Te Kāwanatanga o Aotearoa
New Zealand Government

Enhancing the cyber security of New Zealand's critical infrastructure system

Digitally resilient critical infrastructure services to power New Zealand's economy and protect our communities

FEBRUARY 2026 | DISCUSSION DOCUMENT

Why is the Government considering a new approach to the cyber security of critical infrastructure?

Cyber risks are generally not well understood or collectively managed to a consistent level across New Zealand's critical infrastructure system. These risks are escalating due to changing technology, economic instability and a more volatile geopolitical environment.

The impact of cyber harm is also intensifying, with a rise in reported financial losses[1] and a global increase in cyber attacks that severely disrupt or even halt the operation of critical infrastructure, paralysing the delivery of essential services to businesses and communities. Beyond downtime and data loss, consequences of a cyber incident can include public health risks, social unrest, reduced trust in government and erosion of strategic advantage.

New Zealand's critical infrastructure system – encompassing everything from the electricity grid, transport system and telecommunications networks to health services and financial payment systems – is the lifeblood of our country. Protecting this infrastructure against cyber threats is paramount to New Zealand's economic growth and prosperity and deserves renewed attention given the perilous threat landscape we face today.

Cyber criminals are using increasingly sophisticated tools to extort ransoms or exploit data, while malicious state actors are targeting critical infrastructure for espionage as well as for political and military purposes. This type of activity is not hypothetical but becoming more common and harder to detect – posing a significant risk to both our national and economic security.

In October 2025, New Zealand's National Cyber Security Centre (NCSC) joined international counterparts in drawing attention to a campaign of malicious cyber activity targeting critical infrastructure entities globally. Known as Salt Typhoon, this People's Republic of China (PRC) Government-affiliated threat group targets critical infrastructure to conduct espionage and pre-position for disruptive activity in the event of heightened tensions or conflict. Salt Typhoon activity has been observed in New Zealand and exemplifies the urgent need to address cyber risk as a core business risk.

New Zealanders implicitly understand the risk, highlighted by attacks such as Manage My Health, and rank both cyber incidents and critical infrastructure failure as material national risks.[2] Doing more to address these risks is therefore a key focus of the New Zealand Cyber Security Strategy 2026–2030[3].

New Zealand currently takes a predominantly voluntary approach to cyber security, with tools and guidance provided by the NCSC to help critical infrastructure entities understand and manage their cyber risks. However, the level of investment in cyber security across the critical infrastructure system is not always commensurate with the threats faced.

This discussion document is an invitation to shape a future in which New Zealand and the services that our people depend on every day stand cyber resilient amid the global challenges of the digital age.

We encourage you to critically engage with the ideas and proposals in this document to ensure any approach we progress is appropriate for New Zealand. Your contributions will build the foundations for a practical, flexible and responsive regime that embeds the principles of trust and cyber security into every layer of our critical infrastructure system.

With thanks for your valuable input,

Rt Hon Christopher Luxon
Minister for National Security and Intelligence

1 National Cyber Security Centre. (2025). *Rise in financial losses reported to the NCSC*. https://www.ncsc.govt.nz/news/rise-in-financial-losses-reported-to-the-ncsc
2 Ipsos. (2024). *2024 National Risks Public Survey: All threats & hazards*. https://www.dpmc.govt.nz/sites/default/files/2024-09/2024-National-Risks-Public-Survey-All-Threats-and-Hazards-Report.pdf
3 Department of Prime Minister and Cabinet. (2026). *New Zealand's Cyber Security Strategy 2026-2030.* https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2026-2030

The infrastructure that sustains New Zealand's economy and society is increasingly vulnerable to cyber attack

Cyber attacks cannot always be publicised, but New Zealand's infrastructure has been targeted. Recent examples include the NZX cyber attack in 2020 and the Waikato District Health Board ransomware attack in 2021, which disrupted healthcare for around 400,000 people.

The critical infrastructure supply chain also creates vulnerabilities. In 2024 a CrowdStrike software update caused a widespread IT outage for some Microsoft customers, leading to disruption across sectors including finance, healthcare and transport. While not a result of malicious activity, the incident highlights the reliance on the digital supply chain. More recently, the attack on Manage My Health compromised the personal data of up to 126,000 New Zealanders. Manage My Health provides services to some District Health Boards. While there have not been reports of disruption to critical health services, this attack highlights that vulnerabilities in supply chains can translate to vulnerabilities for critical infrastructure entities.

