FEEDBACK TO

THE DEPARTMENT OF PRIME MINISTER & CABINET

ON THE

STRENGTHENING THE RESILIENCE OF AOTEAROA NEW ZEALAND'S CRITICAL INFRASTRUCTURE SYSTEM DISCUSSION DOCUMENT

BY

FOODSTUFFS (NZ) LIMITED

AUGUST 2023

Sent by email: infrastructureresilience@dpmc.govt.nz

Introduction

1. This submission is made by Foodstuffs (NZ) Limited on behalf of Foodstuffs North Island Limited and Foodstuffs South Island Limited, which are each one hundred per cent New Zealand owned retailer co-operatives (together the "Foodstuffs co-operatives"). The regional co-operatives jointly own Foodstuffs (NZ) Limited which represents the Foodstuffs co-operatives' interests in national policy and input on public policy matters.

2. The Foodstuffs co-operatives own and develop retail stores which are franchised to co-operative members. Our co-operatives' retail brands include: PAK'nSAVE, New World, Four Square, Raeward Fresh, and On-the-Spot. Our wholesale brands, servicing non-member businesses, are Gilmours and Trents.

3. As part of their business operations the Foodstuffs co-operatives own many buildings located all around New Zealand, including hundreds of supermarkets and grocery stores, a dozen or so distribution centres and other warehouses; a number of support offices; and a food manufacturing facility. They also run extensive grocery distribution operations with truck fleets involved in primary and secondary freight.

4. Foodstuffs operations are highly dependent on third-party infrastructure, including utilities such as electricity, water, and telecommunications, and transport infrastructure including roading, rail, and ports.

PRELUDE: OBJECTIVES FOR AND PRINCIPLES UNDERPINNING THE WORK PROGRAMME

Does more need to be done to improve the resilience of New Zealand's critical infrastructure system?

5. Yes. The consultation document itself, and prior analysis such as Rautaki Hanganga o Aotearoa 2022-2052 published by Te Waihanga, the Infrastructure Commission, in 2022, and the NZ Lifelines Council's National Vulnerability Assessment Report published in 2021, all provide evidence that New Zealand's critical infrastructure is exposed to numerous risks, many of which would be highly impactful at a regional or national level. Much work needs to be done to strengthen resilience and reduce identified vulnerabilities.

6. We note the consultation document outlines a number of principles which will underpin the future work programme to strengthen resiliency in addressing the risks, including:

    c. critical infrastructure owners and operators are best placed to understand and manage the risks facing their organisation, but government has a responsibility to partner with industry to:
        i. ensure industry has a good understanding of the hazards and threats they face, and
        ii. support owners and operators in making rational investment decisions.

    d. Resilience should be enhanced at least cost to business, consumers, and government by:
        i. using non-regulatory mechanisms whenever possible
        ii. taking advantage of existing sector-based regulatory regimes whenever possible.
        iii. developing proposals that build on existing and forthcoming law.
        iv. ensuring that any new potential regulatory approach is proportionate and dynamic.

    e. The cost of enhancing resilience should, whenever possible be paid by those who benefit from the investment.

7. We support these stated principles and will refer to them in later questions where relevant.

Have you had direct experience of critical infrastructure failures? If so, how has this affected you?

8. Yes. Owning many buildings and other physical assets around New Zealand and being highly reliant on the provision of roading infrastructure and utility services to maintain our day-to-day business operations, we are frequently exposed to failures in critical infrastructure, especially road closures affecting goods distribution and electricity and telecommunications outages affecting our wider business operations.

9. Severe weather events are the most frequent causing disruption to normal service, occurring on an almost monthly basis somewhere in the country, but usually have minor short-term impact. We have also dealt with many larger events including in recent times:
    - the Canterbury earthquakes which caused severe damage to Foodstuffs South Island Limited's Christchurch distribution centre and a number of its Christchurch-sited supermarket properties – each requiring either a total rebuild or substantial repairs.
    - the Kaikoura earthquake event which closed a large section of the state Highway between Picton and Christchurch and disrupted transport operations, with both Foodstuffs and third-party suppliers having to use alternate routes of much greater distance for a prolonged period of time.
    - Cyclones Hale and Gabrielle, which caused significant roading, electricity, and telecommunication outages in the affected communities.

