreed to develop two pieces of legislation enhance critical infrastructure resilience.
   - The first, focussed on cyber threats, was proposed to be fast-tracked for introduction in 2024. This recognised that despite the growing cyber threat, many of our critical infrastructures are insufficiently prepared to respond to, recover from, and prevent cyber incidents, which can severely disrupt or paralyse critical services.
   - The second, focussed on broader resilience against all hazards and threats (including severe weather events), was to be introduced in 2025.

Cyclone Gabrielle has illustrated the need to urgently enhance infrastructure resilience to natural hazards, alongside cyber and other threats

7. In light of the significant infrastructure vulnerabilities to natural hazards demonstrated by Cyclone Gabrielle and the Prime Minister's concern that concluding work to enhance critical infrastructure resilience in 2025 was not fast enough, this paper instead recommends seeking Cabinet agreement to:
   - take forward this work through a single, comprehensive piece of legislation to be introduced in late-2024; and
   - shortly commence consultation on the shortcomings of our current regulatory settings, as a first step towards creating social license for reform and ahead of consultation on specific reform options in early-2024.
8. We consider that prioritising work on resilience against all hazards and threats for introduction in 2024 would most effectively build on, and help to guarantee, the investments that the government and private sector will inject to building back better as part of the immediate recovery. This is because it would best ensure that critical infrastructure owners and operators are subject to regulatory obligations, such as robust minimum standards, that leave us better prepared for future severe weather and national security events.
9. Relative to developing two Bills, we also consider that taking forward a single legislative package would also provide a more coherent public narrative on government priorities; reduce legislative complexity, make better use of agency resources; and free up drafting and Parliamentary time through 2024 and 2025.
10. To deliver on this recommendation, a draft Cabinet paper, discussion document (for technical audiences) and summary discussion document (for lay audiences) are available at Attachments A, B and C respectively.
11. Alternatively, if you would prefer to continue to progress this work through two Bills, Attachment D sets out a proposed approach to doing so, while Attachment E includes a draft Cabinet paper seeking agreement to this.

While necessary, progressing this work quickly will carry risks

12. While this work is highly important, delivering a regulatory regime to enhance critical infrastructure resilience will be complex and costly. Recognising this, coupled with a potentially rapid reform process, s6(a)

13. To help mitigate these risks, we have proposed an intensive two-stage consultation process that will best allow the Government to build social license for reform and tailor any options to New Zealand's specific geographic and economic conditions. However, we also recommend that you (the Prime Minister) agree to:

    s6(a)

    - officials briefing all political parties on this work before consultation commences.

14. Finally, we recognise that you may wish to progress regulatory reform faster still given the devastating impact of recent events. The convention against releasing significant policy announcements or options for reform during the pre-election period will likely constrain our ability to do this. However, this could be overcome with cross-party agreement to continue to progress this work during that period.

Next steps

15. To ensure that the timelines Cabinet agreed in December can be met (irrespective of whether you elect to proceed with two Bills or one), we propose that the attached Cabinet paper and discussion documents be circulated for Ministerial consultation (subject to any desired changes) by 15 March. This would allow these to be considered at DEV on 5 April 2023 and consultation to commence for one month from 12 April 2023.

16. During the proposed Ministerial consultation period, we will continue to make minor editorial and graphical changes to the documents.

17. Subject to your decisions on this briefing, we will also provide additional advice as soon as possible with:

    - talking points to support you at Cabinet;
    - a press release to announce public consultation; and
    - potential meetings with other political parties on the need for and potential pace of reform.

Recommendations

We recommend you:

1. **Note** that in late-2022, Cabinet agreed to progress two Bills to enhance the resilience of New Zealand's critical infrastructure – one focussed on cyber resilience in 2024 (reflecting the urgent need to enhance critical infrastructure resilience to cyber threats) and one focussed on broader resilience in 2025.

2. **Note** that Cyclone Gabrielle has demonstrated the weaknesses of New Zealand's broader critical infrastructure system to natural hazards, with power, communications, transport, and payments systems all experiencing significant outages.

3. **Note,** in light of recent widespread critical infrastructure failures, that Officials from a range of agencies, including the National Cyber Security Centre, recommend progressing measures to enhance critical infrastructure resilience through a single Bill.

4. **Note** that holistic regulatory reform would complement short-term efforts to build back damaged infrastructure better, by ensuring that all critical infrastructures are subject to robust minimum resilience standards.

5. **EITHER (RECOMMENDED)**

5.1. **Agree**, subject to any required changes, to circulate the attached draft Cabinet Paper (Attachment A) seeking approval to take forward work on infrastructure resilience as a single Bill and release a discussion document and summary discussion document on the need for reform (Attachments B and C) for Ministerial consultation. **YES / NO**

OR (NOT RECOMMENDED)

5.2. **Agree**, subject to any required changes, to circulate the attached alternative draft Cabinet Paper (Attachment E) seeking approval to continue to prioritise work on cyber resilience and release a discussion document and summary discussion document on the need for reform (Attachments B and C) for Ministerial consultation. **YES / NO**

6. **Note** that there are risks and constraints on delivering this project, including s6(a)

7. **Agree** that DPMC work with Treasury to revise its 2023 Budget bid to support accelerated work to enhance infrastructure resilience. **YES / NO**

8. **Agree** that officials brief relevant members of all political parties on the need for reform ahead of the proposed discussion document being released. **YES / NO**

9. **Agree**, if you wish to further expedite this work by consulting on options for reform during the pre-election period, to seek cross-party support to do so. **YES / NO**

10. **Agree** to proactively release this report, subject to withholding any information justified under the Official Information Act 1982. **YES / NO**

Tony Lynch **Deputy Chief Executive** **National Security Group**	Rt Hon Chris Hipkins **Prime Minister and Minister for National Security and Intelligence**
01/03/2023	……../……../……..
Hon Grant Robertson **Minister for Cyclone Recovery**	Hon Dr Megan Woods **Minister for Infrastructure**
……../……../……..	……../……../……
Hon Andrew Little **Minister Responsible for the GCSB**	Hon Ginny Andersen **Minister for the Digital Economy and Communications**
……../……../……..	……../……../……

Background

Background and context

1. Critical infrastructures provide the goods and services we rely on to live fulfilling lives. Their loss, damage, disruption, or immobilisation severely prejudices the provision of essential services, pose risks to national security, and can undermine public safety and/or the maintenance of law and order.
2. In September 2022, as part of its response to Rautaki Hanganga o Aotearoa, New Zealand's first Infrastructure Strategy, the Government announced that in the first half of 2023 it would commence consultation on whether New Zealand's regulatory approach to delivering resilient critical infrastructure was fit for purpose.
3. This work has the goal of enhancing critical infrastructure resilience against all hazards and threats. This is intended to:
   - enhance wellbeing, by reducing the number and consequences of infrastructure failure (including loss of lives and livelihoods);
   - support economic growth, by providing people with confidence to take risks and invest knowing that critical services and systems will remain available;
   - save public (and the broader economy) money, given:
     i. the government's significant and growing exposure to emergencies as private insurers withdraw from a number of markets; and
     ii. economic analysis indicates that investing in resilience ahead of an event is cheaper than funding recovery after one.
4. In December 2022, Cabinet separately agreed to prioritise the delivery of cyber resilience initiatives, including minimum cyber security standards and mandatory reporting of cyber incidents, through standalone legislation [ERS-22-MIN-0063 refers]. This reflected Cabinet's view of the need to address cyber security more urgently than other threats, and improve the ability of critical infrastructures to respond to, recover from, and prevent cyber incidents. Legislation to implement these measures was to be introduced to the House in 2024, with consultation to commence in the first half of 2023.
5. In light of pronounced critical infrastructure failures in the wake of Cyclone Gabrielle, on 20 February 2023 the Prime Minister expressed concern that finalising work to enhance critical infrastructure resilience in 2025 was not fast enough.

Guide to this paper

6. Recognising the changed context, this paper:
   - sets out how this work could be taken forward through a single, urgent, legislative programme; and
   - provides a draft Cabinet paper (Attachment A) for Ministerial consultation seeking:
     i. approval of this approach; and
     ii. the release of a discussion document and summary discussion document focussed on the limitations of our current regulatory settings for stakeholder feedback (Attachment B and C, respectively).
7. The discussion documents referred to above would need to be released in April to meet Cabinet's agreed timelines, irrespective of whether Ministers elect to proceed with two bills or one. However, if Ministers prefer to continue to progress this work through two Bills, Attachment E details how this could best be achieved, with Attachment F providing an alternative Cabinet paper for Ministerial consultation that would deliver on this approach.

Cyclone Gabrielle has demonstrated the need to prioritise and accelerate work on infrastructure resilience to natural hazards

Recent infrastructure failures highlight the importance of building resilience to address non cyber risks

8. Poor weather throughout summer 2022/23 in Northland and the Bay of Plenty, Auckland's January storms and flooding, February's Cyclone Gabrielle, and flooding across Nelson, Tasman and Marlborough in 2022 have demonstrated how fragile New Zealand's critical infrastructure system is. This includes:
   - significant communications failures, complicating search and rescue and the coordination of emergency response as well as inhibiting citizens' abilities to access emergency information, contact family and friends, and conduct essential business;
   - the closure of Auckland International Airport due to flooding and pre-emptive closure of a range of ports (with implications for the supply of essential goods, including food);
   - loss of power supply to hundreds of thousands of people across Hawke's Bay and Gisborne;
   - outages to payments systems in Northland, following the severing of an internet cable, leaving citizens unable to buy groceries and other essential goods; and
   - the collapse and significant deterioration of many regionally and nationally significant transport links, including State Highway 1.
9. These events highlight New Zealand's significant exposure to extreme weather events, as well as how underprepared our infrastructure system is to manage and respond to an increasingly complex and compounding set of challenges (climate change chief among them). In this context, it is increasingly clear that cyber risks – while essential for us to manage – are but one of many significant risks to infrastructure resilience, and we must urgently move to enhance infrastructure resilience against all of them.

Progressing a single Bill to manage all risks to infrastructure resilience will have several benefits…

10. Given this changed context, we recommend that Ministers seek Cabinet approval to combine all measures to enhance infrastructure resilience into a single Bill to be delivered in late-2024 (as per the project timeline at Table 1). This is on a similar but slightly longer timeline to the proposed standalone Cyber Resilience Bill, due to the additional work required to address all hazards and threats (relative to only focussing on cyber resilience).
11. Proceeding with a single legislative programme is strongly supported by government agencies. In addition to better managing both natural hazard and cyber risks to infrastructure resilience (among other threats) as quickly as possible, it would:
    - build on proposed reforms to the emergency management system (which will go some way to setting new resilience requirements for critical infrastructures);
    - complement, through the establishment of robust and enforceable minimum standards for all critical infrastructures:
      i. immediate efforts to build damaged critical infrastructure back better (in some cases using public funds) by best ensuring that those assets are long lived; and
      ii. amendments to the resource management regime (which will better ensure that new critical infrastructures are not constructed in hazard-exposed areas);
    - reduce legislative and engagement complexity (and the risk of errors and stakeholder opposition), simplifying the process for the largely identical group of industry and community stakeholders that will be central to the design of cyber and broader risk mitigations;

- make better use of agency and drafting resources, recognising that that the legislative measures required to enhance cyber resilience would be very similar to those required to lift broader resilience (for example, powers to prescribe specific resilience standards);
- provide a legislative mechanism to deliver on some commitments under the National Adaptation Plan (particularly action 5.6, developing a resilience standard); and
- free up additional drafting, Select Committee, and Parliamentary time through 2024 and 2025 for the Government to progress work on other legislative priorities.

Table 1: Timeline for delivering legislation to enhance infrastructure resilience

Prospective Date	Milestone
April – May 2023	Consultation on Discussion Document on need for reform
s9(2)(f)(iv)	

…however, there are still constraints on how quickly legislative reform can be progressed.

12. We understand – and share – Ministers' desire to act urgently to remediate the regulatory gaps made evident by the recent extreme weather events.
13. Nevertheless, there are several constraints and risks that we consider would make it difficult to deliver comprehensive legislation prior to November 2024.

- **The need for broad-based community and industry support:** Domestic and international experience consistently reinforces the importance of securing broad community and industry support for the long-term success of prospective legislation. This is because local communities, industry and government ultimately need to partner in the delivery of resilient critical infrastructure – with cross-party support on the need for and objectives of reform critical to achieving this.

- **General Election conventions:** Ordinarily the Government would not release any significant policy proposals (in this case, options for regulatory reform) in the three months before the General Election (that is, from July 2023). Given the complexity of this work – and economy-wide consequences of any errors – we do not consider it would be feasible to consult on well-developed options for reform by June 2023.
- **Delays in Government formation:** The delivery of a Bill early in 2024 is contingent upon a Government being able to form – and Ministers being confirmed – soon after the October 2023 General Election.

s6(a) [redacted]

14. There are, however, options available to overcome some of these constraints. To support this work being delivered as quickly as possible, we seek your agreement to:
    - **build additional broad-based community support** through officials engaging with other political parties on this work ahead of the proposed discussion document's release;
    - **accelerate this work while complying with general election conventions,** by seeking cross-party agreement to consult on options for reform during the pre-election period. This would bring delivery of the reform forward by at least four months (to around July 2024 rather than November 2024); and
    - **address resourcing gaps** by working with Treasury to increase the $3.2 million Budget bid lodged on behalf of the Minister for National Security and Intelligence to support this work (building on NSG's efforts to establish a cross-agency project team, drawing on existing resources across government).

Consultation will be critical to the Government's success.

15. To further maximise the possibility of broad community support, we propose a two-stage consultation process to progress this work. These stages are:
    - **Stage one:** Consultation on the need for reform and potential options that government should consider to address current shortcomings. This is to commence in April 2023.
    - **Stage two:** Consultation on specific reform options to enhance the resilience of critical infrastructures. This would be intended for release after the 2023 General Election (unless there is cross-party agreement to this work being released during the pre-election period).

16. While this approach is relatively time-consuming, we consider it essential to ensuring that even if this work is delivered at pace, it will be seen as credible and enduring. This reflects that any reforms will be complex and costly, for:
    - critical infrastructure owners and operators, in terms of direct investments and any additional compliance costs; and
    - consumers that will ultimately pay for investments to enhance resilience (at least in part) through higher bills and/or rates. (This has been a sticking point for investments in resilience in the past, with many examples of industry attempting to invest to enhance resilience but consumers being unwilling to pay for it).

17. Taking the time to consult widely with all New Zealanders, will allow us to:
    - clearly articulate that while investments in resilience will be more visible to New Zealanders through their bills, these costs will ultimately be lower than the cost to society of frequent outages, service restoration, and infrastructure rebuilds;

- develop options that are tailored to New Zealand's economic and geographic realities and regulatory landscape, rather than simply duplicating models adopted overseas; and
- save time at the end of the process, learning from Australia's recent experience which was seen as insufficiently consultative and led to significant delays during the Parliamentary process.

18. This approach, as distinct from moving rapidly to consult on options, also recognises that:
    - critical infrastructure entities, lifeline groups, and iwi (among others) that we will need to consult, and government agencies that would need to input into option design, are actively supporting immediate recovery efforts. It would be inappropriate to distract them from this work given their limited resources; and
    - iwi have significant interests in the critical infrastructure sector, but also limited bandwidth to engage intensively at this time given the scale of the Government's reform agenda. A more considered process therefore offers the Government the best opportunity to deliver on its obligations as Treaty partner.

Meeting these ambitious timelines requires public consultation on the need for reform to commence as soon as possible

19. To meet the ambitious timelines outlined in Table 1 (and agreed by Cabinet in December 2022), we have prepared a draft Cabinet paper (Attachment A) to urgently seek approval to:
    - progress this work as a single legislative package; and
    - commence the first stage of consultation (ideally in April 2023).
20. Consistent with this, we have prepared a draft discussion document (Attachment B; written for a technical audience) and summary discussion document (Attachment C; written for a lay audience) for release. These documents outline the:
    - work programme's objective and principles underpinning reform;
    - four megatrends that require New Zealand to update its approach to critical infrastructure regulation (climate change; the rapid advent and take-up of new technologies; a more complex geopolitical and national security environment; and weaknesses in the globalised economic model); and
    - shortfalls in New Zealand's regulatory system relative to global best practice, including our inability to set enforceable resilience standards.
21. If endorsed for release, there would be around four weeks for the public to prepare written submissions. This would be supplemented by open-invite town-hall style sessions with expert stakeholders (such as local government and cyber security experts) in Wellington, Auckland and Christchurch, in addition to hui with Māori and iwi.
22. Finally, while this consultation period is shorter than best practice, a longer period would place our ability to deliver legislation to enhance resilience in 2024 at risk.

Next steps

23. To ensure that legislation can be introduced to the House in 2024 – and we can meaningfully engage with stakeholders on this topic – the proposed approach to the project and discussion document need to be considered at DEV on 5 April 2023.

24. The key milestones to meet this deadline are detailed below.

Milestone	Due date
Ministers provide decisions and feedback on this report	7 March 2023
Ministerial consultation on draft Cabinet paper and discussion document	15 March – 29 March 2023
Lodgement of Cabinet paper and discussion document	30 March 2023
Consideration of Cabinet paper by DEV	5 April 2023
Consideration of Cabinet paper by Cabinet	11 April 2023
Release of discussion document	12 April 2023

25. During the Ministerial consultation period, officials will continue to make minor editorial and graphical changes to the proposed discussion documents. The final versions of these documents will be provided to your offices ahead of lodgement for Cabinet.

26. Subject to your decisions, we will provide additional advice as soon as possible with:

- talking points to support you at Cabinet;
- a press release to announce the commencement of consultation;
- potential meetings with other parties on the need for and potential pace of reform; and
- information on any interactions between this work programme and broader work being undertaken in support of Cyclone recovery.

27. If you elect to proceed with developing two Bills to enhance critical infrastructure resilience, we will update the consultation materials to reflect the reasons for prioritising cyber resilience. We will work to the same milestones set out in paragraph 24 but circulate the Cabinet paper in Attachment E for Ministerial consultation.

Attachments:	Title	Security classification
Attachments relevant to delivering on an alternative and recommended single Bill approach to enhancing infrastructure resilience (RECOMMENDED)		
Attachment A:	Draft Cabinet paper	IN-CONFIDENCE
Attachment B:	Draft Discussion Document	IN-CONFIDENCE
Attachment C:	Draft Summary Discussion Document	IN-CONFIDENCE
Attachments relevant to delivering on Cabinet's previously agreed two Bill approach to enhancing infrastructure resilience (NOT RECOMMENDED)		
Attachment D:	Proposed approach to delivering on two Bill approach	IN-CONFIDENCE
Attachment E:	Alternative draft Cabinet paper	IN-CONFIDENCE

Attachment A: Draft Cabinet Paper (RECOMMENDED)

Attachment B: Draft Discussion Document (RECOMMENDED)

Attachment C: Draft Summary Discussion Document (RECOMMENDED)

Attachment D: Proposed programme to deliver on agreed two Bill approach to enhance infrastructure resilience

1. This attachment proposes an approach to delivering on Cabinet's decisions to develop two Bills (one on cyber resilience in 2024, and one on broader resilience in 2025) to collectively improve the regulatory approach to delivering resilient critical infrastructure.

2. As noted in the body of the report, this is not recommended. Cyclone Gabrielle has clearly demonstrated that New Zealand's critical infrastructure resilience is highly vulnerable to natural hazards and working to manage these vulnerabilities as quickly as cyber (and other vulnerabilities) is in the interests of all New Zealanders.

We propose three phases of public consultation to best ensure coherent reform…

3. If Ministers do wish to proceed with the development of two Bills focussed on infrastructure resilience, we judge that a three-phase approach to public consultation would meet Cabinet's timetable for introducing a standalone cyber resilience Bill, while enabling sufficient public feedback and buy-in.

4. This approach would allow the public to provide feedback across the policy process while presenting a consistent narrative on how the related reforms to enhance critical infrastructure resilience[1] build to a coherent whole.

5. Table 2 contains a detailed project plan for your information. In general terms, the three phases of public consultation would be:

   - **Phase one:** As recommended under the single Bill approach, consultation on the shortcomings of our current regulatory approach to delivering critical infrastructure resilience (covering cyber threats and broader hazards), with the goal of building understanding of the need for government intervention to boost resilience.