Global concern about targeting of critical infrastructure for cyber espionage or sabotage has become more acute. In 2023, successful infiltration of US critical infrastructure networks was attributed to an advanced persistent threat group linked to the PRC, known as Volt Typhoon. The US assessed this activity was part of a broader campaign to stealthily compromise multiple sectors (including communications, energy, transportation and water systems) and maintain long-term access to disrupt operations in the event of a crisis or conflict.

In 2024, the US confirmed that another advanced persistent threat group affiliated to the PRC, known as Salt Typhoon, had compromised the networks of at least nine major telecommunications providers, enabling broad access to users' communications as part of an espionage campaign.

New Zealand's critical infrastructure is not immune – there is evidence of Salt Typhoon targeting New Zealand entities too. Our critical infrastructure could be vulnerable in a similar way as documented in the US and other countries.[4]

Technology is exacerbating cyber risks

The adoption of new technologies facilitates greater automation, better remote monitoring and management of infrastructure assets and greater connectivity. However, technological innovation has also driven the convergence of operational technology (OT) and information technology (IT) systems. This integration enables malicious actors to access systems controlling industrial equipment and processes to disrupt critical infrastructure operations without even setting foot in New Zealand.

The continued and widespread use of legacy infrastructure also creates vulnerabilities:

- Of private sector experts interviewed in 2024 on their organisation's security, 80 percent revealed that their organisation did not have basic cyber hygiene in place to protect their OT[5].
- Data from the Commerce Commission indicates that approximately 35 percent of SCADA assets (a type of OT) are at or nearing the end of their life. Such assets tend to no longer be supported by the original supplier, creating vulnerabilities that can be used by malicious actors to access and compromise core IT networks.

[4] Cybersecurity and Infrastructure Security Agency. (2024). *PRC state sponsored cyber activity: Actions for critical infrastructure leaders*. https://www.cisa.gov/sites/default/files/2024-03/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c_0.pdf

[5] Parmar, B. (2024). *Improving cyber defence for critical national infrastructure in New Zealand* (Master's thesis). The University of Waikato. https://researchcommons.waikato.ac.nz/server/api/core/bitstreams/d1c6b6b7-3c26-4c3c-a0aa-f603fa960334/content

Market forces may not be driving the appropriate level of investment in cyber security

Underinvestment in cyber security is a rational response to several market forces:

- The costs of enhancing cyber security are borne directly by critical infrastructure entities and the value is often not realised until an incident occurs, whereas the cascading costs of disruptive cyber incidents are distributed more widely across the economy.
- Many of New Zealand's critical infrastructure entities are monopolies or oligopolies, reducing consumers' power to drive investment.
- An entity's level of cyber security is not visible to consumers and does not serve as a market differentiator between services, allowing critical infrastructure entities to underinvest in cyber security and offer cheaper but less-secure services.

Current regulatory settings are not designed to drive a consistent uplift in cyber security across the critical infrastructure system

New Zealand largely relies on non-regulatory approaches to manage cyber risks to our critical infrastructure system. While there are pockets of regulatory reform under way to address cyber risks in certain sectors, there is no single piece of legislation that mandates enforceable minimum cyber security requirements to achieve a consistent and enhanced level of cyber security across the entire critical infrastructure system.

The measures proposed in this discussion document are not intended to replace or usurp current work to introduce sector-specific regulatory requirements for cyber security, including:

- The Reserve Bank of New Zealand (RBNZ) is working to enhance existing requirements for prudentially-regulated entities via the Deposit Takers Act 2023.[6]
- The New Zealand Customs Service is progressing a Border Security Bill, part of which seeks to strengthen the Customs-controlled area regime at maritime ports and airports, including establishing information security requirements.