10. As a result of these events, and the COVID-19 pandemic response, we have developed a reasonably good understanding of potential vulnerabilities, and extensive experience with crisis management, which has strengthened our own resilience and business continuity planning.

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

11. This will depend on the individual circumstances, including: the size, scale, and nature of the event and its location; the nature of the critical infrastructure that is impacted, its underlying resilience and the level of redundancy available within the wider infrastructure system; and the availability of alternate services if needed e.g. if a road becomes impassable, whether there was an alternate route providing access, albeit impaired.

12. If events are localised and cause minor damage or disruption e.g. disruption to electricity transmission due to power lines falling in a storm, we might expect normal services to be resumed quickly i.e. in a matter of hours or days. However, at the other end of the scale, such as a large earthquake triggering Tsunami, we would anticipate significant outages across all the key utilities and service disruption at a level that would take weeks, months, or years to fully restore all infrastructure to pre-event levels.

13. Even with significant redundancy built in, some events can be so large, and with such significant impact, that it is simply not realistic to expect critical infrastructure to perform through the event, in the immediate aftermath, and for some time later. For example, in the event of a rupture of the Alpine fault, we would expect all three major highways providing access to the West Coast to have multiple blockages due to landslides. In this scenario, supplies of essential goods would need to be transported by air or sea for a considerable length of time. A similar scenario is anticipated in terms of a major earthquake affecting the Wellington region.

14. In this sense, an expectation that critical infrastructure can be strengthened to the point it will continue to perform during and after a very major event is unrealistic. Accordingly, the emphasis needs to be on identifying vulnerabilities and taking steps to reduce these to the greatest extent practical, and preparing for the speediest recovery practical when critical infrastructure fails.

15. The Civil Defence Emergency Management Act 2002 and the Emergency Management Bill require lifelines sectors (critical infrastructure entities in the Bill) to function to the greatest extent possible during and after an emergency. We think this is a pragmatic approach, signalling an expectation that all practical steps will be taken to maintain service while acknowledging service will be compromised.

16. We are open to working with central and local government and other relevant parties such as the lifeline sector (national and regional) to plan for greater resiliency in response to significant threats.

Would you be willing to pay higher prices for a more resilient and reliable system?

17. Yes. We agree that upfront investment in resilience makes good financial sense as it will reduce impacts when events occur, as well as recovery time and cost. A fast recovery is desirable in terms of maintaining business operations and public confidence. Critical infrastructure providers should be encouraged to adopt a risk-management based approach, so their investment is optimally targeted.

The work programme's objective is to enhance the resilience of New Zealand's critical infrastructure systems 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?

18. We agree with these over-arching objectives along with the additional objectives set out in the consultation document, including the intent to extend the work programme to cyber risks.

19. We believe the initial focus should be on addressing "significant" hazards and threats.

Do you agree with the proposed criteria for assessing reform options? What changes do you propose?

20. The proposed criteria for assessing options are:
    - how well the option enhances infrastructure resilience?
    - how it changes the regulatory burden, and creates regulatory certainty across the infrastructure community?
    - how the option changes the regulatory system's complexity, including considerations of cost?

21. We agree that effectiveness in enhancing resilience, providing regulatory certainty, and the complexity of implementation and cost, are appropriate criteria for assessing each reform option.

SECTION 1: BACKGROUND AND CONTEXT

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 have not mentioned? If so, please provide details.

22. We agree that the identified mega trends are all valid.

23. A review against the World Economic Forum's "*Global Risks Report 2023*" would be appropriate for completeness, if this has not already been done?