   - **Phase two:** Consultation on specific reform options to enhance the cyber resilience of critical infrastructures. This would be released in June 2023, to ensure that advice on final policy decisions can be taken immediately after the General Election, allowing a Bill to be drafted for introduction in mid-2024.

     NB: This would require consultation to close after the commencement of the pre-election period.

   - **Phase three:** Consultation on broader options to enhance critical infrastructure resilience against all hazards and threats. This would be released in 2024 following Cabinet taking final decisions on measures to enhance cyber resilience, with the goal of introducing a Bill on broader infrastructure resilience in 2025.

6. This approach to consultation has been designed to manage the various path dependencies between the separate, but related legislative programmes. We consider that it would enable the optimal delivery of the two Bills because it:

   - recognises that the fundamental drivers behind the poor cyber and broader resilience of New Zealand's critical infrastructures are the same for both cyber risks and other

[1] That is, the recently tabled Emergency Management Bill (which will extend resilience requirements to a range of new critical infrastructures) as well as the proposed Bills to enhance infrastructures' cyber and broader resilience discussed in this Report.

hazards (for example, limited market incentives to invest in resilience to a 'socially optimal' level),

- ensures that work to enhance cyber and broader critical infrastructure resilience are publicly understood as two parts of a coherent whole, and that recommended policy options across both programmes complement each other and are informed by stakeholder feedback, and

- does not slow the delivery of measures to enhance cyber resilience (reflecting that it was not possible to deliver Cabinet a consultation document with well-considered options for cyber resilience reforms prior to April 2023).

7. If this option is preferred, a draft Cabinet paper for Ministerial consultation setting this work programme out and seeking agreement to commence of the first phase of consultation is available at Attachment F.

Table 2: Detailed project plan and key milestones for delivery of infrastructure resilience through two Bills (cyber milestones in blue, broader resilience milestones in green)

Prospective Date	Milestone
April 2023	Cabinet consideration and release of Phase 1 Discussion Document (need for regulatory reform)
s9(2)(f)(iv)	

Prospective Date	Milestone
s9(2)(f)(iv)	

Attachment E: Alternative Draft Cabinet Paper

Office of the Minister of National Security and Intelligence

Cabinet External Relations and Security Committee

Acting urgently to strengthen the resilience of New Zealand's critical infrastructure system – Release of Discussion Document

Proposal

1 This paper seeks agreement to:

1.1 progress, as a high priority, work on a single comprehensive legislative package to enhance the resilience of New Zealand's critical infrastructure to all hazards and threats – including natural hazards – to be introduced in early-2025; and

1.2 release the attached discussion document titled "Strengthening the Resilience of New Zealand's Critical Infrastructure System" ('Discussion Document').

Relation to government priorities

2 Resilient infrastructure is essential to ensure we are better prepared to protect our communities and withstand more extreme weather in the future. This is fundamental to the wellbeing of our people, and shaping New Zealand's economy to be more productive, more sustainable, and more equitable.

3 Regulatory reform to enhance critical infrastructure resilience, as proposed in this paper, will deliver on our commitments in the Infrastructure Action Plan, as part of our response to Rautaki Hanganga o Aotearoa, New Zealand's Infrastructure Strategy.

4 It would also complement the Government's commitment to improve the resilience of New Zealand's critical infrastructure, which features as one of the four key themes of Budget 2023. This includes funding of $6 billion for a new National Resilience Plan to build back better from Cyclone Gabrielle and support necessary investments to future proof our road, rail, telecommunications, and electricity networks.

Executive Summary

5 Critical infrastructures – like electricity, water, transport, and telecommunications networks – underpin almost all of New Zealand's economic activity and are essential to New Zealanders' daily life, health, security and wellbeing.

6 In September 2022, the Government agreed to commence public consultation in the first half of 2023 on the adequacy of New Zealand's current regulatory approach to delivering resilient critical infrastructure. In December 2022, Cabinet agreed to develop standalone legislation on cyber resilience for critical infrastructure for introduction in 2024. This reflected our view at that time that protecting critical infrastructure against cyber threats should be prioritised ahead of broader resilience, which would be legislated for in a subsequent Bill.

7 However, severe weather events over the summer, including storms in Auckland and Cyclone Gabrielle, highlighted our significant exposure to extreme weather events, as well as how underprepared our infrastructure system is to manage and respond to them. In this context, I consider that we must act now to strengthen our critical infrastructure system's resilience against all hazards and threats, as a high priority.

8 I therefore seek Cabinet's agreement to take forward this work through a single, comprehensive piece of legislation to be introduced in 2025.

9 I also seek agreement to release the attached Discussion Document and Summary Document (Attachments A and B, respectively) to commence the first phase of consultation. These documents outline the four megatrends already placing our critical infrastructure system under pressure, the shortcomings in our current regulatory approach that make these difficult to manage, and potential regulatory features that will strengthen resilience and futureproof our critical infrastructure.

Background

10 In September 2022, as part of its response to Te Waihanga's Infrastructure Strategy, the Government announced that in the first half of 2023 it would commence public consultation on whether regulatory reforms are required to manage compounding challenges to critical infrastructure resilience, including:

10.1 climate change

10.2 deteriorating geopolitical and national security environment

10.3 economic fragmentation

10.4 rapid advent and uptake of new technologies.

11 In December 2022 – and to reflect the urgent need for critical infrastructures to better manage cyber risks – Cabinet agreed to fast-track the delivery of cyber resilience initiatives, including enforceable minimum cyber security standards and other measures, such as mandatory reporting of cyber incidents [CAB-22-MIN-0586 refers]. Standalone legislation to implement these measures was intended to be introduced in 2024, with a second piece of legislation to manage other hazards and threats to infrastructure to be introduced in late-2025.

What is infrastructure resilience?

Resilience is the capacity of critical infrastructure entities – and the critical infrastructure system that they collectively constitute – to absorb a shock, recover from disruptions, adapt to changing conditions, and retain essentially the same function as before (even if delivered in a different way, or from a new location).

Resilience is not just the physical resilience of the asset - it requires organisations to have the right leadership and culture, networks and relationships, and organisational preparedness and processes in place before an event, so that they can recover and thrive afterwards. Resilience therefore includes 'building back better' from disasters.

Cyclone Gabrielle has demonstrated that New Zealand's critical infrastructure system is not meeting community expectations

12 The fragility of New Zealand's critical infrastructure system was evidenced by the January storms and flooding in Auckland and Northland, followed weeks later by Cyclone Gabrielle. Disruption to critical infrastructures was widespread and prolonged, affecting the lives and livelihoods of New Zealanders across the North Island. Infrastructure failures included significant communications, power, and payment system outages; the closure of Auckland International Airport; and collapse of many regionally and nationally significant transport links.

13 These events highlighted New Zealand's significant exposure to extreme weather, as well as how underprepared our infrastructure system is to manage and respond to them. They have also fuelled significant public calls for additional government intervention to enhance infrastructure resilience (particularly given that climate change will only increase the frequency, intensity, and consequences of such storms).

14 While the Government's December 2022 decision was prudent with the information then available, I consider that recent infrastructure failures have illustrated that there is a more urgent need to address other pressing risks to resilience, including climate change and natural hazards, than we had assumed last year.

15 I therefore seek Cabinet agreement to take forward all previously commissioned work on critical infrastructure resilience through a single, comprehensive piece of legislation to be introduced in early-2025 (that is, a Bill that will cover both cyber and broader resilience to manage all hazards and threats).

16 I consider that prioritising work on resilience against all hazards and threats for introduction in early-2025 would most effectively safeguard the investments that the Government and private sector will inject to building back better as part of the immediate recovery. Regulatory reform will best ensure that critical infrastructure owners and operators are subject to regulatory obligations, such as robust minimum standards, that leave us better prepared for future severe weather and national security events.

17 This approach will also:

17.1 reduce legislative and engagement complexity (including the risk of errors and stakeholder opposition), with government only having to design and communicate the need for a single reform; and

17.2 free additional drafting, Select Committee, and Parliamentary time through 2024 and 2025 for the government to progress work on other priorities.

The Emergency Management Bill will go some way to enhancing critical infrastructure resilience

18 The Emergency Management Bill that will be introduced into the House in early-June proposes to define 'critical infrastructure' as assets, systems, networks, and services that are necessary for the provision of public services and are essential to public safety, national security, economic security, or the functioning and stability of New

Zealand (LEG-22-MIN-0239 refers).[1] It provides for the Minister to recognise an entity as a critical infrastructure entity or a sector, or group of entities, as a critical infrastructure sector.

19 A wide variety of entities across New Zealand's economy and communities likely satisfy these requirements, including, but not limited to: energy, telecommunications, water services (for fresh, waste and storm water), government services (including emergency management, defence, intelligence, and government data), food and grocery providers, financial services and payments, cloud service and data storage providers, transport, and the health system.

20 The Bill will improve the resilience of New Zealand's infrastructure and infrastructure services before, during, and after an emergency by—

20.1 clarifying the roles and responsibilities of critical infrastructure providers in the emergency management system, including a general (but unenforceable) requirement to be resilient

20.2 requiring critical infrastructure entities to proactively, and on request, share information with the National Emergency Management Agency (NEMA), regulatory agencies, and Emergency Management Committees for monitoring and planning

20.3 requiring critical infrastructure entities to establish and publish their planning emergency levels of service

20.4 requiring annual reporting to the Director of Emergency Management, and the critical infrastructure entity's responsible agency.

Further regulatory reform will be required to deliver resilient infrastructure in line with what New Zealanders expect

21 While the changes proposed in the Emergency Management Bill are important, the urgent need for further Government action to enhance infrastructure resilience was clearly demonstrated by Cyclone Gabrielle, which left hundreds of thousands of New Zealanders without power or communications for a prolonged period.

22 The resilience of New Zealand's critical infrastructure system is under increasing pressure from climate change; heightened threats to our national security; economic fragmentation (which is making it harder and more expensive to secure critical goods and services); and technological change (which, while enhancing efficiency is also creating new vulnerabilities – including to cyber attacks).

23 Managing these kinds of complex and intersecting challenges requires shifting our focus away from regulating individual critical infrastructure sectors in isolation, to instead regulating all critical infrastructures as a deeply interconnected system. Such an approach, which would be consistent with global best practice, will support

[1] The current legislation (the Civil Defence Emergency Management Act 2002) currently applies resilience requirements to a subset of critical infrastructure entities referred to as 'lifeline utilities'. This includes entities involved in electricity generation and distribution, telecommunications network providers, water services providers, and the largest ports and airports.

wellbeing, underpin economic growth, and reduce fiscal pressures on the government associated with recovery from natural and other disasters.

24 Officials have identified four substantive changes required to deliver such a systems-based regulatory framework:

24.1 information-sharing on hazards and threats, vulnerabilities and mitigations, and ownership and control to enable critical infrastructure entities to maximise the amount of resilience gained for each dollar invested

24.2 robust, clear and enforceable minimum standards, to:

24.2.1 ensure that critical infrastructure owners and operators are prepared to manage different types of disruption irrespective of whether they relate to extreme weather events, cyber attacks, offshore conflicts that disrupt supply chains or other causes, and

24.2.2 reduce the risk of some owners and operators underinvesting and undercutting more resilient entities to the detriment of all New Zealanders and the robustness of the overall critical infrastructure system

24.3 new government powers, to directly intervene in critical infrastructure entities to manage particularly significant national security events

24.4 clear Ministerial and agency accountabilities for the resilience of the critical infrastructure system. Currently no agency or Minister has policy or regulatory responsibilities for the entire system, which has curtailed previous efforts to advance this essential work.

A systems-based regulatory approach will complement a range of other Government priorities

25 A new systems-based regulatory approach (particularly the introduction of minimum standards) requiring critical infrastructures to enhance their resilience against all hazards and threats will:

25.1 deliver on our commitments in the Infrastructure Action Plan to ensure that our infrastructure system is resilient in the face of climate change, natural disasters, and increasing extreme weather events;

25.2 reinforce our immediate efforts in Budget 2023 to build critical infrastructure back better (in some cases using public funds) by best ensuring that those assets are long lived; and

25.3 complement amendments to the resource management regime (which will better ensure that new critical infrastructures are not constructed in hazard-exposed areas).

26 This regulatory reform will also provide a legislative mechanism to deliver on our commitments under the National Adaptation Plan to:

26.1 design and implement a resilience standard or code for infrastructure;

26.2 develop tools and guidance that will support infrastructure owners and operators to undertake risk assessments; and

26.3 establish a model to assess infrastructure criticality and understand vulnerability.

Consultation and community partnership are essential to this work succeeding

27 As Cabinet previously discussed, the cost and complexity of any regulatory reform in relation to critical infrastructure requires extensive business and community consultation to build social license for successful intervention.

28 To best balance these competing tensions while having legislation ready for introduction in early-2025, I propose to take this work forward through two phases of public consultation:

28.1 **Phase one**: consultation on the limits of New Zealand's current regulatory approach to critical infrastructure resilience and the need for reform. Consistent with Cabinet's commitments, this is intended to commence in June 2023.

28.2 **Phase two**: consultation on specific reform options to enhance the resilience of critical infrastructure in the first half of 2024.

29 A phased approach to consultation is critical to obtaining the cross-community buy-in required for any new regulatory regime to be seen as credible and enduring. Without adequate consultation and social license for reform, there is a significant risk of alienating the industry and community bodies that we will need to partner with for successful implementation.

30 Further, given the number of entities that we will need to consult that are actively supporting recovery efforts, the proposed approach ensures that Māori and iwi, critical infrastructure owners and operators, lifeline groups, local government, and central government agencies do not have to make choices between engaging in this important process and managing the immediate rebuild.

Release of the Phase One discussion document: a frank conversation with the public about changing threats

31 Enhancing the resilience of New Zealand's critical infrastructures will impose significant costs on industry and the broader public.

32 It is therefore critical that the Government clearly and frankly articulate the objectives and principles underpinning the need for reform. This, and using early community feedback to inform the design of policy options, should elicit instructive feedback on the options themselves when they are presented to the public.

33 The attached Discussion Document (Attachment A) therefore articulates:

33.1 the **work programme's objective** (to protect wellbeing, and support sustainable and inclusive economic growth)

33.2 the **principles for reform**, including that any response will be consistent with the principles of the Treaty of Waitangi

33.3 the **need for reform** (as set out in paragraphs 22-24 above)

34 To complement this Discussion Document, and best ensure that this material is accessible to all members of our community, officials have also prepared a Summary Discussion Document (Attachment B).

35 I seek Cabinet's approval to release the Phase One Discussion Document and Summary Document for public consultation.

Next Steps

36 If endorsed for release, there will be around eight weeks for consultation on the first Discussion Document. This will be largely through written submissions, with officials also planning to hold town hall sessions and hui in person and online.

37 A timeframe with key milestones for this work programme is set out below.

Prospective Date	Milestone
June – August 2023	Consultation on Discussion Document on need for reform
s9(2)(f)(iv)	

Prospective Date	Milestone
s9(2)(f)(iv)	

Financial Implications

38 While this paper has no direct fiscal implications – as Cabinet noted in December 2022 – there will be potential financial implications associated with:

38.1 any policy changes arising from this work programme, particularly with the potential establishment of a system-wide regulator; and

38.2 complying with any new regulatory requirements that also apply to Crown-owned assets (for example, as could occur if certain defence assets were defined as critical infrastructure).

39 The scale of any costs and affected agencies will be dependent on the changes that are agreed to by Cabinet. This will likely include both implementation costs (if agency responsibilities shift or expand) and a general increase in the amount required to regulate the critical infrastructure system.

40 Greater detail regarding potential financial implications will be provided in further advice when policy decisions are sought from Cabinet.

Legislative Implications

41 There are no legislative implications arising directly from this paper.

42 There will be legislative implications associated with any policy changes arising from this work programme. Greater detail regarding any such implications will be provided in future Cabinet papers when policy decisions are sought.

Impact Analysis

Regulatory Impact Assessment

43 A regulatory impact assessment is not required at this stage. The Discussion Document incorporates elements of the regulatory impact assessment and an interim quality assurance panel have met to review this document. A full assessment will be prepared when policy decisions are sought.

Population Implications

44 This paper has no significant population implications.

45 Some policy options could have implications for the cost of accessing critical infrastructure services, which may disproportionately affect some population groups (such as Māori, recognising that this group tend to earn lower incomes and that the cost of essential, such as electricity or communications, make up a larger share of their household expenditure). This will be considered as part of any subsequent advice on options.

Human Rights

46 This paper has no human rights implications.

Consultation

47 The National Security Group in the Department of the Prime Minister and Cabinet prepared this Cabinet paper and the attached Discussion Document. There was widespread support for these proposals from all agencies consulted, including: Ministry of Foreign Affairs and Trade, Treasury, Ministry of Business, Innovation and Employment, Ministry of Transport, Department of Internal Affairs, Ministry for the Environment, Te Waihanga, Ministry of Defence, New Zealand Defence Force, New Zealand Security Intelligence Service, Government Communications Security Bureau, Commerce Commission, Electricity Authority, Reserve Bank of New Zealand, National Emergency Management Agency, and Land Information New Zealand.

48 The Policy Advisory Group in the Department of the Prime Minister and Cabinet were informed.

Communications

49 The Discussion Document will be made available on the Department of the Prime Minister and Cabinet's website. I also intend to issue a press release to accompany the release of these documents to emphasise the Government's focus on critical infrastructure resilience following Cyclone Gabrielle.

50 A programme of stakeholder engagement is planned to follow the release of the Discussion Document, including open access town-hall style meetings with industry experts and interested individuals in Wellington, Auckland and Christchurch. This will supplement written submissions, and best ensure we hear from all relevant groups, including: critical infrastructure owners and operators, industry associations, local government, lifeline councils and regional lifeline groups, sectoral regulators.

51 We will also seek early engagement with Māori and iwi, including through meeting with key Māori leaders who are well connected to their communities, and well placed to comment on the implications of this work for the wellbeing of those communities. This initial engagement will provide a platform for ongoing engagement on critical infrastructure resilience, consistent with our Te Tiriti o Waitangi obligations.

52 The topic being consulted on is likely to be of interest to disabled people who experience or feel disproportionate risk when natural disasters occur, and infrastructure fails. For this reason, the consultation process will need to be accessible to disabled people – the Discussion Document Summary will be published in an accessible format for the visually impaired, and officials will reach out to relevant peak bodies to best ensure that these communities are able to fully contribute to the national discussion on this topic. An analysis of the human rights impacts on populations, such as disabled people, will be provided as part of the regulatory impact assessment.

53 The Discussion Document identifies a range of limitations with New Zealand's current regulatory settings for critical infrastructure resilience and clearly signals the potential introduction of additional regulatory requirements to remediate these shortcomings. This will attract significant domestic interest, particularly from affected stakeholders, who will be concerned about the cost implications of any changes.

54 The Discussion Document will also likely attract international attention. This will include interest from overseas governments, from critical infrastructure entities that operate internationally, and from investors and investment funds with significant equity interests in our critical infrastructure system.

Proactive Release

55 Consistent with Cabinet Office circular CO(18)4, I intend to publish this Cabinet paper and the Discussion Document online within 30 business days of Cabinet making the decisions required by this paper, subject to redactions as appropriate under the Official Information Act 1982.

Recommendations

The Minister for National Security and Intelligence recommends that the Committee:

1 **Note** that in September 2022, the Government announced its intention to consult on the limitations of our current regulatory approach to enhancing infrastructure resilience of the first half of 2023.

2 **Note** that in December 2022, Cabinet agreed to fast-track measures to enhance the cyber resilience of critical infrastructure ahead of work on broader resilience.

3 **Agree**, in light of the broader vulnerabilities in New Zealand's critical infrastructure system exposed by Cyclone Gabrielle, to progress, as a high priority, the development of a single comprehensive piece of legislation to enhance critical infrastructure resilience against all hazards and threats for planned introduction in 2024.

4 **Agree** that the Minister for National Security and Intelligence release the attached Discussion Document and Summary Discussion Document to the public**.**

5 **Authorise** the Minister for National Security and Intelligence to approve minor amendments and refinements to the Discussion Document and Summary Discussion Document prior to public release.

6 **Note** that the public consultation period is intended to commence from early June 2023 and conclude in early August 2023, with officials to undertake a range of public meetings over this period.

7 **Note** that feedback on this Discussion Document will inform the development of options to enhance critical infrastructure resilience, ahead of final advice being provided to Cabinet in 2024.

8 **Note** that there will likely be financial and legislative implications associated with any policy changes arising from this further policy advice to Cabinet.

Authorised for lodgement

Rt Hon Chris Hipkins

Minister for National Security and Intelligence

Attachment A: Draft Phase One Discussion Document

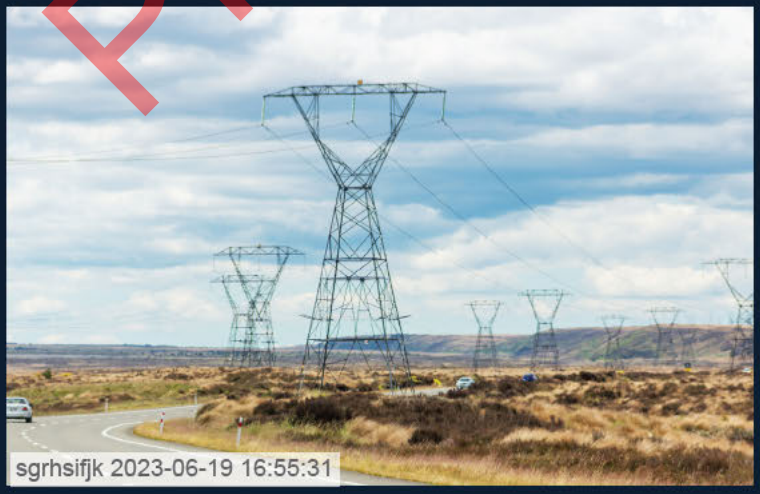
Attachment B: Draft Phase One Summary Discussion Document

Te Kāwanatanga o Aotearoa
New Zealand Government

June 2023

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

Summary discussion document



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

Aotearoa New Zealand is exposed to a wide range of hazards that can wreak havoc and devastation on lives and livelihoods. The destructive impact of earthquakes, volcanic eruptions, and extreme weather events are all too familiar for New Zealanders, as we recently experienced with Cyclone Gabrielle. Unfortunately, it is not just natural hazards that can trigger infrastructure failures, causing severe disruption to our society and economy. There are a range of other threats, such as cyber attacks, espionage, and terrorism, which can bring the delivery of crucial services to a halt.

Historically, we have tended to respond to infrastructure failures reasonably well, but as the recent power, communications, and water outages demonstrate, there is a pressing need to boost the resilience of our critical infrastructure system. This question only becomes more urgent when we consider the compounding risks posed by climate change, a deteriorating national security environment, fragmentation in the global economy, and rapid technological change.

For these reasons, the Government committed in its response to Rautaki Hanganga o Aotearoa, New Zealand's first Infrastructure Strategy, to consult on improving our current regulatory settings so we can deliver a robust and resilient critical infrastructure system.

This document, which provides a summary of the information available here, is the first step towards delivering on that commitment. It describes what we mean when we talk about critical infrastructure and resilience, and it outlines why a resilient critical infrastructure system matters for our country and people. It explores the trends that are going to make critical infrastructure resilience more important and the barriers that need to be addressed to deliver better outcomes that will benefit us all.

It is important that the steps we take to enhance critical infrastructure resilience are informed by a wide range of perspectives and designed in partnership with all New Zealanders. With your input, we can design a fit-for-purpose regulatory framework that ensures our critical infrastructure system is best positioned to manage the range of risks we face today and in the future.

As part of this consultation, the Government is seeking your views on:

a. the need to adapt our approach to critical infrastructure regulation, to create a more secure platform for sustainable, inclusive, and productive growth in the future

b. potential options for delivering a more resilient critical infrastructure system.

Feedback on this paper will inform the development of a subsequent consultation document on options for reform, planned for release in early 2024.

We invite individuals and organisations to provide their views on the ideas in this document. You can do this by:

attending a public meeting with details available at consultation.dpmc.govt.nz; and/or

completing a written submission and emailing it to infrastructureresilience@dpmc.govt.nz

or posting it to:

National Security Group
Department of the Prime Minister and Cabinet
Level 8 Executive Wing, Parliament Buildings,
Wellington 6021

The closing date for submissions is 14 July 2023.

Resilient critical infrastructure underpins our health and prosperity

What is critical infrastructure?

Critical infrastructures provide a range of services that are essential to the functioning of our society. Loss, damage or disruption to these services can adversely affect our economy, security and, most importantly, threaten lives and livelihoods.

What constitutes critical infrastructure is not currently defined in New Zealand law. However, there are a wide variety of entities across New Zealand that provide essential services, including the following sectors: energy, telecommunications, water services (for fresh, waste and storm water), food and grocery, financial services, digital services, transport and health.

These kind of entities, and the assets, systems, and networks that make them up are what we refer to as 'critical infrastructure'.

What is resilience?

Resilience is the capacity of our critical infrastructures – and the critical infrastructure system that they collectively make up – to absorb a shock, recover from disruptions, adapt to changing conditions, and retain essentially the same level of function as before.

Resilience is not just the physical characteristics of the asset – it also requires organisations to have the right kind of leadership and culture, networks and relationships, and organisational processes in place before an event, so that they can adapt, recover, and thrive afterwards.

Why is resilience important?

Private businesses, civil society, and government are all responsible for ensuring the continued functioning of our critical infrastructures – but the government has a particular interest for the following reasons.

Resilient infrastructure supports wellbeing.
Cyclone Gabrielle has clearly demonstrated how catastrophic the consequences of infrastructure failure can be, as disruptions flow across the critical infrastructure system and one outage triggers another. For example, widespread power outages can cause communications networks to fail, limiting people's ability to access critical emergency information and use payment systems (such as EFTPOS) to purchase essential food and medicines.

Resilient infrastructure supports economic growth.
Resilient critical infrastructure gives people confidence to take risks, invest, and grow their businesses. In an uncertain world defined by complex challenges like climate change and geopolitical competition, a resilient critical infrastructure system will attract productive and sustainable foreign investment.

Resilient infrastructure saves money.
Research by the New Zealand Institute of Economic Research has found that early investment in infrastructure resilience is cheaper than the cost to repair after an event. By investing early and reducing the Crown's significant – and growing – exposure to infrastructure failures, funding can be freed up to deliver on other government and community priorities.

Figure 1: Critical infrastructure can take many forms, including (but not limited to):

Currently, we have limited tools to ensure critical infrastructure resilience

To date, the New Zealand government has not taken a comprehensive or coordinated approach to critical infrastructure regulation. No agency has policy or regulatory responsibility for New Zealand's critical infrastructure system.

Instead, New Zealand's regulatory approach has been focussed on protecting critical infrastructure assets within a given sector – for example, ports, airports, telecommunication networks, power stations, and water plants are each regulated in isolation.

Primary responsibility for determining what level of resilience is appropriate currently sits with critical infrastructure owners and operators, with their decisions typically informed by:

- pressure from consumers and other critical infrastructure owners and operators, to provide a minimum level of reliable service
- specific regulatory requirements where they exist (for example, those that the Electricity Authority imposes on energy market participants).

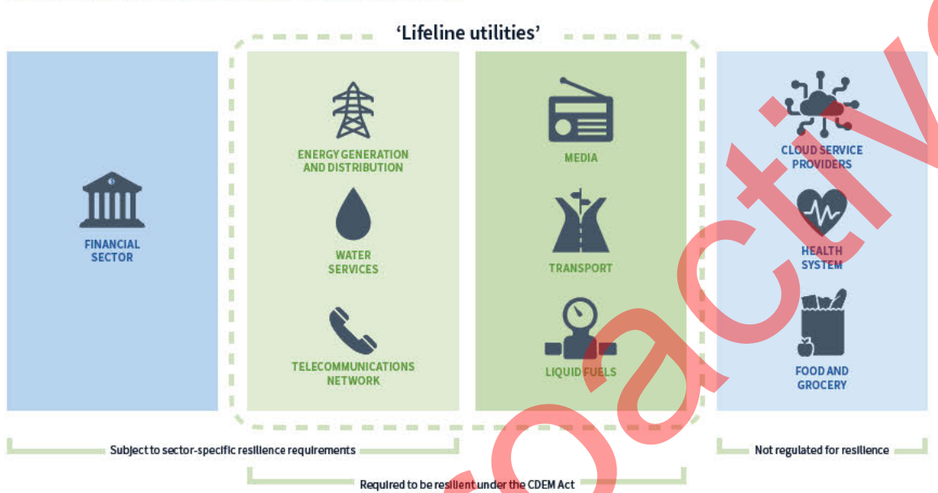
There are limited exceptions to this sector-level approach, most clearly in relation to emergency preparedness and response through the Civil Defence and Emergency Management (CDEM) Act 2002. This Act requires 'lifeline utilities' (a limited subset of our critical infrastructure) to "function to the fullest possible extent" following an emergency.

The diagram below provides a simplified overview of New Zealand's approach to regulating infrastructure resilience.

This sector-by-sector approach to delivering resilient critical infrastructure has historically served us reasonably well. However, its decentralised nature has meant that:

a. insufficient attention has been paid to building a shared understanding of risks, vulnerabilities, critical infrastructure interdependencies, and mitigations
b. we lack consistent resilience standards to manage risks to our critical infrastructure system
c. we are unable to mitigate and remediate weaknesses within that system in a coordinated way.

Figure 2: Simplified overview of statutory resilience requirements.



We urgently need a more resilient critical infrastructure system

New Zealand's environment and geography mean that our critical infrastructures are exposed to a broader and more consequential range of potential shocks than any other highly developed country. Our geography makes us particularly prone to a range of natural hazards, while we remain susceptible to other risks that are not geographically confined, such as cyber attacks.

Lloyds' assesses that New Zealand has the second highest disaster loss risk in the world.

Japan, another country on the Pacific Ring of Fire, is the only other high-income country in the top ten (with risks less than half of New Zealand's).

The United Nations Disaster Risk Reduction database highlights that New Zealand's natural hazard risks are unusually weighted towards low frequency and comparatively unpredictable but inevitable high impact events (also known as 'high impact but rare events'). In particular, earthquakes and tsunamis, but also volcanic eruptions.

Global megatrends pose challenges for our critical infrastructure system

Four global megatrends are placing increased pressure on our critical infrastructure system. These trends will present new challenges, amplify existing vulnerabilities, and heighten the risk of infrastructure failure.

Megatrend #1: Climate Change

Climate change will have a range of direct and indirect effects. Direct impacts include:

- more extreme and frequent weather events
- more frequent and severe droughts
- sea level rise.

Indirect impacts include:

- continued transformation of electricity generation and distribution
- changing consumer demands and preferences.

Megatrend #2: Deteriorating national security environment

New Zealand faces a more challenging strategic environment than it has for decades.

This increases the risk of deliberate attacks on infrastructure, including through:

- espionage
- sabotage
- cyber attacks.

Megatrend #3: Economic fragmentation

Geopolitical competition has put the rules that underpin global trade under increasing pressure. This means that:

- countries are more willing to exploit each other for strategic gains (for example, the use of trade or import restrictions)
- supply chains are less resilient
- divergent technology standards are emerging across countries and groups of countries, increasing costs and decreasing product availability.

Megatrend #4: Rapid technological change

Rapid technological change offers efficiencies and other opportunities but can also amplify risks. For example, the uptake of new technologies has contributed to:

- the emergence of new types of critical infrastructure that are not subject to any regulation
- increased vulnerabilities to cyber attack
- more links between critical infrastructures, causing failures to spill further across the critical infrastructure system.

The growing risks to our critical infrastructure system

New Zealand's regulatory approach is increasingly out of step with global best practice.

A range of countries and regions – including Australia and the European Union – are shifting from sector-level regulations to a system-wide regulatory approach. Such an approach allows requirements to be set evenly across all critical infrastructure sectors to manage the risk that weakness in any critical infrastructure creates systemic weaknesses across the critical infrastructure system.

In light of cascading and prolonged infrastructure outages affecting large numbers of New Zealanders, it is clear that change is required. We are seeking your views on what you think is required to strengthen the resilience of our critical infrastructure system, with a focus on addressing the following **four barriers** to resilience.

- Ad hoc and inadequate information sharing on issues fundamental to infrastructure resilience
- Limited tools to manage threats to our national security
- No enforceable minimum resilience standards
- Unclear government and private sector accountabilities for delivering critical infrastructure resilience

The costs of lifting infrastructure resilience

The government is highly conscious of cost-of-living pressures and that the investments required to deliver more resilient critical infrastructure may be passed onto New Zealanders through higher prices for goods and services.

In designing options for reform, the Government would seek to lift resilience at least-cost through:

- focussing, at least initially, on 'lifting the resilience floor', particularly for critical infrastructures not subject to regulation – recognising that many owners and operators are already investing a lot in their resilience
- timing the introduction of any new regulatory requirements to align with investment plans, to the extent possible
- considering direct support for more vulnerable New Zealanders to ensure that boosting resilience does not reduce access to essential services.

There are four potential barriers to delivering a more resilient critical infrastructure system

Barrier 1: Information sharing is ad hoc, rather than comprehensive and systematic

Why is information sharing important?

The exchange of information on hazards, threats, outages, and near-misses is essential to enable:

- critical infrastructures to target resilience investments towards their most important assets and managing the most significant risks
- regulators to develop proportionate settings that are fit for purpose.

How well is information shared between government and critical infrastructure owners and operators currently?

Information sharing between government and infrastructure owners and operators is fragmented and often ad hoc, with only certain types of risk assessment information shared publicly (for instance, on the likelihood of natural hazards or the effects of climate change).

This, in part, reflects that New Zealand has no secure platform for the exchange of sensitive information.

Will any reforms already underway fix this problem?

No. there are no mechanisms currently planned to better ensure the timely flow of information on specific threats, including those that may undermine New Zealand's national security.

Transparency around certain issues will be increased through the establishment of the Natural Hazards Commission and the release of the first National Security Strategy (outlining national security risks).

Barrier 3: There are limited tools to manage national security risks

Why does the government need tools to manage national security threats to our critical infrastructure system?

New Zealand faces a deteriorating national security environment, and our critical infrastructure system is an attractive target for espionage, sabotage, cyber attacks, and other types of interference.

The government has a unique understanding of this environment – and given its access to sophisticated intelligence and cyber capabilities – will often be best qualified to detect and disrupt such threats. In some instances, the government may need to take action quickly to mitigate or respond to threats.

Clear direction and intervention powers, such as those adopted by Australia to manage significant national security threats, could support this.

How well can the government intervene to manage such risks currently?

The government does have some tools to intervene to support the response to a significant cyber threat to New Zealand's critical infrastructure, but not any other type of threat.

Will any reforms already underway fix this problem?

No.

Barrier 2: There are no enforceable minimum resilience standards

Why are enforceable minimum resilience standards important?

Critical infrastructures cannot operate without services provided by other critical infrastructures (for example, many power grids rely on telecommunications networks to function). Minimum resilience standards can:

- mitigate the risks that vulnerabilities in any critical infrastructure asset could pose to the entire system's stability
- align investment in resilience to the level that New Zealanders expect (given limited market incentives to do so)
- counteract cognitive biases that lead to underinvestment in managing high impact but rare events that we are exposed to.

How effective are minimum resilience standards currently?

New Zealand has no mechanism to set enforceable and consistent minimum resilience standards for all critical infrastructure system. While the CDEM Act does impose a general requirement on lifeline utilities to be resilient against all hazards and threats, this requirement is unenforceable.

Will any reforms already underway fix this problem?

No. Through reform of the emergency management system, the Government proposes to extend the requirement to be resilient to a wider set of critical infrastructures. However, compliance cannot be verified or enforced.

Barrier 4: There are unclear accountabilities for system resilience in government and across the community

Why are clear accountabilities for the resilience of the system helpful?

Strengthening resilience requires coherent and well-understood accountabilities. This includes providing clarity on the responsibilities of critical infrastructure owners and operators as well as responsibilities across government for delivering a resilient critical infrastructure system.

Recognising this, other countries are establishing agencies with an exclusive focus on critical infrastructure. These agencies tend to be responsible for:

- developing and maintaining resilience policies and standards
- monitoring the implementation of these standards and taking enforcement action if they are not met.

How clear are accountabilities for delivering a resilient infrastructure system currently?

No agency or Minister has responsibility for developing policy applicable across the critical infrastructure system, including in relation to system resilience.

Similarly, no regulator has powers to monitor or enforce minimum standards. This precludes us from verifying that critical infrastructure is as resilient as the New Zealand public might expect.

Will any reforms already underway fix this problem?

No.

Cover photo credits (istock.com):
Cranes: BrianScantlebury | Airport: GordonImages | Powerlines: MollyNZ | Windmills: xiaoke chen

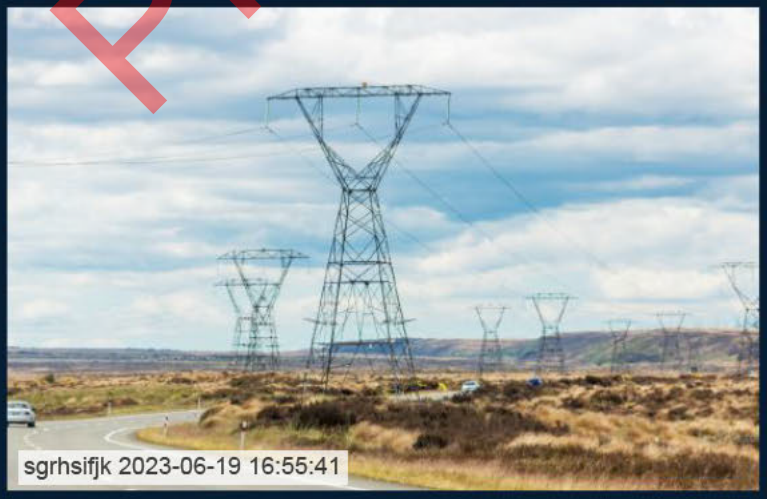
Te Kāwanatanga o Aotearoa
New Zealand Government

June 2023

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

Ensuring Aotearoa New Zealand has a secure platform for a productive, sustainable, and inclusive economy

Discussion Document



Department of the Prime Minister and Cabinet (DPMC)

DPMC occupies a unique position at the centre of Aotearoa New Zealand's system of democratic government. Its purpose is to advance an ambitious, resilient, and well-governed Aotearoa New Zealand.

More information

Information, examples and answers to your questions about the topics covered here can be found on our website www.dpmc.govt.nz

Media enquiries can be directed to media@dpmc.govt.nz

Disclaimer

This document is a guide only. It should not be used as a substitute for legislation or legal advice. DPMC is not responsible for the results of any actions taken on the basis of information in this document, or for any errors or omissions.

ISBN: 978-0-947520-39-7 (online)

Cover photo credits (istock.com):
Cranes: BrianScantlebury | Airport: GordonImages | Powerlines: MollyNZ | Windmills: xiaoke chen

Contents

Ministerial foreword

New Zealanders are all too familiar with critical infrastructure failures. We have a complicated geography and face high earthquake, volcanic and tsunami risks. For our society to continue functioning in the face of natural hazards and other threats, we need to adapt our regulatory settings to enhance critical infrastructure resilience.

Often unseen when working well, we rely on critical infrastructures like power, telecommunications, transport, water services, and the financial sector every day. They underpin our health, prosperity, and ability to live fulfilling lives.

Unfortunately, the risks facing our critical infrastructures are changing and increasing.

We live in a more complex national security environment. Climate change is increasing the frequency and impact of severe weather events. Cyber attacks threaten – and do – disrupt the delivery of critical services. Meanwhile, COVID-19 exposed underlying fragilities in the economic structures we rely on. Ongoing supply chain disruptions are a daily reminder of this.

New technologies are also deepening the connections between critical infrastructures, making them more reliant on one another but also more vulnerable. In this changed environment, weakness in any of our critical infrastructures can manifest as weakness in all of our critical infrastructures.

Aotearoa New Zealand's success in the 21st century will depend on our ability to withstand, respond to, and recover from complex and cascading infrastructure failures.

This discussion document builds on Rautaki Hanganga o Aotearoa, New Zealand's first Infrastructure Strategy, produced by Te Waihanga – New Zealand's Infrastructure Commission.