24. Other trends that could be considered as mega trends are:
    - Inflationary pressures increasing costs, especially labour and material costs for building and construction. This will impact the cost of strengthening resiliency, as well as the related business cases for investment. Roading is hugely expensive, as is water and hospital infrastructure which in New Zealand are both now aged and massively underinvested.
    - Long-term labour and skill shortages driven by changes in the nature of work (greater demand for technical skills), and changes in demographics (smaller proportion of the population in work as a consequence of an ageing population), impacting capacity to complete the necessary work.

Have we described the financial implications of enhancing resilience accurately?

25. We agree that increasing annual investment in high-quality critical infrastructure resilience should save money in the long-term. This is underpinned by the time value of money concept.

26. The consultation document theorises that investments to improve resiliency will be shared by shareholders, employees, customers, and government (tax-payers) where government owns the relevant infrastructure. Again this is rational. There is a cost to capital and investments in strengthening resilience will result in one or more and maybe all of the following: higher product pricing, reduced dividends to shareholders, lower employee payments or reduced increases over time.

27. The consultation document suggests that cost increases would, in most cases, be gradual because assets are long-lived and investments to enhance their resilience will also occur over lengthy time periods. This is an assumption as the time allowed for investment to strengthen resiliency will, to a degree, depend on government expectations and may involve government direction. In this respect it is helpful that government acknowledges the potentially significant financial implications of strengthening resilience and anticipates that the investment will occur over reasonably long time-horizons. We encourage the government to consider whether this should be framed as a principle?

SECTION 2: POTENTIAL BARRIERS TO INFRASTRUCTURE RESILIENCE

Building a shared understanding of issues fundamental to system resilience

How important do you think it is to have a greater shared understanding of hazards and threats?

28. We believe this is very important. If we collectively understand where the risks and vulnerabilities lie, we are all better placed to manage those risks, at an enterprise level, sector level, and wherever co-dependencies exist.

29. The New Zealand Lifelines Council has undertaken valuable work producing a National Vulnerability Assessment however the 2021 report is high-level, is now outdated, has information gaps, and is not widely known about.

30. Foodstuffs would meet the definition of a “critical customer” of the lifeline sector - an organisation that provides services deemed critical to the functioning of communities, but we do not have a good understanding of the vulnerabilities of the third party critical infrastructure on which we rely for business continuity. It would be extremely helpful to our own planning to have a better understanding of where those vulnerabilities lie, the level of risk involved, and the anticipated timelines for services to be restored if service disruptions are anticipated.

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

31. As above, having a greater understanding of where the utility service providers vulnerabilities lie, particularly the assets vulnerable to "single point failure" and their geographic location, would be extremely helpful for our contingency planning.

32. As a case study, after the failure of critical fibre cables during the respective Hale and Gabrielle cyclones due to earth movement, Foodstuffs North Island Ltd lost internet connectivity with some stores in the Gisborne, Wairoa, and Northland districts. The affected stores did not have any ability to communicate with the support office or connect to a payment service. To resolve this issue the Company hastily purchased Starlink satellite devices and EFTPOS units with suitable specifications to connect with these but had to arrange to have the equipment flown in by helicopter due to road closures (other single points of failure). The problems were solved but the fixing took time to organise and execute. For contingency purposes, Foodstuffs is considering whether to equip other at-risk stores with Starlink devices, however we do not know enough about our provider's Internet service vulnerabilities to make informed decisions.

33. We have engaged with utility suppliers but have mixed responses from them about sharing this type of information. It would be helpful if the lifeline utilities were required to share information with "critical customers" so the parties have a shared understanding of risks and vulnerabilities and can negotiate contingency arrangements or otherwise make their own plans from a more informed perspective.

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

34. Government could play a role in initiating and facilitating forums for critical infrastructure entities which have co-dependencies to come together to share information on risks and vulnerabilities and plan resilience strengthening activities. However we note that this role is already performed, to a degree, by the New Zealand Lifelines Council at a national level and by regional lifeline groups. There needs to be a discussion about whether there is a need for government to take a more direct lead in co-ordinating resiliency strengthening or provide greater support to the lifeline sector to lead this work with government input.