In the wake of the devastation wrought by Cyclone Gabrielle, we are seeking your views on the need – and potential mechanisms – to improve our approach to infrastructure resilience.

This recognises that our communities, businesses, and institutions rely on one another for success – and that we have a shared interest in the strength of the critical infrastructure ecosystem that underpins this.

This will require transformational change and affect all of us. So, it is important that our choices are informed by a wide range of perspectives and designed in partnership with all New Zealanders.

I encourage you to provide your views on the ideas presented in this discussion document. We must urgently work together to tackle the pressing challenges of the 21st century.

Rt Hon Chris Hipkins
Prime Minister and Minister for National Security and Intelligence

What is this consultation document about?

1. Critical infrastructures – like electricity grids, water systems and telecommunications networks – underpin almost all of Aotearoa New Zealand's economic activity and are essential to New Zealanders' health and wellbeing.

2. This consultation document seeks your views on the need to reform New Zealand's existing regulatory approach to delivering a resilient critical infrastructure system, and the shortcomings that need to be addressed to strengthen resilience.

3. In 2019, the Government established Te Waihanga – the Infrastructure Commission – with the goal of lifting infrastructure planning and delivery to a more strategic level. This is intended to improve New Zealand's long-term economic performance and social wellbeing.

4. One of the ways that Te Waihanga delivers on this objective is by providing the government with an Infrastructure Strategy every five years, with its view on:

   a. the ability of existing infrastructure to meet community expectations for the next 30 years

   b. priorities for infrastructure for the next 30 years.

5. Rautaki Hanganga o Aotearoa 2022-2052, New Zealand's first Infrastructure Strategy was tabled in New Zealand's Parliament on 3 May 2022.[1] In this, Te Waihanga notes New Zealand's vulnerability to a wide range of shocks and stresses – from natural hazards such as earthquakes, to climate change, terrorism, and cyber attacks. While we are not always able to prevent these shocks, the Strategy says we can and should do more to prepare for them to make our infrastructure more resilient.

6. To enhance the resilience of critical infrastructure, Te Waihanga recommended that steps be taken to achieve the following strategic direction:

   a. a common definition of what counts as critical infrastructure and a framework for identifying which infrastructures are most critical

   b. a shared understanding among critical infrastructure entities and the government of hazards and threats affecting infrastructure systems

   c. a coordinated approach to managing risks across the infrastructure system which accounts for the growing dependencies and interdependencies within and between infrastructures.

7. In its response to the Infrastructure Strategy, the New Zealand Government supported Te Waihanga's assessment in full.[2]

[1] See: https://strategy.tewaihanga.govt.nz/strategy.

[2] See: https://www.treasury.govt.nz/publications/commissioned-report/government-response-rautaki-hanganga-o-aotearoa-new-zealand-infrastructure-strategy.

8. While our historic approach to infrastructure resilience has served New Zealand well, the infrastructure system of today is markedly different to the systems of 30 years ago. Our expectations are different too, as critical infrastructures continue to underpin the success of a growing share of our economy. We should expect the next 30 years to see similar changes, with critical infrastructures becoming increasingly complex and connected.

9. Given these changes to the make-up and operation of our infrastructure system, and the challenges that are increasing the system's vulnerabilities, this consultation document seeks to:

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

   b. start an open conversation with New Zealanders about what steps we should take to enhance critical infrastructure resilience.

10. Feedback on this paper will inform subsequent consultation in early 2024, exploring in more detail the options identified for enhancing infrastructure resilience to all hazards and threats.

11. In some places, this document describes parts of New Zealand's regulatory environment and requirements, to provide context and support you to provide your views. These are generalised descriptions, and not intended to be relied on when determining your potential legal obligations. For legal or other expert advice, you should contact a professional advisor.

12. A glossary of terms used in this discussion document can be found at Appendix A.

How can you contribute?

13. Consultation is open on critical infrastructure resilience from **13 June to 8 August 2023**.

14. We want to hear views from individuals and organisations on the ideas in this document. This discussion document is primarily aimed at critical infrastructure owners and operators, who would be directly affected by regulatory reforms to enhance the resilience of critical infrastructure. In particular, Section 2 on how to address current barriers to resilience is designed to draw on the specialist views of industry stakeholders. We also welcome input from individuals and communities, who of course are directly affected by the resilience of critical infrastructure. We are particularly interested to understand how you expect the system to perform (see section 1, page 9 for further detail).

15. You can provide your feedback by:

    a. attending a public meeting (with details available on DPMC's website); and/or

    b. completing a written submission online on DPMC's website, by emailing it to infrastructureresilience@dpmc.govt.nz, or posting it to:

       National Security Group
       Department of the Prime Minister and Cabinet
       Level 8 Executive Wing, Parliament Buildings, Wellington 6011

16. Your submission may respond to any or all of the issues we ask about. The Government is particularly interested in your views on:

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

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

17. To support your response, each section of this document includes sample questions. Appendix C provides a complete list of these questions.

18. The questions are designed to help guide your feedback, but you should not feel restricted to answering these questions or using this format.

19. Officials will analyse all submissions that are received by the closing date and consider them in developing potential options for reform to enhance the resilience of New Zealand's infrastructure.

20. You can find more information about the public meetings and this reform on the DPMC website at https://consultation.dpmc.govt.nz/national-security-group/critical-infrastructure-phase-1-consultation.

How your submission will be used and your rights

21. Submissions will be used for the purpose of helping us develop policy advice in relation to this reform. All submissions are intended to be published in PDF format on the DPMC website. Additionally, submissions provided to DPMC, whether published or not, may be required to be disclosed in response to individuals' requests under the Official Information Act 1982.

22. If your submission contains confidential information, or you do not want it published for any other reason, please:

    a. indicate this on the front of the submission, and mark any confidential information clearly

    b. if practicable, provide a separate version that excludes the relevant information, which officials can then publish on the DPMC website.

23. If you are an individual, as opposed to an organisation, DPMC will consider removing your personal details from the submission. If you have any objection to us publishing or releasing your personal details, or any other information in your submission, please state that clearly in the cover letter or email that goes with your submission, including the parts that you consider should be withheld and your reasons for withholding the information. DPMC will take your objections into account and consult relevant submitters when responding to requests under the Official Information Act 1982.

24. You also have rights under the Privacy Act 2020 in relation to the way that DPMC (and other government agencies) can collect, use, and disclose information about you and individuals referred to in your submission. In particular, you have the right to access personal information about you that DPMC holds and to seek any corrections.

Prelude: What principles would underpin any potential reform and how would reform options be assessed?

This section sets out the objective of this programme: enhancing critical infrastructure resilience to protect New Zealanders' wellbeing and to create additional opportunities for economic growth.

The section also describes the policy principles that will underpin any options that are developed as well as the criteria for evaluating them. Criteria relate to:

- **effectiveness:** will it enhance resilience?
- **cost:** what direct and indirect costs will options impose on the economy?
- **complexity:** how does the option impact the regulatory system's complexity?

Your feedback is sought on each of these matters.

Objectives for this work programme and discussion document

1. A resilient critical infrastructure system enables all New Zealanders, and the communities that they reside in, to participate in society and the economy with confidence that their essential needs will be met.

2. This **work programme's objective** is to enhance the resilience of New Zealand's critical infrastructure system to all hazards and threats, both natural (such as earthquakes and floods) and man-made (such as cyber security incidents and espionage). This would put us in a better position to:

   a. protect New Zealand's wellbeing, by reducing outages that undermine New Zealanders' health and living standards

   b. support sustainable and inclusive growth in New Zealand's wellbeing, by enhancing New Zealand's attractiveness to investment and business formation.

3. The Government recognises, however, that resilience is one of many competing objectives for the infrastructure system. These include efficiency; affordability (given implications for equal access to these services); sustainability; and high levels of competition between critical infrastructure entities.[3]

4. Enhancing resilience can be in tension with these other objectives. Recognising this, the government is committed to working with critical infrastructure owners and operators and the general public to identify and deliver the 'socially optimal' level of resilience.[4]

[3] There are limited exceptions to this, such as in the telecommunications and energy sectors, where natural monopolies are consequently subject to price regulation.

[4] This is the level of resilience that it is rational to deliver when accounting for all the costs of infrastructure failure (not just those borne by individual service providers) and the risks of those failures occurring.

5. This level of resilience is not, and cannot be, a 'point in time' destination. Resilience is something that must be continuously invested in to make constant improvements at the knowledge, asset, process, organisational, and community level.

6. Additional objectives for this work programme include:

    a. improving New Zealand's regulatory approach to the critical infrastructure system so it is dynamic and better able to adjust to technological and other developments that change what kind of infrastructure is considered 'critical'

    b. extending New Zealand's regulatory approach to cover cyber risks and impose clear, consistent standards to protect critical assets against risks to information and operational technology

    c. enhancing alignment between other regulatory regimes relevant to critical infrastructure resilience, including (but not limited to) resource management, emergency management, and climate change response

    d. improving awareness of the range of hazards and threats facing New Zealand's infrastructure system.

7. The specific **objectives for this first discussion document** are related but narrower in scope:

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

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

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

Principles underpinning this work programme

8. Throughout this work programme, the Government will be guided by the principles listed below.

    a. Any reform will be consistent with the principles of Te Tiriti o Waitangi and other domestic policy obligations.

    b. Any response will apply to all critical infrastructures equally, irrespective of their ownership, consistent with our international obligations. This reflects the fact that critical infrastructure faces a range of hazards and threats, irrespective of an asset's ownership.

    c. Critical infrastructure owners and operators are best placed to understand and manage the risks facing their organisations, but government has a responsibility to partner with industry to:

        i. ensure that owners and operators have a good understanding of the hazards and threats that they face

        ii. support owners and operators in making rational investments to enhance resilience

iii. set minimum standards[5] in areas where market forces do not deliver the optimal level of resilience.

d. Resilience should be enhanced at the least cost to businesses, consumers, and government by:

i. using non-regulatory mechanisms (such as information sharing) wherever possible, to better target and prioritise investments in resilience, to deliver optimal improvements for each dollar spent

ii. taking advantage of existing sector-based regulatory regimes wherever possible, by identifying and filling gaps in the existing regulatory landscape, rather than replacing or usurping them

iii. developing proposals that build on existing and forthcoming laws (to the extent possible)

iv. ensuring that any new potential regulatory approach is proportionate and dynamic. It should be able to respond to changing risks, technologies, and consumer preferences, to ensure that legislation does not become rapidly outdated or otherwise no longer fit for purpose.

e. The costs of enhancing resilience should, where possible, be paid by those who benefit from those investments.[6]

Criteria for assessing options

9. This discussion document does not evaluate the benefits and costs of specific options for amending New Zealand's regulatory and organisational settings for critical infrastructure resilience. However, it is the government's intention that feedback on this document will inform the development of options for regulatory reform, which will then be presented for a subsequent round of public consultation.

10. As part of the next phase of this work (and consistent with the programme objectives and underpinning principles), the government proposes to test each option against the three criteria listed below.

a. **Criterion A: How well does the option enhance infrastructure resilience?**

This question considers how effectively an option enhances resilience across all critical infrastructure sectors.

b. **Criterion B: How does the option change regulatory burden and regulatory certainty across the community?**

This question considers an option's regulatory burden on critical infrastructure owners and operators. An example of this cost would be an option that creates new information-sharing obligations for owners and operators.

This question also includes consideration of:

i. the degree of certainty that an option will provide for affected entities as to their obligations and how to meet them, recognising that navigating uncertainty increases compliance costs for critical infrastructure owners and operators

[5] Such standards can take many forms, including principles that must be met and processes that must be adopted.

[6] Te Waihanga, 2022, "Infrastructure Strategy", page 123. Available at: https://media.umbraco.io/te-waihanga-30-year-strategy/1sfe0qra/rautaki-hanganga-o-aotearoa-new-zealand-infrastructure-strategy.pdf.

ii. any change in the number of regulatory relationships or 'touch points' that an option will create for critical infrastructure owners and operators, recognising that this will directly increase compliance costs.

This question is important, because any increase in regulatory burden will result in increased costs for end-users, increased costs for government, and/or lower quality services.

c. **Criterion C: How does the option change the regulatory system's complexity?**

This question considers:

i. any additional expenses the government may incur to administer an option on an ongoing basis, including expenses associated with a need for additional coordination between government regulators

ii. any costs associated with an option's implementation (eg. the establishment of a new entity or shifting of responsibilities between existing government agencies).

The government wishes to keep this cost low, because any additional spending to regulate the critical infrastructure system will have trade-offs for existing or new government programmes that could be funded in all New Zealanders' interests.

The Government would like your views

- Does more need to be done to improve the resilience of New Zealand's critical infrastructure system?
- Have you had direct experience of critical infrastructure failures, and if so, how has this affected you?
- How would you expect a resilient critical infrastructure system to perform during adverse events?
- Would you be willing to pay higher prices for a more resilient and reliable critical infrastructure system?
- The work programme's objective is to enhance the resilience of New Zealand's critical infrastructure system to all hazards and threats, with the intent of protecting New Zealand's wellbeing, and supporting sustainable and inclusive economic growth. Do you agree with these objectives? If not, what changes would you propose?
- Do you agreed with the proposed criteria for assessing reform options? If not, what changes you would propose?

Section 1: Background and context

This section defines what is meant by:

- critical infrastructure (in general terms, assets, systems networks, and services that are essential to our safety, security, and economy)
- resilience (which does not just measure an entity's ability to absorb a stress or shock – like an earthquake – but also accounts for an entity's ability to recover).

The section then describes:

- **society's interests in a resilient critical infrastructure system**, which is essential to protecting New Zealanders' lives and livelihoods, but also is important for economic growth and reducing the amount that government must spend on recovery from events
- the government's current **approach to delivering resilient critical infrastructure**, which often differs across regulated sectors and is very limited within the many sectors that are not regulated
- the **four megatrends that pose new risks to New Zealand's critical infrastructure** and may justify a different regulatory approach. These are: climate change, growing national security risks, a fragmented global economy, and technological change
- the **financial implications of enhancing critical infrastructure resilience** and ways to potentially reduce incurred costs over time**.** This recognises that while enhancing infrastructure resilience will save New Zealand money in the long run, it will increase costs in the short term for individual New Zealanders, critical infrastructure owners and operators, and the government.

Your feedback is sought on each of these matters.

What is critical infrastructure?

11. Critical infrastructures provide a range of services that are essential to the functioning of our society, the economy, public safety and security, and the provision of public services. Loss, damage or disruption to these entities may severely prejudice the provision of essential services to the public, national security, public safety, the maintenance of law and order, and, most importantly, may threaten lives and livelihoods.

12. What constitutes critical infrastructure is not currently defined in New Zealand law, however, there are a wide variety of entities across New Zealand that provide essential services, including, but not limited to: energy, telecommunications, water services (for fresh, waste and storm water), government services (including emergency management, defence, intelligence, and government data), food and grocery providers, financial services and payments, cloud service and data storage providers, transport, and the health system.

13. A definition for critical infrastructure is included in the Emergency Management Bill. This will expand upon those entities already listed as 'lifeline utilities' under the current Civil Defence Emergency Management Act 2002 (CDEM Act). When this document refers to 'critical infrastructures', it is referring to the assets, systems and networks that will be designated as such through the implementation of the Emergency Management Bill.

14. This consultation process is therefore focussed on seeking feedback on the regulatory reforms that are proposed to apply to those entities, rather than what criteria should be used to designate entities as critical infrastructure.

What is resilience and why is it important?

What is meant by resilience for critical infrastructures?

15. Resilience[7] is the capacity of each critical infrastructure – and the critical infrastructure system that they make up – to absorb a shock; recover from disruptions; adapt to changing conditions; and retain essentially the same function as they had before.

16. Resilience is not just about physical assets – it is a strategic capability. It requires organisations to have the right leadership and culture, networks and relationships, and organisational processes[8] in place before an event, so that they can recover and thrive afterwards.

Defining stresses and shocks

Infrastructure resilience is measured by the infrastructure system's ability to absorb, adapt, and recover from stresses and shocks. Shocks are sudden, sharp events that have the potential to disrupt infrastructure services, such as earthquakes or cyber attacks.

Stresses, in contrast, are longer-term, chronic conditions that negatively affect physical assets, operational processes and organisations by:

- increasing the likelihood of a shock occurring
- increasing the impact of a shock were it to occur.[9]

Defining resilience domains

For critical infrastructures, resilience can be considered across five domains:

- **physical resilience** (the resilience of premises and other physical assets)
- **cyber and information system resilience** (the resilience of information and information systems – including systems that process personal data)
- **personnel security** (the ability to manage insider security risks from staff and contractors)
- **supply chain resilience** (continued access to critical goods and services irrespective of operational disruptions or changes in the global or domestic environment)
- **procurement security** (ensuring that acquired goods and services that do not pose security risks, both at the point of acquisition and over the life of the contract).

Achieving resilience across each of these domains will require investment in assets, but also processes and relationships, with the ratio between these differing across them.

---

7 OECD, 2019, "Good Governance for Critical Infrastructure Resilience", OECD Reviews of Risk Management Policies, OECD Publishing, Paris.

8 New Zealand's 'Resilient Organisations' have – drawing on academic research – developed a list of capabilities that resilient organisations should have, expanding on those mentioned here. Additional information can be found at: https://www.resorgs.org.nz/about-resorgs/what-is-organisational-resilience/.

9 Infrastructure Australia and Infrastructure New South Wales, 2021, "A pathway to infrastructure resilience: Advisory Paper 1: opportunities for systemic change", page 1. Available at: https://www.infrastructureaustralia.gov.au/publications/pathway-infrastructure-resilience-0.

17. Resilience is distinct from the ability to simply absorb shocks. Instead, resilience is both about absorbing shocks, but also having the capacity to adapt to those shocks and rapidly recover, even if that means providing services in a new way. That is, the most resilient organisation is not necessarily the one with the 'hardiest' assets, but the one that can continue to deliver services to communities most consistently. An organisation that uses less robust assets that are easily replaceable may be more resilient from a service delivery perspective than one that relies on highly engineered assets that take a long time to replace when they fail.

18. This focus on innovation – to 'bounce forward' from a crisis – is one of the reasons why governments across the world are increasingly focussed on how to build and sustain resilient economic systems. For example, in 2021, in the face of increasing geopolitical tensions and COVID-19, the Organisation for Economic Co-operation and Development (OECD) was commissioned to report on how to foster greater resilience in a world of open and integrated markets.[10]

19. This document has been developed in the same vein, with the goal of putting New Zealand in a position where it can both absorb, and take advantage of, the challenges of the future to further all New Zealanders' interests.

20. This will require a significant shift. "New Zealand's Infrastructure Challenge", released in 2021, identified that New Zealand had a significant historic infrastructure deficit of $104 billion – with infrastructure investment not keeping pace with the needs of our growing population – and without policy change was on track to add another $106 billion to this figure over the next thirty years. Investments to enhance service quality, which includes resilience, accounted for approximately $4.25 billion of this unbudgeted for total.[11]

What is New Zealand's interest in a resilient infrastructure system?

21. All New Zealanders have a direct interest in a resilient critical infrastructure system. This is because it supports wellbeing, provides a solid foundation for economic growth, and saves taxpayers and the broader economy money in the long term.

Infrastructure failures can have catastrophic consequences

22. As recently demonstrated, the consequences of infrastructure failures can be devastating for our communities.

23. The interdependent nature of our infrastructures means that disruption in one sector can quickly cascade and degrade services in another. For example, a prolonged electricity outage would significantly affect the performance of our telecommunications sector; limit communications, payments, and transport flows; and severely impair the ability of businesses and the government to function. For example, during Cyclone Gabrielle power outages and telecommunications outages quickly limited citizens' access to payments systems (including Automatic Teller Machines), reducing their ability to access critical supplies and up-to-date information during the emergency.

24. In all cases, such disruptions undermine trust in New Zealand's government and institutions. However, at their worst, such disruptions can cause New Zealanders to lose their lives or livelihoods. They can

---

10 See: https://www.oecd.org/newsroom/OECD-G7-Report-Fostering-Economic-Resilience-in-a-World-of-Open-and-Integrated-Markets.pdf.

11 Sense Partners, 2021, "New Zealand's Infrastructure Challenge: Quantifying the gap and path to close it", pp 1-2. Available at: https://www.tewaihanga.govt.nz/assets/Uploads/Infrastructure-Challenge-Report.pdf .

also trigger an economic contraction that permanently disrupts business growth, career pathways and life trajectories, even with significant government support.[12] For example:

a. Treasury has estimated the cost of asset damage alone from Auckland's flood and Cyclone Gabrielle at between $9 billion and $14.5 billion alone. This does not include the cost of economic disruption for businesses and workers that were unable to operate for a sustained period, or the longer-term costs of repairing and rebuilding infrastructure.

b. From a cyber perspective, the Australian Government estimated in 2020 that a four-week interruption to digital infrastructures caused by a significant cyber incident would cost their economy approximately 1.5 per cent of Gross Domestic Product.[13] The scale of costs would likely be similar in New Zealand (that is, around $6 billion).

Resilient critical infrastructures underpin economic growth and reduce fiscal pressures on government

25. As climate change and associated weather events intensify, and other risks to infrastructure – such as cyber attacks – grow, resilience will also become an important economic advantage. Investments in critical infrastructure resilience today will help to attract the business investment we need to support productive, sustainable, and inclusive economic growth tomorrow.

26. While the costs of infrastructure failure are borne by all areas of our economy, the government has a significant fiscal exposure to these costs. This includes both direct costs associated with recovery and any changes in revenue or expenditure (for example on social programmes) associated with long-term support for businesses, communities and individuals.[14] These costs are in addition to the significant expenditures made by the private sector to restore their own networks. This liability for the government is forecast to increase, with research by the New Zealand Institute of Economic Research indicating that without action the Crown's annual contingent liability for natural hazards alone will be $3.3 billion by 2050.[15]

27. While insurance and reinsurance can cover some of the risks to specific assets, it cannot cover or compensate individuals for any long-term hardships they experience as an indirect result of an event. Even where insurance does exist, the government has historically had a critical role in reinstating damaged infrastructure and providing disaster relief.

28. Changes over time in insurance markets are also likely to increase the portion of disaster risk that is held by the government and public more generally.[16] A reduction in domestic competition in the insurance market; rising premium and excess charges; and growing risk aversion among insurers are already reducing the number of New Zealand businesses and households that can be adequately

---

12 Significant national or regional recessions can lead to "economic scarring" – lasting damage to individuals' economic situations and the economy more broadly. This can manifest in a number of ways but includes skill atrophy for unemployed workers who may find it harder to find new jobs post-recession, and delays or declines in business investment and formation – reducing long-term potential gross domestic product.

13 AustCyber, 2020, "Australia's Digital Trust Report". Available at: https://www.austcyber.com/resource/digitaltrustreport2020.

14 The New Zealand Government provides estimates of these exposures in its twice-yearly Economic and Fiscal Updates. The most recent update can be found here: https://www.treasury.govt.nz/publications/efu/half-year-economic-and-fiscal-update-2022.

15 Clough, P and Gamperle, D, 2020. "Natural hazards Mitigation Report 2020". NZIER.", page ii. Available at: https://www.dia.govt.nz/diawebsite.nsf/Files/Central-Local-Government-Partnerships/$file/NZIER-Natural-hazards-mitigation-report-2020.pdf.

16 Currently, the Crown already holds this risk in respect of assets it owns (because they are self-insured), while critical infrastructures owned by local government, or the private sector tend to seek insurance through insurance markets.

insured. As the risk of extreme weather events grows and sea-levels continue to rise, these pressures are expected to get worse with the result that many of our critical infrastructure assets will become more expensive to insure or even uninsurable.[17]

29. Given that investments in resilience can generally occur at a lower cost than paying for repairs and recovery after an event,[18] enhancing the critical infrastructure system's resilience is likely to reduce the government's and broader societies' fiscal exposure to disasters over time.

30. Shifting the balance of our expenditure away from (largely government-funded) recovery, towards resilience, is also likely to increase equity, both for members of our communities today and on an intergenerational basis. This is because:

    a. the beneficiaries of underinvestment in resilience for each critical infrastructure entity are relatively narrow (shareholders and customers), while all New Zealanders bear the costs of infrastructure failure[19]

    b. lower income New Zealanders who receive a greater share of direct government fiscal support (eg. through the social welfare system) bear a disproportionate share of the burden of government funds being redirected towards disaster recovery

    c. on an intergenerational basis, the costs of disaster recovery will be largely (if not entirely) borne[20] by New Zealanders at the time following the event, while current and previous taxpayers, ratepayers, shareholders, and customers may have underinvested in resilience prior to the event.

31. Given the time horizons that some natural hazards occur on (eg. a major earthquake on New Zealand's Alpine Fault occurs, on average, every 250 years),[21] the intergenerational transfer of wealth associated with these policy settings is significant.

17 Te Waihanga, 2022, "Infrastructure Strategy", page 91. Available at: https://media.umbraco.io/te-waihanga-30-year-strategy/1sfe0qra/rautaki-hanganga-o- -new-zealand-infrastructure-strategy.pdf.

18 Clough, P and Gamperle, D, 2020. "Natural hazards Mitigation Report 2020".

19 While there will always be some overlap between the populations who benefit from underinvestment, and those who bear the cost, it is unlikely to ever perfectly match. For example, natural disasters are generally region-specific.

20 The proportion of cost borne by each age cohort after an event will depend on whether the expenditure is financed from general revenue or debt. If the latter, costs will be borne by a larger cohort over the time period until the debt matures. However, this does not remove any inequities associated with underinvestment by groups prior to the event occurring.

21 Howarth, J and Sutherland, R, 2021, Nature Geoscience, "Spatiotemporal clustering of great earthquakes on a transform fault controlled by geometry", *Nature Geoscience* 14(5): 1-7, available at: https://www.researchgate.net/publication/350979782_Spatiotemporal_clustering_of_great_earthquakes_on_a_transform_fault_controlled_by_geometry.

How is critical infrastructure resilience currently delivered?

32. Successive New Zealand Governments have not taken a comprehensive or coordinated approach to critical infrastructure regulation. No single agency has had policy or regulatory responsibility for New Zealand's critical infrastructure system.

33. Instead, New Zealand's regulatory approach is asset- and sector-centric. The primary responsibility for determining what level of resilience is appropriate and investing to deliver on this rests with critical infrastructure owners and operators. The target level of resilience is informed by:

    a. market pressure from consumers and other critical infrastructure entities to meet performance expectations

    b. in some sectors, requirements imposed by independent regulators consistent with their legislative mandates (eg. the Electricity Authority in respect of energy market participants; the Reserve Bank of New Zealand in respect of banks' and insurers' financial stability; and the Commerce Commission in respect of electricity lines, gas pipelines, telecommunications).[22]

34. Not all regulation is sector specific. For instance, the CDEM Act 2002 is hazard agnostic legislation that, amongst other things, sets out the roles and responsibilities for hazard readiness, emergency response, and recovery. This supplements the roles and responsibilities established in hazard-specific legislation to support effective coordination, such as the Biosecurity Act 1993. The CDEM Act 2002 requires lifeline utilities (a limited subset of critical infrastructures)[23] to "function to the fullest possible extent" following an emergency,[24] and imposes duties across the "four Rs"[25] of emergency management. Reflecting the National Emergency Management Agency's (NEMA) role as a steward, operator, and assurer of the emergency management system, NEMA does not have any formal enforcement functions within the critical infrastructure system.

35. Beyond formal regulatory requirements, critical infrastructures are also supported in preparing for, and mitigating the consequences of, potential hazards and threats through awareness and capability building. This is provided by government agencies. For example:

    a. the Earthquake Commission and National Institute of Water and Atmospheric Research (NIWA) provide significant information on natural hazard exposures

    b. the New Zealand Security Intelligence Service and Government Communications Security Bureau (GCSB) can provide guidance, expertise, and specialist technical capabilities to critical infrastructure owners and operators to assist with managing cyber and other national security risks.

36. Additional detail on specific aspects of New Zealand's regulatory approach is discussed in Section 2. An overview of the current regulatory model is at Figure 1 on page 17.

---

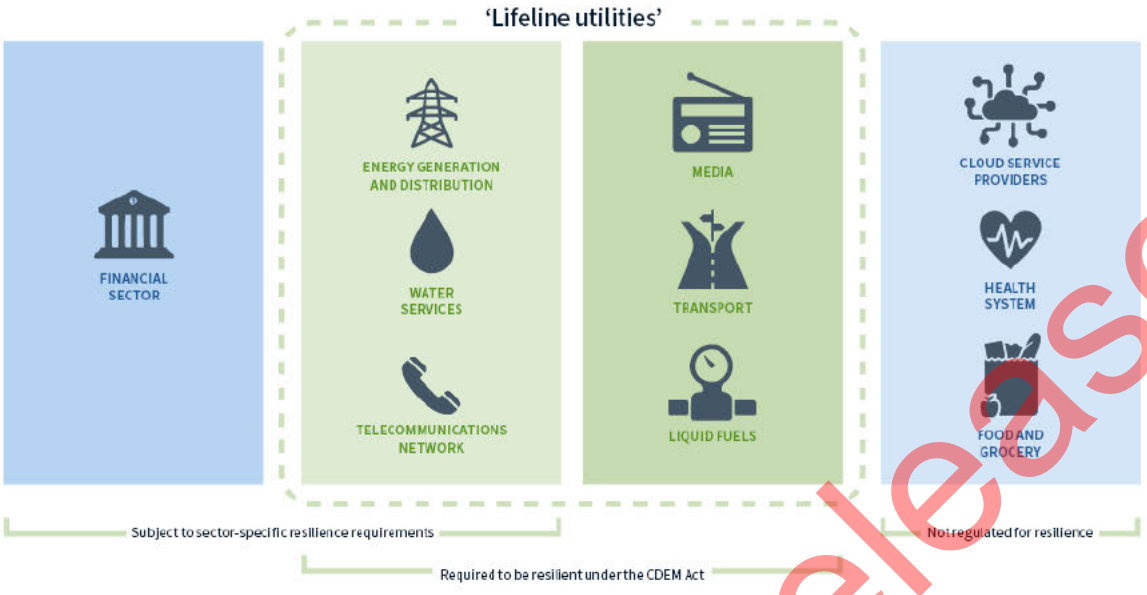
22 These requirements take many forms, from financial incentives or penalties to ensure that critical infrastructure entities meet minimum reliability requirements, to explicit prescriptive requirements around the level of resilience required (for example, capital requirements for banks).

23 Lifeline utilities are prescribed in Schedule 1 of the Civil Defence Emergency Management Act 2002. This is available here: https://www.legislation.govt.nz/act/public/2002/0033/51.0/whole.html#DLM150766.

24 See section 58 of the Civil Defence Emergency Management Act 2002.

25 The four Rs are: reduction (g, enhancing resilience), readiness and response (eg. developing operational systems and capabilities before an emergency occurs), and recovery (eg. coordinated efforts and processes for community regeneration).

Figure 1: Simplified overview of New Zealand's regulatory approach to infrastructure resilience



Proposed reform of the Civil Defence Emergency Management Act 2002 and its relevance to this discussion document

Overview of the proposed reform

NEMA has established a programme to review the current regulatory and legal framework for emergency management

The Emergency Management Bill is one part of this programme – introduced in June 2023, it proposes some changes to enhance the resilience of lifeline utilities, which include:

- replacing the term 'lifeline utilities' with a new principles-based definition of "critical infrastructure" with specific critical infrastructures to be listed in the Gazette; and
- enhancing information-sharing requirements between critical infrastructures and government, to support monitoring and planning (for example, reporting of cyber incidents).

Relationship between these reforms and this discussion document

The government's proposed reforms of the emergency management system will go some way to enhancing New Zealand's critical infrastructure resilience. In particular, the shift from 'lifeline utilities' to 'critical infrastructure' will futureproof New Zealand's emergency management regulatory regime so it can adapt to the emergence of new critical infrastructures.

Irrespective of the outcomes of this work on critical infrastructure resilience, it is intended to retain and implement the provisions in the Emergency Management Bill to ensure they are embedded as an initial step towards improving resilience.

Why a new regulatory approach may be required

New Zealand's infrastructure is increasingly vulnerable to stresses and shocks

37. New Zealand's environmental and physical features mean that our critical infrastructures are exposed to a broader and more consequential range of shocks, particularly natural hazards, than any other developed country. For example:

    a. Lloyds assesses that New Zealand has the second highest disaster loss risk in the world, with Japan – another country on the tectonically active Pacific Ring of Fire – the only other high-income country listed in the top ten (with Japan's risk estimated to be less than half of New Zealand's).[26]

    b. The United Nations (UN) Disaster Risk Reduction database[27] highlights that these natural hazard risks are unusually weighted towards low frequency, and comparatively unpredictable, high-impact events (also known as 'high-impact, inevitable, but rare events' or HIRE events). The UN notes earthquakes and tsunamis as examples, but volcanic eruptions are also a risk for New Zealand.[28]

38. This reflects New Zealand's unique and complicated geography, with the country on the collision zone between two tectonic plates. While this risk has always existed, our understanding of it is constantly improving – with the latest national seismic model estimating that the threat posed by the Hikurangi subduction zone is 1.5 to 2.5 multiples higher than it was previously understood to be (as just one example).[29]

39. Together with this 'hazardscape', the country's long, narrow shape creates infrastructure challenges, with electricity, telecommunications and transport networks running north to south. In some instances, there is limited capacity for growth or redundancy supply in the case of infrastructure failure (for example, Auckland's fuel pipeline and limited transport links to Wellington).

40. We also have other vulnerabilities, including aging infrastructure (for example, much of New Zealand's water infrastructure) and the use of outdated or relatively unsecure technologies by some operators. Combined, these make enhancing our resilience a priority. Managing these pressures alongside population growth will already require significant additional investments in resilience (with pre-pandemic forecasts suggesting New Zealand's population would reach six million by 2050).[30]

41. In addition to these longstanding pressures, four 'megatrends' will heighten the risk of a range of shocks and increase the likelihood of New Zealanders experiencing service disruptions and outages. These megatrends mean that New Zealand's need for greater infrastructure resilience is only going to increase.

26 Lloyds, 2018, "A world at Risk: Closing the Insurance Gap". Available at: https://www.lloyds.com/worldatrisk.

27 See: https://www.undrr.org/.

28 Noting that volcanic eruptions are excluded from the United Nation's analysis.

29 GNS Science, 2022, "National Seismic Hazard Model", available at: https://www.gns.cri.nz/research-projects/national-seismic-hazard-model/.

30 StatsNZ, 2020, available at: https://www.stats.govt.nz/news/new-zealands-population-could-reach-6-million-by-2050/.

Four megatrends will reshape New Zealand's infrastructure system

42. The first of these megatrends is **climate change**. Climate change is expected to undermine the resilience of New Zealand's critical infrastructure system by both increasing stresses and vulnerabilities and increasing the risk of shocks.

43. As laid out in New Zealand's first National Adaptation Plan,[31] some direct effects of climate change include:

    a. more extreme and more frequent weather events, such as storms, heatwaves, and heavy rainfall with numerous risks to infrastructure resilience

    b. fewer frost and snow days, with significant impacts on hydrology and the seasonal cycle of snowmelt, with material implications for the energy sector

    c. more frequent and severe droughts, putting pressure on our freshwater resources – potentially affecting the reliable supply of drinking water and electricity generation

    d. sea level rise, which may compromise or strand existing communities and critical infrastructure assets.

44. Global efforts to mitigate the direct effects of climate change will also have significant implications for critical infrastructure operations and resilience. This includes, but is not limited to, changes in: how electricity is generated; how and when electricity is used (for example, as more consumer and commercial processes are electrified); what materials are used to build and maintain infrastructures; and pricing structures, which will need to better reflect the cost of greenhouse gas emissions.

45. These changes will affect all of our critical infrastructures, directly and indirectly, including through supply chain disruptions, physical impacts, and changes in demand.

46. The second megatrend is **a more complex geopolitical and national security environment**.

47. As described in the Defence Assessment 2021,[32] New Zealand faces a substantially more challenging and complex strategic environment than it has for decades. This makes the risks of manmade shocks higher than they have been in a generation. Risks of particular relevance to New Zealand's critical infrastructures include those, in cyber space, where:

    a. between 2019 and 2022 there was a 45% increase in reports of cybercrime, with intelligence estimates pointing to an actual rise of over 80%; and

    b. attacks are increasingly motivated by factors other than financial gain, for example, many cyber attacks are geopolitically motivated and linked to nation state actors, who seek to disrupt essential services.

48. Geopolitical tensions are not limited to the cyber domain. By virtue of holding large amounts of sensitive information and their integral role in our economy, critical infrastructures are also attractive targets for:

    a. espionage (the covert collection of non-publicly available information)

---

31 Available at: https://environment.govt.nz/assets/publications/climate-change/MFE-AoG-20664-GF-National-Adaptation-Plan-2022-WEB.pdf.

32 New Zealand Ministry of Defence, 2021, "Defence Assessment 2021: He Moana Pukepuke E Ekengia E Te Waka / A Rough Sea can still be Navigated". Page 6. Available at: https://www.defence.govt.nz/assets/publication/file/Defence-Assessment-2021.pdf.

b. sabotage (service disruption)

c. coercion (the threat of service disruption to extract concessions from critical infrastructure owners and operators).

49. These risks can arise through foreign states, or proxies working on their behalf, who gain control of, or access to, New Zealand's infrastructures. This may include through:

a. investment and other commercial partnerships (such as joint ventures)

b. the supply of goods and services (such as managed service providers or software vendors, that could extract sensitive information from corrupted or insecure assets)

c. employment.

50. Related to this more challenging strategic environment, the third trend is vulnerabilities in the globalised economic model and the rapid policy changes to respond to them, which are driving **economic fragmentation**.

51. This change can already be observed through the operation of global supply chains. For example, border closures and recent difficulties in global travel have placed significant pressures on the ability of owners and operators to access the goods and services needed to build, maintain, and operate our critical infrastructure. This is exacerbated by the small size of our domestic market, which leaves us nearly wholly reliant on offshore suppliers for many critical inputs.[33]

52. While the COVID-19 pandemic highlighted these vulnerabilities, they are vulnerabilities that could also be exploited by a foreign state for strategic ends or exacerbated by conflict. They also overlap with broader concerns about the scale and distribution of the benefits that the globalised economic model has delivered.

53. Worldwide, there are now efforts to enhance domestic economic resilience, with a 'just in time' approach to managing the supply of strategically important goods[34] (ie. goods arrive just as they are required) being replaced in some jurisdictions with a 'just in case' approach (ie. sufficient supplies are kept on hand to manage disruptions).[35] Technological change, particularly automation, is accelerating this transition. Previously some goods could not be produced competitively onshore, whereas it is becoming affordable to do so again – with the added benefit of shorter and less complex supply chains.

[33] Currently, 90 per cent of our construction products needed to build or repair our physical infrastructures are either imported or contain imported products that cannot be easily sourced within Aotearoa New Zealand. See EBoss, 2021, "Construction Supply Chain Report. Aotearoa New Zealand. 2021:", page 7. Available at: https://www.eboss.co.nz/assets/marketing/supply-chain-survey/EBOSS-Construction-Supply-Chain-Report-2021.pdf.

[34] For example, semiconductors, pharmaceuticals and fertilisers.

[35] This is not just happening at the macroeconomic level. Some governments are also imposing requirements on infrastructure operators to secure their supplies of critical inputs.

54. This economic fragmentation is not just being driven by jurisdictions' desires to ensure a continuous domestic supply of critical goods and services. Many governments are also placing new barriers around the use of some imported products and the export of some products[36] to respond to concerns that:

    a. the purchase and installation of some goods may, in itself, pose risks (eg. certain IT equipment may allow systems to be remotely accessed or controlled or allow data to be exfiltrated), or facilitate unethical practices (eg. modern slavery and other human rights abuses)

    b. the sale of some goods (eg. semiconductors) may aid the military capabilities of states that are perceived to be hostile.

55. Collectively, these measures are increasing the risk that product standards and logistics chains become fragmented. This will likely increase costs and reduce product availability over the medium term. To manage these breakdowns in supply, critical infrastructure owners and operators may have no choice but to adapt their approach to securing critical inputs, likely at higher cost, which will ultimately be at least partly passed on to all New Zealanders through higher service charges. Depending on how product availability changes, it may also adversely affect the stability of the infrastructure system over the long term.