35. Our initial view is that the government could create a statutory obligation for the lifeline sectors to engage with each-other to co-ordinate resilience strengthening work where there are co-dependencies, with the intention that the lifeline sector leads this effort with greater funding support from government. As we understand, the sector currently relies on sponsorship, including from government agencies, and "in-kind" contributions from members. A more sustainable funding model is needed. There is a large amount of public good in the work undertaken, so there is a strong justification for public funding contributions.

36. The relevant agencies would continue to be heavily involved and would contribute additional resourcing where needed. Additionally, government needs to share its own research and other intelligence to assist the private sector with its own resilience strengthening. A scenario-driven approach would be useful here: i.e. what are the risks and probabilities, by locality.

37. This approach is consistent with principles c (i)&(ii) – critical infrastructure owners and operators are best placed to understand and manage the risks facing their organisation, but government has a responsibility to partner with industry to ensure industry understands the hazards and threats faced and is supported in making rational investment decisions.

38. As discussed earlier, lifeline utilities should also be required to share relevant information on risks and vulnerabilities with critical customers. A statutory obligation would ensure this occurs.

39. The relevant statutes should be reviewed to ensure that they assist collaborative planning and do not hinder it. In particular, the Commerce Act 1986 could state more directly that competitors are permitted to share information and work together for the purposes of emergency planning and response without the risk of breaching competition rules.

40. Related to this, government could support the regime by ensuring sensitive data, when shared, is protected from improper use e.g. for anti-competitive purposes. Critical infrastructure providers will be more open to sharing sensitive information if such protections are afforded.

41. Government also undoubtedly has a role to play in communicating risk to the wider business sector and general public, so they have a good general understanding of risks, realistic expectations about service impacts post-events, and are encouraged and assisted to take steps to be prepared for service outages.

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 (e.g. 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?

42. Resiliency is about good risk management and there are strong commercial incentives for businesses to manage their risks, however a benefit of government prescribing standards is that all obligated parties would know what is expected of them and market competitors would have the same obligations, removing competitive risk. In this sense, standards set a baseline for the expected behaviour, as well as ensuring a level playing field among competitors.

43. Critical infrastructure owners and operators should identify and manage risks at an enterprise level. We are familiar with models operating in other spheres – the Food Act 2014 requires all food businesses to adopt a risk-management framework to identify and manage food safety risks to protect public health, while the Health and Safety at Work Act 2015 imposes a duty on persons conducting a business or undertaking to ensure the health and safety of workers by identifying, then eliminating or minimising, health and safety risks.

44. Adoption of or alignment with existing resilience standards should be considered before new bespoke standards are developed. From an IT perspective, there is already a New Zealand government standard for information security (the New Zealand Information Security Manual) which sets out the controls that providers are required to have in place for information security assurance in dealings with government. The obligation to comply with this standard could be extended to critical infrastructure providers. On a broader front, a number of international standards for resilience already exist. These may be suitable for adoption to support a standardised approach to strengthening resiliency outside of the cyber-risk sphere.

45. If there is to be a statutory obligation for critical infrastructure owners and operators to share information and collaborate with each-other and others to strengthen resiliency and manage risks across the wider community, a principle-based approach is recommended. Principles could include an obligation to be honest and transparent about resiliency risks, act in good faith in dealings with other relevant parties, and respect the confidentiality of others' information etc.

46. We would be cautious about implementing minimum performance standards i.e. expected service levels, during or after an event, as there are simply too many unknowns and variables, many beyond the control or influence of critical infrastructure owners and operators, to have confidence they could be achieved.

47. As previously stated, it can be expected that a lot of critical infrastructure will fail during a large event. The focus should be on reducing risk, and planning for the readiness, response, and recovery phases. Additionally, government-mandated performance standards may be inconsistent with principles c and d.

48. If performance standards are to be pursued, there will need to be adequate consultation with affected parties to understand the operational challenges faced when events occur, as well as the limitations of planning processes. As such, defences would be needed for non-performance on justifiable grounds.

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?