56. The final megatrend is the **advent and rapid take up of new technologies**. This is expected to compound the consequences associated with the potential shocks described above.

57. The adoption of new technologies facilitates (among other things) greater automation, better remote monitoring and management, and greater connectivity. This is delivering savings for business and consumers and enhancing productivity and economic growth. For these reasons, their deployment is welcomed and consistent with the Government's broader economic objectives.

58. However, the adoption of new technologies also creates new vulnerabilities and stresses by:

    a. changing what we consider to be critical infrastructure, leaving regulatory systems out of date. For example, as the New Zealand economy becomes more digitised, the service providers that underpin that transformation (eg. cloud service and data storage providers) will become increasingly critical to the economy's day-to-day function. However, these service providers are not currently subject to regulations to support or enhance their resilience

    b. introducing new vulnerabilities. For example, technological innovation is driving physical and digital systems to converge (eg. operational technology (OT) systems are now integrated with information technology (IT) systems such that physical events can be controlled through digital systems connected to the internet). This creates new challenges to infrastructure resilience – it expands the attack surface and enables malicious actors to gain access to the systems that monitor and control physical equipment, and ultimately disable or disrupt operations.[37]

[36] For example, on 7 October 2022, the United States' Government announced new controls on the sale of semiconductors and other advanced computing products to the People's Republic of China. Additional detail is available at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file

[37] Australian Strategic Policy Institute, 2019, "Protecting Critical National Infrastructure in an era of IT and OT convergence", page 4. Available at: https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence; US Cybersecurity and Infrastructure Security Agency, "Cybersecurity and Physical Security Convergence", page 1. Available at: https://www.cisa.gov/cybersecurity-and-physical-security-convergence.

c. increasing the number of dependencies and interdependencies between New Zealand's critical infrastructures, meaning that:

   i. the impact of any emergency will be deeper and more pervasive than previously experienced, as outages cascade across the critical infrastructure system (ie. the likely consequence of any shock has increased)

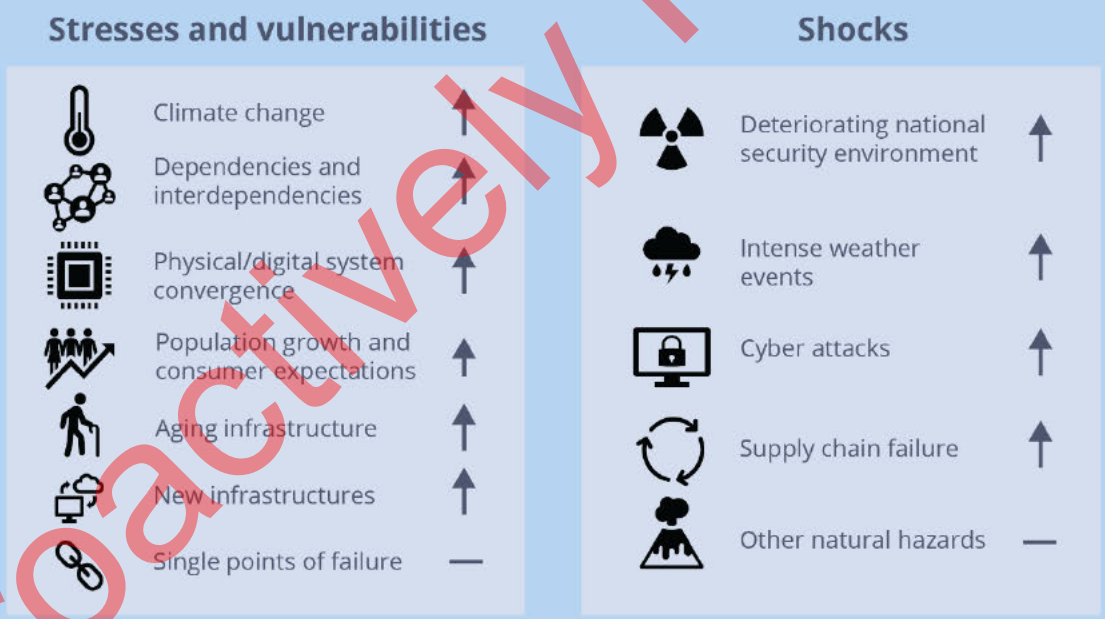
   ii. weaknesses or vulnerabilities in any part of the infrastructure system could appear as weaknesses in every part of the infrastructure system. Widescale outages could increasingly be triggered by outages or disruptions to assets that were previously peripheral

   iii. the costs of infrastructure failure will be borne more widely, while the costs of enhancing resilience will remain borne by critical infrastructure owners and operators. Over time, this is likely to contribute to further underinvestment in resilience.

How these megatrends affect the stresses and shocks that are likely to impact New Zealand's critical infrastructure resilience

The primary stresses and shocks that New Zealand's infrastructure system is exposed to are summarised in Figure 2. The arrows indicate where a pressure is growing or staying the same in the face of the four megatrends.

Figure 2: Stresses and shocks that pose risks to infrastructure resilience



The Government would like your views

- The paper discussed four megatrends: i) climate change, ii) a more complex geopolitical and national security environment, iii) economic fragmentation, and iv) the advent and rapid uptake of new technologies. Do you think these pose significant threats to infrastructure resilience?
- Are there additional megatrends that are also important that we haven't mentioned? If so, please provide details.

These megatrends risk exposing the limitations of our current approach to resilience

59. New Zealand's long-standing approach to regulating for critical infrastructure resilience has relied on the assumption that critical infrastructure owners and operators (or regulators) could accurately determine:

    a. the likelihood of a shock occurring

    b. know who or what would be affected by that shock

    c. estimate a shock's costs

    d. make rational choices about what investments to make to reduce those costs.

60. This approach to ensuring resilience has historically served New Zealand reasonably well. However, it is not likely to be well suited to manage the complex challenges to come. For example, these four megatrends will make it more difficult to:

    a. forecast the likelihood of shocks, particularly those linked to a changing climate and state threats

    b. determine a shock's impact, as effects ripple through an increasingly interconnected infrastructure system

    c. establish clear and simple accountabilities for mitigating certain risks, because responsibility for action is more likely to be shared.

61. For this reason, Te Waihanga and New Zealand's National Adaptation Plan for climate change recommend taking a coordinated, systematic approach to building infrastructure resilience. This requires the focus to shift from the resilience of each distinct infrastructure asset, to how infrastructure assets and the networks between them can contribute to the resilience of the whole infrastructure system.[38]

62. Adopting such a systems-based approach would be consistent with OECD best practice, and frameworks that have been adopted in, (or are increasingly proposed to be adopted in) other jurisdictions, including Australia,[39] Japan,[40] the United States, and the European Union.[41]

63. This kind of regulatory model would also likely offer benefits beyond enhancing infrastructure resilience. It could, for example, provide for a more coordinated approach to, and understanding of, New Zealand's critical infrastructure system and its strengths and vulnerabilities. In turn, this would:

    a. benefit emergency management and the delivery of broader community resilience objectives

    b. complement the government's proposed reforms of the Resource Management Act 1991, requiring future critical infrastructures to be built in the 'right' places and to the right standards.

---

38 Infrastructure Australia and Infrastructure New South Wales, 2021, "A Pathway to Infrastructure Resilience – Advisory Paper 1: Opportunities for systemic change", page 6.

39 Australian Government, 2020, "Protecting Critical Infrastructure and Systems of National Significance". Available at: https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf.

40 A summary of Japan's proposed economic security Bill, which includes new measures to enhance critical infrastructure resilience, is available here: https://www.japantimes.co.jp/news/2022/02/14/business/economic-security-law-business-worries/.

41 European Commission, 2019, "Evaluation of council directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". Available at: https://ec.europa.eu/home-affairs/system/files/2019-07/20190723_swd-2019-308-commission-staff-working-document_en.pdf.

Overview of Australia's recent reforms to enhance infrastructure resilience

In April 2022, Australia's Parliament passed the second of two legislative amendments to enhance the resilience of its infrastructure system.

The reforms are designed to uplift the security and resilience of Australia's critical infrastructure, and the delivery of essential services. This is to protect against all hazards and threats, including physical, supply chain, cyber, and personnel risks.

Australia's Security of Critical Infrastructure Act 2018 (amended in December 2021 and April 2022 respectively) defines 22 classes of critical infrastructure assets across 11 sectors: communications; data storage or processing; financial services and markets; water and sewerage; energy; health care and medical; higher education and research; food and grocery; transport; space technology; and the defence industry.

Owners and operators of critical infrastructure assets are now required to implement three preventative obligations, as listed below.

1. Provide ownership and operational information to Australia's Register of Critical Infrastructure Assets to ensure the government knows who owns and controls critical infrastructure assets.
2. Report certain types of cyber security incidents to the Australian Cyber Security Centre to build a rich picture of cyber incidents against Australian critical infrastructure and inform technical advice on how best to prepare and respond to incidents.
3. Establish, maintain, and comply with a risk management program to identify and mitigate 'material risks' that have a substantial impact on the availability, reliability, and integrity of critical infrastructure in Australia.

A smaller group of critical infrastructure assets can be declared by Australia's Minister for Home Affairs as 'Systems of National Significance', by virtue of their interdependencies across sectors and the potential for cascading consequences to other assets and sectors if disrupted. Systems of National Significance can then be subject to up to four Enhanced Cyber Security Obligations, including: the development of an incident response plan; undertaking an exercise to build preparedness; undertaking a vulnerability assessment and/or providing systems information.

Finally, to support the management of national security risks, the SOCI Act provides the government with two tools.

1. **A direction power:** In respect of all types of national security risks, the relevant Australian Minister can direct any critical infrastructure entity to do (or refrain from doing) an act or thing where necessary to mitigate that risk and where no other tools are available to achieve that outcome.
2. **An intervention power:** In the event of malicious cyber activity that poses an imminent and significant risk to national security, the relevant Australian Minister can invoke, as a last resort, 'Government Assistance Measures' that allow for direct intervention in the critical infrastructure entity to defend the asset.

Australia's reforms are still being implemented and their effectiveness in enhancing the resilience of Australia's critical infrastructure system is still to be determined.

What would the financial consequences of enhancing the critical infrastructure system's resilience be?

64. Increasing New Zealand's annual investment in high-quality critical infrastructure resilience should save money in the long term. Increased investment costs will be more than offset by a reduction in expenses and asset value associated with infrastructure outages and failure. This is in the interests of all New Zealanders, but also government and critical infrastructure owners and operators.

65. In the short-term, however, additional investments will come at a cost. Consistent with Te Waihanga's infrastructure funding and financing principles,[42] these costs are best borne by the predominant beneficiaries of more resilient institutions. These are a mixture of:

    a. shareholders, through a lower return on equity

    b. employees, through lower salaries (particularly where remuneration is linked to equity or other measures of financial performance)

    c. customers, through higher prices

    d. government, particularly where it is the owner of the relevant infrastructure.

66. This outcome would be more efficient than the status quo approach, where all New Zealanders pay for a significant amount of post-event remediation through taxes, to offset underinvestment and uninsured costs at the local or regional level. It would also increase transparency for users if the cost of improving resilience is embedded in service charges.[43]

67. Acknowledging inflationary pressures, this does not mean that costs for consumers would go up rapidly or by a significant amount. This is because:

    a. many critical infrastructures, particularly in regulated sectors, are already performing well and may not have to significantly increase their expenditure to meet any new requirements

    b. where significant additional investments are required, any cost increases are expected – in most cases – to be gradual, rather than as a one-off increase. This because critical infrastructure assets are long lived and investments to enhance their resilience also occur over lengthy timeframes.

[42] Te Waihanga, 2022, "New Zealand Infrastructure Strategy", page 123.

[43] Relative to the status quo, where the expenses associated with infrastructure failure are abstract and difficult to measure (for example, a reduction in society's wellbeing because other government programmes cannot be funded).

68. Additionally, as the government develops options to enhance system resilience, significant attention will be given to minimising the scale and consequences of any cost increases. For example, this could be achieved through:

a. an initial focus on 'lifting the floor' of critical infrastructure resilience, particularly for those entities currently not subject to regulation

b. timing the introduction of any new regulatory requirements to align with businesses' existing investment plans, to the extent possible

c. considering direct government support for more vulnerable New Zealanders, to ensure that resilience does not reduce their access to critical services.

The Government would like your views

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

Section 2: Potential barriers to infrastructure resilience

The OECD has outlined regulatory features that support a best practice systems-based approach to critical infrastructure resilience.[44]

These principles recognise that critical infrastructure resilience depends on governments partnering with critical infrastructure owners and operators. This vision of partnership underpins this discussion document, as well as the government's broader work on this issue.

Drawing on the OECD's principles as well as relevant aspects of comparable overseas regimes, this section:

- describes the regulatory features that could support a more systems-based approach to critical infrastructure resilience
- seeks your views on whether this change in regulatory approach would likely improve New Zealand's ability to deliver a resilient infrastructure system. This feedback will inform consideration of potential reform options, tailored to New Zealand's specific context.

The regulatory features discussed are:

- mechanisms to build a shared understanding between government, regulators, and critical infrastructure owners and operators of key issues to system resilience
- proportionate and targeted regulatory tools to ensure that the infrastructure system has a baseline level of resilience
- last resort powers to manage significant national security risks (such as malicious cyber activity) where they arise
- clear accountabilities and accountability mechanisms for enforcing infrastructure resilience, across both government and critical infrastructure owners and operators.

[44] OECD, 2019 "Good Governance for Critical Infrastructure Resilience". Available at: https://www.oecd-ilibrary.org/docserver/02f0e5a0-en.pdf?expires=1683501029&id=id&accname=ocid56017414&checksum=A11158D51D597E8921A2B0747988EB08.

Building a shared understanding of issues that are fundamental to system resilience

This subsection outlines why a shared understanding of hazards and threats between government and critical infrastructure entities is essential to enhancing resilience. In short, this knowledge is needed:

- for critical infrastructure owners and operators to confidently target their limited resilience budgets at their most important assets, to manage the most likely and most consequential risks, and
- for regulators to develop appropriate and proportionate policies and other regulatory settings.

The subsection also describes how successfully the government is building a shared understanding today, and how reforms already underway will improve this. It concludes that the government's current approach to information sharing is not sufficiently comprehensive or regular to deliver on this goal. This is despite the success of tools like the advisories, alerts and cyber defence services provided by CERT NZ and the GCSB's National Cyber Security Centre, and the introduction of a beneficial ownership register.

Feedback is sought on both the need for greater information sharing and potential mechanisms to deliver that outcome.

Why is developing a shared understanding of hazards, threats and risks important?

69. The Infrastructure Strategy,[45] OECD guidance, academia, and a cross-country comparison of regulatory systems all highlight the importance of robust information sharing as an important mechanism for enhancing resilience.

70. Access to the same information enables regulators and critical infrastructure owners and operators to make informed decisions about what events to plan for, how much to invest, and how to prioritise investments to manage them. This requires a shared and comprehensive understanding of:

a. hazards and threats facing New Zealand's infrastructure system

b. the location and nature of New Zealand's most critical assets (ie. the assets most essential to the delivery of services)

c. vulnerabilities already embedded in the infrastructure system, such as: ownership or control by foreign states that could be used to facilitate espionage or sabotage, or reliance on certain suppliers for critical goods that could be subject to disruption

d. the risks associated (or likely to be associated) with building or retaining assets in certain geographical areas, particularly as climate change affects the type, frequency, and intensity of natural hazards

e. dependencies and interdependencies between infrastructures and critical assets, including how service disruptions may cascade across the infrastructure system and the vulnerabilities that this may create for other sectors – even those investing heavily in their own resilience

f. the government's objectives for the resilience of the critical infrastructure system.

[45] Te Waihanga, 2022, "New Zealand Infrastructure Strategy", page 97.

71. More broadly, comprehensive information sharing is necessary to foster a culture of trust and partnership between the public and private sectors in managing infrastructure risks. This is important given each group's distinct but overlapping roles, and the complex, competing issues to be balanced including competition, affordability, equity, and efficiency.

72. While some hazard and threat information can be shared publicly (eg. government assessments of the likelihood of various natural hazards or the effects of climate change) or provided to government without explicit regulatory powers, the exchange of other types of information depends on trust between parties and confidence that it will not be publicly disclosed. For example:

    a. critical infrastructure owners and operators are understandably reluctant to share sensitive information about vulnerabilities, experiences of malicious cyber activity, or critical dependencies outside of a trusted and secure environment, because these disclosures could:

        i. create legal liabilities

        ii. have implications for their competitiveness, or breach anti-trust legislation

        iii. reveal their vulnerabilities to those that would seek to take advantage of them

        iv. otherwise damage their reputation

    b. for government, trust and security is an essential precondition for sharing sensitive, national security information.

73. To manage these challenges, many jurisdictions supplement the public release of information by:

    a. establishing formal legislative powers to enable the collection of certain business-sensitive information (eg. on ownership and governance) from critical infrastructure operators

    b. providing secure systems to share sensitive information between governments, regulators, and critical infrastructure owners and operators. Systems like Australia's 'Trusted Information Sharing Network'[46] and the United States' Domestic Security Alliance Council have been highlighted as best practice mechanisms, which support infrastructure resilience.[47]

[46] For additional information, see: https://www.cisc.gov.au/engagement/trusted-information-sharing-network.

[47] For additional information, see: https://www.fbi.gov/file-repository/dsac_fact_sheet_10-26-2020.pdf/view.

How successfully is New Zealand building a shared understanding of issues fundamental to system-level resilience?

74. New Zealand has regulatory and non-regulatory mechanisms, led by government and the critical infrastructure sector itself, to foster a shared understanding of system-level infrastructure hazards, threats and risks. Mechanisms include those that:

    a. enhance understanding of threat and hazard exposures such as:

        i. the public release of information on natural hazards across a range of platforms (eg. seismic and other hazards through the EQC, and climactic events through NIWA)

        ii. public updates on cyber security threats and emerging issues by CERT NZ

        iii. the targeted release of some information on national security threats by the Intelligence Community, either directly to potentially affected critical infrastructures or to entire sectors (eg. advice from the National Cyber Security Centre on the potential for malicious cyber activity associated with Russia's invasion of Ukraine)[48]

        iv. regulatory powers to request critical infrastructure owners and operators to provide information (eg. on climate change risk and adaptation responses under the Climate Change Response Act 2002,[49] and climate related disclosures under the Financial Sector (Climate-related Disclosures and Other Matters) Amendment Act 2021[50])

        v. critical infrastructure owners and operators voluntarily providing information to government on experienced events or identified vulnerabilities

    b. map vulnerabilities and interdependencies between critical infrastructures (eg. periodic work by the New Zealand Lifelines Council[51] and regional Lifelines Groups)

    c. inform critical infrastructure owners and operators of the government's expectations for the system's resilience (eg. publication of strategies and guidance that intersect with critical infrastructure resilience or covers some constituent elements, such as the National Disaster Resilience Strategy).[52]

48 For example, see: https://www.ncsc.govt.nz/newsroom/gsa-2022-2940/.

49 For additional information, see section 5ZW of the Climate Change Response Act 2002 available at: https://www.legislation.govt.nz/act/public/2002/0040/latest/DLM158584.html.

50 Climate Related Disclosures are currently required by large, listed companies (with a market capitalisation of more than $60 million). Additional information is available at: https://legislation.govt.nz/act/public/2021/0039/latest/whole.html.

51 For example, see Section 4 of the New Zealand Infrastructure Vulnerability Assessment 2020. This is available at: https://www.civildefence.govt.nz/assets/Uploads/lifelines/nzlc-nva-2020-full-report.pdf.

52 See: https://www.civildefence.govt.nz/assets/Uploads/publications/National-Disaster-Resilience-Strategy/National-Disaster-Resilience-Strategy-10-April-2019.pdf.