49. It is essential to understand which assets are critical for the on-going provision of essential services, the risks they face, and the anticipated impact if specific risks eventuate. This is a necessary precursor to effective management of the identified risks. As a starting point we recommend that government funds the New Zealand Lifeline Council to review and update the National Vulnerability Assessment Report last published in 2021. This report needs to be reviewed and updated in the context of the mega trends that have been identified in the consultation document and feedback provided, and to take account of all relevant scientific research published in the intervening period. There should be commitment to fund the National Vulnerability Report on an ongoing basis, at regular reporting intervals i.e. a 3-5 year cycle. Again, this approach would be consistent with principles c (i)&(ii).

50. We note that the Emergency Management Bill provides powers for the Minister to recognise new critical infrastructure. The National Vulnerability Assessment would provide valuable information allowing government to identify where gaps in the designation of critical infrastructure exist.

51. In terms of criteria for determining a critical infrastructure's importance, we would suggest:
    - Criticality, in terms of the importance of the infrastructure in supporting essential public services.
    - Vulnerability, as determined through the National Vulnerability Assessment. This should include assessment of both the severity of impact if a large event occurs, and the probability of such events.
    - Redundancy within the wider infrastructure system if a specific piece of infrastructure breaks.
    - The practicality of strengthening resilience and cost. Replacing assets may be more cost-effective.

52. Following on from the identification of critical infrastructure, industry needs to understand whether government will support critical infrastructure owners and operators to strengthen the resiliency of key assets if commercial business cases for the recommended investment do not align. In this case, financial support may make the difference as to whether the investment is made and/or its timing.

Managing significant national security risks to the critical infrastructure system

Does the government need 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?

53. The government already has significant powers under the Civil Defence Emergency Management Act 2002, and proposed Emergency Management Bill, during times of emergency, including the Minister having "general powers of direction" and designated officials having powers related to: the evacuation of premises/places; entry to premises; closing of roads and public places; requisitioning of private property; giving directions that must be followed; requiring assessment of structures; and carrying out inspections in relation to property, among others.

54. These existing powers are wide sweeping and significant, so it is unclear what gaps the government may be alluding to, and what additional powers the government might be contemplating. It would be helpful if the next consultation on options detailed this to a greater degree including providing scenarios for industry to respond to.

55. It is important that there are safeguards to protect against the improper use of what are already very extensive powers. However we have limited expertise in this area of law so we will leave it to others to comment.

56. For its part, Foodstuffs envisages significantly increased security risks in the aftermath of a large scale event, particularly in relation to supermarkets as repositories of food i.e. potential for looting etc. In this regard, government planning needs to contemplate government-provisioned security at vulnerable sites.

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:

- Should the regulatory functions be the responsibility of separate agencies or a single agency?
- Should an existing entity assume these functions, or should they be invested in a new entity?
- How do you see the role of a potential system regulatory relative to sectoral regulators?

57. We think it is sensible to have a single agency providing stewardship for the resilience system for relevant risks. NEMA currently has the mandate for the overall management of readiness and response to events involving natural disasters. It makes sense to extend its remit to the oversight of resilience strengthening for these events. At a practical level, co-ordination occurs via the National Lifelines group structure, and we see that continuing, albeit with wider scope if new critical infrastructure entities are designated under updated legislation. The National Cyber Security Centre co-ordinates the response to cyber security threats. We support extending its remit to resilience strengthening in the cyber sphere. This aligns with principle d – taking advantage of existing regulatory regimes and resilience is strengthened at least cost.

58. This leaves the question of where pandemic, epidemic-type events lie. During the COVID-19 pandemic the Ministry of Health took the lead role. We note that a Royal Commission of Inquiry into the COVID-19 response is currently underway and will make recommendations that will need to be considered. For its part, Foodstuffs would welcome stronger engagement with business than which occurred during the response.

Do you think there is a need for compliance and enforcement mechanisms (e.g. mandatory reporting, penalties, offences) to ensure that critical infrastructure operators meet 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?

59. It is difficult to respond to questions about compliance and enforcement and mandatory reporting without a better understanding of what proposed and who will have to comply. In this regard we will wait to see policy proposals before providing comment.

End.