75. These are important mechanisms. However, gaps remain in both the collection and distribution of information, which leave our current settings short of global best practice. For example, only one in five New Zealanders consider that the government shares enough information on national security threats.[53] These gaps inhibit our ability to collectively identify the biggest risks and prioritise our regulatory and investment settings to manage them. In particular:

    a. while the government does share some information on national security risks, the lack of a secure platform to exchange information likely limits broader and more regular distribution of information (eg. government assessments of specific threats)

    b. the government does not have the power to collect the range of information necessary to form an accurate and aggregated picture of the threats facing the infrastructure system. In particular, the government currently does not have access to the following relevant information:

        i. complete data on outages, failures, and potential threats, such as cyber incidents (which could also inform timely advice to other infrastructure operators on mitigations)

        ii. the identities of the individuals and entities that own and control New Zealand's infrastructure assets, and whether that control and access could be used to undermine New Zealand's national interests

        iii. the types of equipment being used within critical infrastructures, and whether they increase the risk of successful espionage, sabotage, coercion or malicious cyber activity

        iv. the suppliers of critical goods and services to critical infrastructures, and whether there are greater risks associated with some suppliers (eg. access to such goods being cut off to undermine New Zealand's national interests).

    c. there is no real-time national view of the dependencies and interdependencies between critical infrastructures to inform an assessment of how service disruptions are likely to cascade across the infrastructure system (and which infrastructures are the most important to protect). Further, no government agency has the mandate or expertise to develop and maintain such a model, even if it had access to the relevant information

    d. the government does not clearly articulate its expectations for the resilience of the infrastructure system. This makes it more difficult for critical infrastructure owners and operators, as well as regulators to balance different system objectives in line with the government's expectations.

[53] DPMC, "Draft Long-term Insights Briefing 2022", page 22. Available at: https://dpmc.govt.nz/sites/default/files/2022-10/Draft%20National%20Security%20Long-term%20Insights%20Briefing_1.pdf.

What reforms are already underway that will help address this problem?

76. The Government has proposed measures that will partially resolve some of these information gaps. These include:

a. introducing a beneficial ownership register, which will make it easier to identify the ultimate ownership of unlisted New Zealand companies and limited partnerships, and to understand any risks associated with those positions[54]

b. enhanced information gathering and sharing powers for NEMA through the Emergency Management Bill. This could allow for the collection of information on dependencies and interdependencies and experienced events.[55]

77. While these measures will support the government, regulators, and critical infrastructure owners and operators in understanding threats and vulnerabilities, gaps will remain relative to the OECD's best practice guidance. For example:

a. there will be no change in the ability of government or critical infrastructure entities to share sensitive information securely, or with confidence that sharing sensitive information will not conflict with other requirements, like anti-trust

b. the government's understanding of malicious cyber activity and other experienced national security events will remain, at best, partial

c. the changes will not, on their own, allow real-time mapping of dependencies and interdependencies

d. the information sharing that occurs will remain fragmented across multiple websites and platforms.

78. These measures will also not enhance New Zealanders' understanding of the government's objectives for the infrastructure system.

The Government would like your views

- If you are a critical infrastructure owner or operator, what additional information do you think would best support you to improve your resilience?
- What do you think the government should do to enable greater information sharing with and between critical infrastructure owners and operators?

54 For additional information, see: https://www.beehive.govt.nz/release/govt-cracks-down-misuse-nz-companies.

55 For additional information, see the Civil Defence Emergency Management Bill.

Setting proportionate resilience requirements

This subsection describes the potential benefits of:

- all critical infrastructure owners and operators meeting shared minimum resilience standards (whether those standards are prescriptive, principles-based, or process-based)
- critical infrastructures of particular significance (eg. those that have a significant number of connections with other critical infrastructures) being subject to higher resilience standards.

In both instances, minimum resilience standards can be used to:

- better align investment in resilience with the level of resilience that New Zealanders expect (recognising that because the costs of infrastructure failure are widely spread, this is unlikely to occur without regulation)
- prevent vulnerabilities in unregulated sectors resulting in outages that undermine the resilience of highly regulated sectors
- counteract cognitive biases that can cause critical infrastructure entities to underinvest in resilience
- focus attention on key measures to better manage the types of high-impact, rare events to which New Zealand is predominantly exposed.

The subsection notes that New Zealand currently has no mechanisms to deliver consistent minimum resilience standards to enhance critical infrastructure resilience against all hazards and threats (as recommended by the National Adaptation Plan), or any mechanisms that will bring our regulatory settings materially closer to this outcome.

Feedback is sought on the potential suitability of such standards in New Zealand, as well as how any standards could or should be applied.

Why may it be important for all critical infrastructures to meet a minimum level of resilience?

79. Critical infrastructures operate as a system. Each critical infrastructure depends on services provided by other critical infrastructures (eg. many power grid functions rely on telecommunications). The breadth and depth of connections between infrastructures, means that vulnerabilities in any critical infrastructure asset can pose risks to the entire system's stability.

80. These features can make it more difficult to build appropriate levels of resilience without government intervention. This is because:

a. the costs of infrastructure failure are spread widely across the community, but the costs of enhancing resilience are borne by individual infrastructure entities. Given that critical infrastructure owners and operators only have financial incentives to an amount equal to their own potential losses of infrastructure failure, this can create a gap between the level of resilience optimal for the infrastructure entity and the 'socially optimal' level of resilience.

b. It is difficult for consumers to identify whether critical infrastructure is resilient (eg. whether both their supplier, and their suppliers' supplier, has robust cyber security practices). Many New Zealanders continue to live and invest in locations without resilient infrastructure, especially since the benefits of infrastructure resilience are not actively promoted. This reduces the power of consumer choice as a tool in driving the necessary investment in resilience. It also means that for those critical infrastructures that increase their resilience, costs will go up for their customers. In competitive markets, these customers may be easily poached by a competing supplier that is not investing in resilience to the same level.

81. New Zealand's unusually high distribution of HIRE events (as discussed in paragraph 37) further inhibit the ability of the critical infrastructure system to reach the 'socially optimal' level of resilience without government intervention. This is because HIRE events are subject to 'normalcy' bias[56], which leads to underinvestment ahead of adverse events and overreaction after they occur.[57] These factors help explain New Zealand consumers' historic reluctance to pay higher prices for more resilient organisations, even where this has been advocated.[58] For this reason, managing HIRE risks almost always requires coordination beyond the individual and enterprise level.[59]

82. To overcome these disincentives, many jurisdictions are working to introduce – or have introduced enforceable **minimum resilience standards** for all critical infrastructures across all the resilience domains described in Section 1. This is consistent with OECD guidance, which endorses such standards as important tools for minimising 'weak links' that could jeopardise the security of the overall critical infrastructure system.[60]

83. Resilience standards can take various forms and this document does not prejudge what form might be most appropriate for New Zealand. These forms include, but are not limited to:

a. principle-based requirements (eg. an objective, similar to those that exist under the CDEM Act 2002 'to be resilient')

b. process-based requirements (eg. a requirement to adopt a standard process or risk management framework, such as an annual requirement to identify critical assets, risks to them, and implement a mitigation strategy).[61]

84. Standards can apply to a critical infrastructure entity (the approach taken under the CDEM Act 2002), or to its critical assets (the approach taken under Australia's Security of Critical Infrastructure Act). Linking standards to critical assets, rather than the entities that are responsible for them, may be a better way to target expenditure. This is particularly true for infrastructures that provide a range of critical services, only some of which are critical.

---

56 Normalcy bias is a cognitive bias which leads people to disbelieve or minimise threat warnings. Consequently, individuals underestimate the likelihood of a disaster, when it might affect them, and its potential adverse effects.

57 Schildberg-Horisch, H., 2018, "Are Risk Preferences Stable", Journal of Economic Perspectives. Available at: https://www.aeaweb.org/articles?id=10.1257/jep.32.2.135.

58 For example, the 2019 business case developed by Wellington Lifelines calling for $3.9 billion of investment to enhance resilience that was not taken forward in full.

59 New Zealand Treasury, 2022, "New Zealand's wellbeing: Is it sustainable and what are the risks?". Available at: https://www.treasury.govt.nz/publications/tp/new-zealands-wellbeing-sustainable-what-are-risks.

60 OECD, 2019 "Good Governance for Critical Infrastructure Resilience", page 52.

61 Additional information on NIST, which is just referenced as an example, is available at: https://www.nist.gov/cyberframework/framework.

Examples of dependencies and interdependencies across the critical infrastructure system

The Government considers that a systems-based approach to critical infrastructure resilience is necessary to manage the risks created by the dependencies and interdependencies between critical infrastructures. Some examples of these dependencies and interdependencies, and how they generate a risk of cascading service outages across the economy, are detailed below.

- The **electricity network** underpins the operation of most other critical infrastructures, and a prolonged outage would be expected to adversely affect telecommunications, water supply and wastewater processing, digital service providers, the health system, transportation, and financial services (even accounting for some backup generation).
- A major **telecommunications** failure would significantly curtail the operations of almost all utility businesses, with industrial controls systems and internet-based services particularly affected. While it may be possible for some infrastructures to revert to using manual monitoring and control processes, doing so would not be as efficient or as effective, and overall economic and other impacts would continue to be significant.

Hospitals, emergency services, and the financial system would all struggle to function.

- Disruption in **water supply and wastewater services** would, first and foremost, have significant negative consequences for public health. In addition to critical infrastructures that support basic amenities, this would limit the operations of many that rely on water for cooling and emergency management. This includes fuel terminals, airports, telecommunications, and natural gas-run electricity generators.
- Breakdowns in **road, rail, sea, or air transport** would generate a range of potential disruptions, depending on the mode of transport affected and the scale of the breakdown. These potentially include limits on access to:
  - fast-moving consumer goods, particularly food (and in an emergency, bottled water)
  - fuel, which relies on shipping for domestic distribution, with a range of additional downstream consequences for economic activity
  - emergency services.

Cyclone Gabrielle has recently demonstrated the significant impact that these cascading outages can have on individual New Zealanders and their communities. Power and telecommunications outages directly inhibited and complicated the work of our emergency services in their efforts to save lives and limited the ability of citizens to access essential information on the unfolding disaster. Prolonged payment system failures also made it almost impossible for those most in need to acquire essential medicines and food. However, these types of cascading outages are not unique to this event.

Why may it be important for significant critical infrastructures to be subject to additional requirements?

85. Critical infrastructure entities at the very core of the system generate large spill overs that have far-reaching impacts. Implementing minimum standards would help reduce the risk of weaknesses in one entity adversely impacting the entire infrastructure system, but it would not eliminate the risk entirely. This is because minimum standards might not be stringent enough for critical infrastructures that are nationally important – for example, those that have a significant number of connections with other critical infrastructures and therefore crucial to the overall stability of the infrastructure system (eg. some energy or telecommunications providers).

86. For this reason, some jurisdictions impose additional requirements on their most important critical infrastructures. This is similar to the concept of Globally and Domestically Systemically Important Banks, which must hold additional capital, relative to less important banks, to manage risks to the whole banking system. This kind of proportionate and risk-based regulatory approach, where resilience requirements are tied to an infrastructure's importance, has many advantages. These include:

    a. prioritising spending on resilience investments that would have the most significant impact for New Zealand's infrastructure system

    b. reducing the risk that resilience requirements are set so high for all critical infrastructure entities that they create undue barriers to entry, reducing competition.

87. This type of approach has been central to Australia's recent reforms, with 'systems of national significance' subject to additional reporting and resilience requirements.

How can a critical infrastructure asset's importance be determined?

To apply regulatory requirements in a risk-based and proportionate manner, governments must be able to identify the most critical hubs and nodes of infrastructure systems. This process generally has two steps:

1. mapping dependencies and interdependencies with other parts of the infrastructure system (physical, digital, and geographic), to estimate the full impact that any disruption to that asset might have on the overall functioning of the system

2. using this information to assess the impact of that asset's disruption against a range of criteria.

Generally, two types of assessment models are used to determine the level of criticality:

1. simple models, where the assessment focusses on the geographic area and number of citizens affected

2. holistic models, where the infrastructure's importance is assessed against a broader range of societal domains (including economic, environmental, social and cultural factors). An example of a holistic model developed by Treasury is available at Appendix B.

How successfully is New Zealand setting proportionate resilience requirements for all critical infrastructures?

88. The combination of specific regulatory requirements in some sectors, and requirements for lifeline utilities under the CDEM Act 2002 mean that many – but not all – of New Zealand's most significant critical infrastructures are subject to some standards (eg. the finance, electricity, and telecommunications sectors).

89. However, there is no regulatory regime in place to set, monitor or enforce compliance with standards that apply to common risks across the entire critical infrastructure system (such as cyber risks). This regulatory gap is compounded by an uneven awareness of, and capability to manage, different risks (such as national security risks) within regulated sectors, particularly since each regulator works to their distinct statutory mandates.

90. Without a coordinated approach to setting resilience requirements, New Zealand's infrastructure system will continue to be vulnerable to the impacts of a natural disaster or able to be exploited by a foreign state. This was recognised by the Government in its National Adaptation Plan, with Te Waihanga accordingly tasked with the development of a hazard and threat neutral resilience standard to support climate change management and mitigation.

91. Disparity in resilience requirements between infrastructure sectors can also undermine the value of investments that some critical infrastructure entities are already making to enhance their own resilience. For example, a high level of resilience in the financial sector may not effectively mitigate outages or disruptions to electronic payment systems, if the services that they rely upon (eg. electricity and telecommunications) are not comparatively reliable.

92. In addition, New Zealand does not have a system for determining how critical an asset is and imposing more stringent regulatory requirements on that basis.

93. In some ways, the current regulatory model (where some sectors are subject to regulation and others are not) could be viewed as requiring more important infrastructures to adhere to more stringent standards. However, an Act of Parliament is generally required to change these requirements or the entities that must meet the requirements, meaning that the system is not dynamic or likely to remain proportionate over time (which has been seen to occur).

Managing the interaction between potential minimum standards and other regulatory regimes

The Government has not made any decisions about the form of any minimum resilience standards. Any such decision will be informed by the outcomes of consultation on this document and the subsequent consultation on options.

The Government recognises, however, that whatever form minimum standards take it will be essential that any requirements do not conflict with or duplicate standards in place under other regulatory regimes. In particular, consideration is being given to how any minimum resilience standard would interact with:

- resource management requirements (eg. if standards require additional physical infrastructure to be constructed)
- price-quality settings that apply to some critical infrastructure sectors (most notably electricity and telecommunications)
- existing regulatory standards (such as those applied to many financial institutions) and regulatory 'touch points'.

This includes consideration of recognising regulatory equivalence between overlapping regimes and/or empowering existing sectoral regulators to monitor and enforce any new requirements applied across the critical infrastructure system.

What reforms are already underway that will help to address this problem?

94. The Emergency Management Bill will enhance the resilience of New Zealand's infrastructure system. In particular, the extension of the general requirement to be resilient[62] from 'lifeline utilities' to all critical infrastructure assets should theoretically enhance resilience levels.

95. However, the Emergency Management Bill (and existing requirements for lifeline utilities) focuses on emergency management, rather than critical infrastructure resilience. While the Bill would reinforce the need for resilience, the government – would still be unable to:

a. apply more stringent mandatory requirements to more critical assets

b. apply specific requirements to manage particular risks or vulnerabilities (eg. minimum cyber security standards to protect networks from malicious cyber activity)

c. determine whether the Bill's requirements are being met or met in a consistent way (ie. assess whether critical infrastructure entities are compliant)

d. take enforcement action before or after an emergency event, if it is determined that resilience requirements were not met.

[62] That is, lifeline utilities must be able to function to the fullest possible extent, even though this may be at a reduced level, during and after an emergency.

96. Further, as noted by Infrastructure Australia and Infrastructure New South Wales, situating the government's regulatory regime for resilience in an emergency management context can make cross-government coordination difficult. This recognises that several areas of government outside of the emergency management framework have a regulatory interest in infrastructure resilience (eg. planning and climate change adaptation).[63]

97. Reforms to resource management should also enhance infrastructure resilience over time, by ensuring that newly constructed critical infrastructures are not located in areas, which are particularly at risk from the changing climate or natural hazards. While this is an essential change, it is unlikely to remove the need for resilience standards. This is because:

    a. changes to resource management will have limited, if any, impact on the operations of existing critical infrastructures

    b. while improved consenting can reduce the level of hazards that a critical infrastructure is exposed to, it is not possible in New Zealand to completely eliminate the risk of natural hazards (eg. seismic risks) and threats will persist regardless of location.

The Government would like your views

- Would you support the government being able to set, and enforce, minimum resilience standards across the entire infrastructure system? If so:
  - what type of standard would you support (eg. requirement to adhere to a specific process or satisfy a set of principles)?
  - do you have a view on how potential minimum resilience standards could best complement existing approaches to risk management?
- Would you support the government investing in a model to assess the significance of a critical infrastructure asset is, and using that as the basis for imposing more stringent resilience requirements? If so:
  - what options would you like the government to consider for delivering on this objective?
  - what criteria would you use to determine a critical infrastructure asset's importance?

63 Infrastructure Australia and Infrastructure New South Wales, 2021, "A Pathway to Infrastructure Resilience – Advisory Paper 1: Opportunities for systemic change", page 7.

Managing significant national security risks to the critical infrastructure system

This subsection describes how critical infrastructures are increasingly attractive targets to foreign states and other actors that seek to harm New Zealand and New Zealanders. The ability of critical infrastructures to manage these threats without government support is limited given government's unique intelligence and cyber capabilities, which individual infrastructures cannot replicate.

To address these constraints, the Australian Government recently adopted new powers to direct critical infrastructures to take, or refrain from taking, certain measures. In rare cases, it can intervene directly to manage significant national security risks.

New Zealand does not have any equivalent powers and the government has made no decision to introduce them.

Feedback is sought on whether there is a need for such tools and, if so, what form those tools should take and what protections there should be around their use.

Why may it be important for the government to have the power to intervene to assist critical infrastructures in managing significant national security risks?

98. New Zealand faces a more complex geopolitical and national security environment than in recent history. The risk of foreign states – or proxies acting on their behalf – interfering in New Zealand's infrastructure system contrary to our national interests is higher than it has been in a generation and continues to grow.

99. The critical infrastructure system is an attractive target for such interference. Espionage, sabotage and coercion can be – and is – attempted against the system regularly.

100. The government recognises that:

- **a.** all critical infrastructure entities can be susceptible to sophisticated interference efforts by foreign states or state-linked actors. These adversaries have the means to invest far more to exploit one vulnerability than any potential target could invest to reduce all vulnerabilities
- **b.** the government, given its unique understanding of New Zealand's security environment and its sophisticated intelligence and cyber capabilities (underpinned by significant legislative powers), will often be best qualified to detect and disrupt such threats
- **c.** it may not always be possible to work collaboratively with a critical infrastructure owner or operator to manage a risk due to:
  - i. a reliance upon classified information that may not be possible to share
  - ii. disagreement between the government and the critical infrastructure entity over the risk, or the mitigations necessary to manage it
  - iii. a need to act immediately to protect New Zealand's national interests, where consultation or collaboration is not possible given the constraints
  - iv. the infrastructure owner or operator being unwilling to manage the risk.

101. Reflecting these factors, many jurisdictions facing similar threats to New Zealand have adopted – or are considering – extraordinary government powers to support critical infrastructure operators in managing or mitigating national security events. This includes:

a. new, or enhanced, screening mechanisms for foreign investment in critical infrastructure sectors in countries such as Japan, the United Kingdom, Australia, and the United States. These jurisdictions allow high risk investments to have conditions imposed, or blocked, to mitigate significant national security or other risks

b. backstop tools to manage other types of national security risks, with Australia's regulatory regime for critical infrastructures providing the strongest examples.

What tools does the Australian government have to manage significant national security risks?

Australia's Security of Critical Infrastructure Act 2018 includes two backstop tools to support the Australian government in managing significant national security risks to its critical infrastructure system. In general terms, these are:

- a directions power[64], which allows the Minister for Home Affairs to instruct the critical infrastructure's operator to do, or refrain from doing, any activity necessary to eliminate or mitigate a national security risk
- intervention powers to respond to serious cyber security incidents, which allows the Minister for Home Affairs to do, or refrain from doing, any activity necessary to eliminate or mitigate a cyber incident that poses a material risk to Australia's social and economic stability, defence, or national security.[65] This includes the power for Australian government agencies to provide direct support to an infrastructure entity, if necessary, to manage the risk.

As powers of last resort, both the directions and intervention powers are supported by safeguards. For example, the Minister of Home Affairs will not be able to exercise the direction power unless:

- the Australian Security Intelligence Organisation has determined that there is a national security risk to be mitigated
- good faith negotiations have occurred with the critical infrastructure owner or operator
- the direction is proportionate to the risk that exists
- existing regulatory mechanisms cannot be used to address the risk.

Before issuing a direction, the Minister is also required to consult directly with the affected entity and consider (among other matters): costs likely to be incurred by the entity; consequences for competition; and consequences for customers if a direction was issued.

There are also review rights built in, with any directions issued by the Minister subject to judicial review.

64 See Section 32 of Australia's Security of Critical Infrastructure Act 2018, available at: https://www.legislation.gov.au/Details/C2022C00160.

65 See Part 3A of the Security of Critical Infrastructure Act.

How successfully is New Zealand able to manage national security risks in the critical infrastructure system?

102. The government has limited tools to manage significant national security risks to New Zealand's critical infrastructure system. In particular, while the government can intervene to manage a significant cyber threat to New Zealand's critical infrastructure, this power does not extend to the ability to intervene in the management of any other type of significant national security risk.[66]

103. The government largely relies on non-regulatory mechanisms, such as intelligence community briefings, alerts and technical support, to support critical infrastructure owners and operators in managing national security risks. For example, the National Cyber Security Centre supports nationally significant organisations to protect their networks from malicious, advanced, persistent, and sophisticated cyber security threats, including through cyber security outreach and its cyber defence capabilities CORTEX and Malware Free Networks. However, this model relies upon:

    a. the intelligence community being able to provide sufficient information to the critical infrastructure entity to convince them of the risk

    b. the critical infrastructure entity being willing to take steps to mitigate them, even if the costs of mitigation would outweigh the direct costs to the entity of allowing the potential national security event to occur.

104. A regulatory lever that is available applies to overseas investment. Under the Overseas Investment Act 2005:

    a. controlling investments in 'sensitive assets'[67] must satisfy a number of potential tests before they can receive consent. This can include the 'national interest test',[68] which empowers the Minister of Finance to impose conditions on, or block, investments found to be contrary to New Zealand's national interests – including national security interests

    b. other investments in 'strategically important businesses' can be reviewed irrespective of the value of the proposed transaction or size of the equity stake being acquired. Transactions posing a significant risk to New Zealand's national security are able to have conditions imposed or be blocked if conditions are unlikely to adequately mitigate the national security or public order risks.

105. While these are important tools, it does mean that the government's ability to manage national security risks in the critical infrastructure system is limited.

---

66 Section 12(1)(b) of the Intelligence and Security Act 2017 provides the GCSB with the power to do anything necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand, including identifying and responding to threats or potential threats to those communications and information infrastructures.

67 That is, investments that grant a more than 25 per cent interest in sensitive land (such as foreshore or non-urban land of five hectares or more), significant business assets (ordinarily those worth $100 million or more), or fishing quota.

68 The national interest test is always applied to investments in "strategically important businesses", including businesses involved in military or dual-use technology, as well as a number of critical infrastructure sectors including ports or airports, electricity, water, telecommunications, and financial market infrastructure. The national interest test can also be applied to other transactions that are subject to screening under the Overseas Investment Act 2005 on a discretionary basis.

What reforms are already underway that will help address this problem?

106. The Government has a significant programme of work underway to enhance general awareness of national security risks and the ability of businesses and the wider community to mitigate them. This includes the development of New Zealand's first National Security Strategy.

107. This is an important step towards enhancing New Zealand's resilience to national security risks. At this time, however, the Government is not progressing any regulatory reforms that would enhance the government's ability to directly intervene to support the management of such risks in the critical infrastructure system.

The Government would like your views

- Do you think there is a need for the government to have greater powers to provide direction or intervene in the management of significant national security threats against a critical infrastructure? If so:
  - what type of powers should the government consider?
  - what protections would you like to see around the use of such powers to ensure that they were only used as a last resort, where necessary?

Creating clear accountabilities and accountability mechanisms for critical infrastructure resilience

This subsection outlines how any prospective reform requires clear accountabilities for the successful delivery of resilience outcomes, across both government and the private sector. In particular:

- the advantages of the government identifying a Minister and agencies who have responsibilities for the totality of the infrastructure system, with adequate funding to drive coherent policy settings
- the need for obligations that are placed on critical infrastructure entities to be enforceable, to ensure that resilience objectives are met.

The government does not currently have either clear agency accountabilities or the power to enforce cross-sector resilience requirements (where they do exist) across the infrastructure system. This is distinct from sector-based requirements, which are enforceable. No decisions have been made to change either of these settings to date.

Feedback is sought on:

- the need for a responsible agency and/or regulator for the critical infrastructure system, and what form any entity should take
- the need for enforcement mechanisms to compel compliance.

Why may it be important for the government to have clear accountabilities for the resilience of the critical infrastructure system?

108. While a comprehensive, systems-driven policy framework with the kinds of features described in the preceding sections may be important, outcomes will ultimately depend on the framework's implementation by government and industry. This requires clear accountabilities and accountability mechanisms.

109. For the government, this would likely require designating a central, coordinating point responsible for the resilience of the infrastructure system, to include developing appropriate policy and any corresponding regulatory requirements (whether those responsibilities sit within a single or multiple agencies). Relative to the status quo, this should:

a. reduce the risk of fragmented requirements across different infrastructure sectors

b. support coordination of policies that affect the infrastructure system, to ensure that trade-offs between conflicting policy objectives are understood and that the government's overall regulatory settings are coherent

c. ensure greater democratic accountability for system-level resilience.

110. Reflecting these advantages, it is increasingly common among comparable jurisdictions to establish policy and regulatory agencies exclusively focussed on the critical infrastructure system. These include Australia's Cyber and Infrastructure Security Centre, the United States' Cybersecurity and Infrastructure Security Agency and the United Kingdom's Centre for the Protection of National Infrastructure.

111. For critical infrastructure owners and operators, accountability mechanisms are necessary to verify that legal requirements are being met. The absence of such mechanisms can reduce overall compliance (given the high costs of infrastructure investments). It also creates competitive advantages for critical

infrastructure entities that do not meet their obligations (relative to those that do), by allowing them to charge less and grow their market share.

112. Given this, the OECD recommend that governments introduce the following mechanisms to ensure that critical infrastructures comply with their regulatory requirements:

    a. **government monitoring and supervision**, such as regular reporting (which could be public, private, or a mix of both depending on the information being provided), inspections, and performance assessments

    b. **enforcement mechanisms**, which could range from awareness-raising and education in the first instance, to fines and enforceable undertakings for non-performance. At the most extreme end, this could include criminal penalties for severe breaches of regulatory requirements.

113. There are many ways that enforcement mechanisms could be introduced, impacting who incurs legal liability. These include mechanisms targeted at the critical infrastructure entity itself, and/or mechanisms targeted at directors and other responsible individuals (eg. through an expansion of legal obligations on critical infrastructures' board members – such as those that already apply in relation to workplace health and safety).

How successfully has New Zealand created clear accountabilities for the resilience of the critical infrastructure system?

114. Under subsequent Governments, no agency or Minister has had responsibility for developing policy to enhance the resilience of the critical infrastructure system.

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

116. The government agency that is closest to these functions is NEMA, as the agency with policy and operational responsibility for responding to emergencies under the CDEM Act 2002. However, reflecting NEMA's stewardship of the emergency management system, NEMA does not have the mandate, capability, or resources to ensure the resilience of the critical infrastructure system. For example, NEMA cannot:

    a. serve as the coordinating point for policies relevant to the critical infrastructure system's resilience

    b. verify or enforce compliance with obligations under the CDEM Act 2002 (or the proposed Emergency Management Bill)

    c. build or maintain a real-time model of the infrastructure system's dependencies and interdependencies

    d. identify potential national security risks that are either likely to emerge or are already embedded in the infrastructure system, such as those relating to ownership and/or control of critical infrastructure assets or those embedded in supply chains.

117. NEMA also is not, and should not be, a regulator. NEMA's success and trusted position in the community stems from its strong partnerships with local government, communities, iwi, and businesses. There is a

risk that this partnership could be undermined across some or all critical infrastructure sectors if NEMA were also responsible for monitoring and enforcing compliance with resilience requirements.

118. This agency architecture, however, means that there are also limited accountability mechanisms to ensure that critical infrastructure owners and operators are meeting their emergency management obligations consistently. This creates risks of non-compliance, which in turn have the potential to generate systemic risks if outages generated in one sector cascade to another.

What reforms are already underway that will help address this problem?

119. The Emergency Management Bill will extend the general requirement to be resilient to a broader range of entities than those currently designated as lifeline utilities and introduce some new requirements to provide the community with greater assurance that critical infrastructures are resilient. This includes a proposal to introduce reporting, monitoring and evaluation arrangements by which critical infrastructures must provide an annual statement demonstrating their ability to comply with their duties and responsibilities under the Bill.

120. Regulatory reform to enhance resilience would build on these requirements to enforce mandatory minimum resilience standards and enhance information sharing between government and critical infrastructures. This will involve establishing stronger accountability mechanisms to ensure critical infrastructure owners and operators are meeting their regulatory obligations.

The Government would like your views

- Do you think that there is a need for a government agency or agencies to have clear responsibility for the resilience of New Zealand's critical infrastructure system? If so:
  - do you consider that new regulatory functions should be the responsibility of separate agencies, or a single agency?
  - do you consider that an existing entity should assume these functions or that they should be vested in a new entity?
  - how do you see the role of a potential system regulator relative to sectoral regulators?
- Do you think that there is a need for compliance and enforcement mechanisms (eg. mandatory reporting, penalties or offences) to ensure that critical infrastructure operators are meeting potential minimum standards? If so:
  - do you consider that legal obligations should be applied to the entity, to the entity's directors/executive leadership, or a mix of the two?

Appendix A: Glossary

Term	Definition
CDEM	Civil Defence Emergency Management Act 2002
Commerce Commission	The Commerce Commission is New Zealand's competition, consumer and regulatory agency. It has regulatory responsibilities in the electricity lines, gas pipelines, telecommunications, and airport sectors.
Critical infrastructures	Critical infrastructures are the essential and enabling assets, systems, networks, and services that support New Zealanders' wellbeing, now and into the future. They are critical because: • the functioning of such infrastructure is essential for the economy, security, public safety, and the provision for essential public and other infrastructure services; and • the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice: – provision of essential services to public; – the public interest with regards to safety, security and the maintenance of law and order; – the functioning and stability of the nation; and/or – national security.
Critical infrastructure system	The critical infrastructure system describes New Zealand's network of individual critical infrastructures. It reflects the dependencies and interdependencies between infrastructures (ie. the way they are physically, digitally, or logically linked to one another), which mean that the stability of one critical infrastructure is often dependent on the stability of one or more other critical infrastructures.
DPMC	Department of the Prime Minister and Cabinet
Electricity Authority	The Electricity Authority is the primary regulator of New Zealand's electricity market.
EQC	Earthquake Commission
GCSB	Government Communications Security Bureau
MBIE	Ministry of Business, Innovation and Employment
NIWA	National Institute of Water and Atmospheric Research
NEMA	National Emergency Management Agency. This is the agency responsible for coordinating New Zealand's response to natural disasters and other emergencies.
NCSC	National Cyber Security Centre, part of the Government Communications Security Bureau
NZSIS	New Zealand Security Intelligence Service
RBNZ	Reserve Bank of New Zealand, the prudential regulator of New Zealand banks, insurance companies, and financial market infrastructures.
Resilience	The ability for an object or entity to absorb shocks and/or have the capacity to adapt to those shocks and rapidly recover – even if that means providing services in a new way.
Te Waihanga	New Zealand Infrastructure Commission – Te Waihanga

Appendix B: An example of a holistic model for determining infrastructure criticality

Consequence type	Scope of consequence	Scale of consequence				
		Insignificant	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Human (life)	Human health and wellbeing, physical and mental, includes impacts of illness, injury, income, skills, knowledge and the things that allow people to engage in society.	Mild impacts and inconvenience	Local moderate illness or injury with no deaths, or serious hardship for < 1,000 people	Regional/serious illness or injury, 1 death likely, or serious hardship for > 10,000 people	National/serious illness or injury, up to 10 deaths, serious hardship for > 10,000 people	More than 10 deaths, or serious hardship for > 100,000 people
Social and cultural	Social and cultural structures and norms in New Zealand, law and order, cultural identity, community, and social and cultural facilities.	Local public issue and sense of frustration and disadvantage	Regional public issue, loss of community facilities or impacts to social or cultural practices, sense of injustice within communities	National sense of injustice, damage to many communities, social or cultural values challenged, public protests	Damage to social or cultural structures or values for up to 1-year, serious protests/disruptions, or loss of high value heritage.	Long-term or permanent loss of social structures or key cultural values/identity. Civil disobedience and extended disruptions.
Governance and political	Trust in government or management, maintaining credibility and a mandate to lead and/or continue to supply services. Includes international reputation.	Local issue (single region), stakeholder frustration	Issue for < 1 month, with political embarrassment or reputational damage to Government or asset manager, and some loss of confidence	Issue for < 3 months, with loss of confidence in responsible ministers, officials/= or executives	Issue for > 3 months, with loss of confidence and trust in Government or asset manager	Long-term loss of trust in Government or organisational reputation. Impaired ability to govern.

Consequence type	Scope of consequence	Scale of consequence				
		Insignificant	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Natural environment	All aspects of the natural environment to support New Zealand, the planet, and human wellbeing. Includes land, water, plants, animals, and other natural resources.	Minor, very localised impact (eg. < 1 hectare), no residual effects	Local area impact, recoverable, effects last < 3 months	Local/regional impact, effects last < 1 year	Regional impact, effects last > 1 year, some long-term residual impacts	Regional impact > 1 year or long term or permanent loss of ecosystem, species or a natural resource
Economic and people (proxy number of people impacted)	The economic impact to New Zealand (GDP). This is broadly indicated by the number of people impacted directly and indirectly, and may include customers of impacted businesses, suppliers and others. This includes assessment of dependencies and interdependencies.	< 500 people	> 500 people	> 5,000 people	> 50,000 people	> 500,000 people
Physical (proxy replacement value)	The value of the physical (or intangible) asset being assessed. An estimate of the replacement value of the asset (an indicator of impact to the asset owner).	< $10 million	> $10 million	> $100 million	> $1b	> $10b

Appendix C: Compilation of questions for feedback

Prelude: Objectives for and principles underpinning this work programme

- Does more need to be done to improve the resilience of New Zealand's critical infrastructure system?
- Have you had direct experience of critical infrastructure failures, and if so, how has this affected you?
- How would you expect a resilient critical infrastructure system to perform during adverse events?
- Would you be willing to pay higher prices for a more resilient and reliable critical infrastructure system?
- The work programme's objective is to enhance the resilience of New Zealand's critical infrastructure system to all hazards and threats, with the intent of protecting New Zealand's wellbeing, and supporting sustainable and inclusive growth. Do you agree with these objectives? If not, what changes would you propose?
- Do you agreed with the proposed criteria for assessing reform options? If not, what changes you would propose?

Section 1: Background and context

Why a new regulatory approach may be required

- The paper discussed four mega trends: i) climate change, ii) a more complex geopolitical and national security environment, iii) economic fragmentation, and iv) the advent and rapid uptake of new technologies. Do you think these pose significant threats to infrastructure resilience?
- Are there additional megatrends that are also important that we haven't mentioned? If so, please provide details.
- Do you think we have described the financial implications of enhancing resilience accurately? If not, what have we missed?

Section 2: Potential barriers to infrastructure resilience

Building a shared understanding of issues fundamental to system resilience

- How important do you think it is for the resilience of New Zealand's infrastructure system to have a greater shared understanding of hazards and threats?
- If you are a critical infrastructure owner or operator, what additional information do you think would best support you to improve your resilience?
- What do you think the government should do to enable greater information sharing with, and between, critical infrastructure owners and operators?

Setting proportionate resilience requirements

- Would you support the government having the ability to set, and enforce, minimum resilience standards across the entire infrastructure system? If so:
  - what type of standard would you support (eg. requirement to adhere to a specific process or satisfy a set of principles)?
  - do you have a view on how potential minimum resilience standards could best complement existing approaches to risk management?

- Would you support the government investing in a model to assess the significance of a critical infrastructure asset, and using that as the basis for imposing more stringent resilience requirements? If so:
  - what options would you like the government to consider for delivering on this objective?
- what criteria would you use to determine a critical infrastructure asset's importance??investing in a model to assess a critical infrastructure asset's criticality, and using that as the basis for imposing resilience requirements that are more stringent on particularly sensitive assets? If so:
  - what options would you like the government to consider for delivering on this objective?
  - what features do you think provide the best proxies for criticality in the New Zealand context?

Managing significant national security risks to the critical infrastructure system

- Do you think there is a need for the government to have greater powers to provide direction or intervene in the management of significant national security threats against a critical infrastructure? If so:
  - what type of powers should the government consider?
  - what protections would you like to see around the use of such powers to ensure that they were only used as a last resort, where necessary?

Creating clear accountabilities and accountability mechanisms for critical infrastructure resilience

- Do you think there is a need for a government agency or agencies to have clear responsibility for the resilience of New Zealand's critical infrastructure system? If so:
  - do you consider that new regulatory functions should be the responsibility of separate agencies, or a single agency?
  - do you consider that an existing entity should assume these functions or that they should be vested in a new entity?
  - how do you see the role of a potential system regulator relative to sectoral regulators?
- Do you think there is a need for compliance and enforcement mechanisms (eg. mandatory reporting, penalties, offences) to ensure that critical infrastructure operators are meeting potential minimum standards? If so:
  - do you consider that these should be applied to the entity, to the entity's directors/executive leadership, or a mix of the two, and why?

Cabinet External Relations and Security Committee

Minute of Decision

Acting Urgently to Strengthen the Resilience of New Zealand's Critical Infrastructure System: Release of Discussion Document

Portfolio **National Security and Intelligence**

On 6 June 2023, the Cabinet External Relations and Security Committee (ERS):

1 **noted** that in September 2022, the government announced its intention to undertake consultation in the first half of 2023 on the limitations of the current regulatory approach to enhancing infrastructure resilience [CAB-22-MIN-0362];

2 **noted** that in December 2022, ERS agreed to fast-track measures to enhance the cyber resilience of critical infrastructure ahead of work on broader resilience, and noted that a discussion document will be submitted to Cabinet for approval in the first half of 2023 [ERS-22-MIN-0063];

3 **agreed**, in light of the broader vulnerabilities in New Zealand's critical infrastructure system exposed by Cyclone Gabrielle, to progress, as a high priority, the development of a single comprehensive piece of legislation to enhance critical infrastructure resilience against all hazards and threats, with a view to its introduction in early 2025;

4 **agreed** to the release of the discussion document *Strengthening the Resilience of Aotearoa New Zealand's Critical Infrastructure System* (the discussion document), and the associated summary discussion document, both of which are attached to the paper under ERS-23-SUB-0025, for public consultation;

5 **authorised** the Minister for National Security and Intelligence to approve minor amendments and refinements to the discussion document and summary discussion document prior to their public release;

6 **noted** that the public consultation period is intended to commence from early June 2023 and conclude in early August 2023, with officials undertaking a range of public meetings over that period;

7 **noted** that feedback on the discussion document will inform the development of options to enhance critical infrastructure resilience, ahead of final advice being provided to Cabinet in 2024;

8 **noted** that there will likely be financial and legislative implications associated with any policy changes arising from this further policy advice to Cabinet.

Janine Harvey
Committee Secretary

Present:
Rt Hon Chris Hipkins (Chair)
Hon Carmel Sepuloni
Hon Kelvin Davis
Hon Grant Robertson
Hon Michael Wood
Hon Andrew Little
Hon David Parker
Hon Nanaia Mahuta
Hon Kieran McAnulty
Hon Ginny Andersen

Officials present from:
Office of the Prime Minister
Officials Committee for ERS

Cabinet

Minute of Decision

Report of the Cabinet External Relations and Security Committee: Period Ended 9 June 2023 (Part 1)

On 12 June 2023, Cabinet made the following decisions on the work of the Cabinet External Relations and Security Committee for the period ended 9 June 2023:

ERS-23-MIN-0025 **Acting Urgently to Strengthen the Resilience of New Zealand's Critical Infrastructure System: Release of Discussion Document** CONFIRMED
Portfolio: National Security and Intelligence

[redacted]

Rachel Hayward
Secretary of the Cabinet