Cyber incidents can cascade quickly across the entire economy

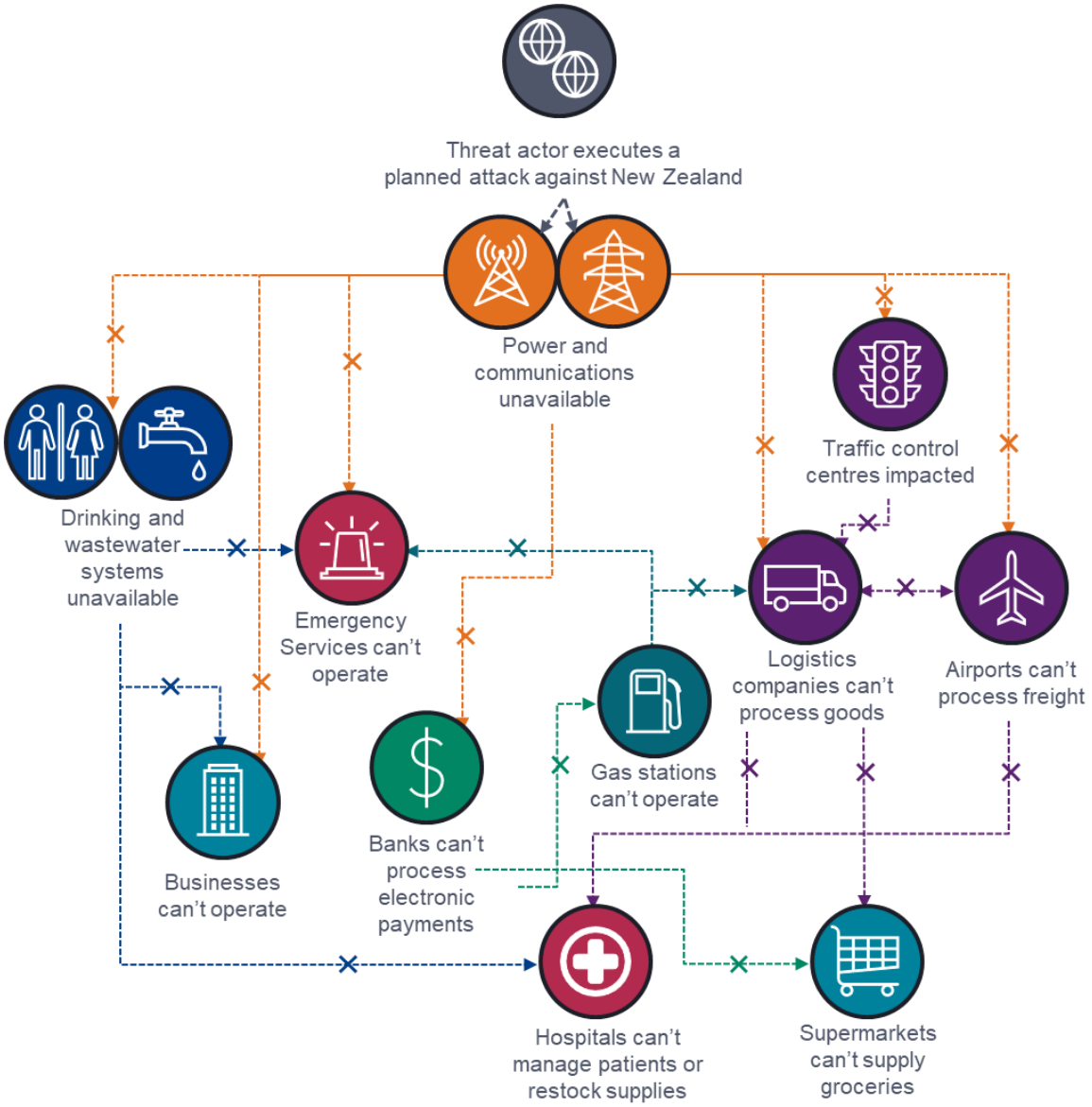
Technology has also increased interdependencies between critical infrastructure, amplifying the cascading impact of cyber incidents (see Figure 1 on page 5). A single vulnerability can trigger widespread outages across multiple essential services, with costs felt far beyond the entity initially affected.

In November 2023, Australia's largest port operator, DP World, experienced a cyber attack that forced the company to disconnect its systems from the internet and halt operations at its major ports in Melbourne, Brisbane, Sydney and Fremantle. The disruption impacted Australia's import and export capacity, resulting in a backlog of over 30,000 shipping containers that took seven days to clear after systems came back online.

Following the incident, the Australian Cyber Security Centre updated its advice on a previously disclosed vulnerability. Cyber security commentators indicated DP World had not patched this known vulnerability at the time of the incident.

[6] The Deposit Takers Act 2023 is currently planned to come into effect in 2028. The RBNZ will issue standards including relating to operational resilience and risk management.

FIGURE 1: **CASCADING FAILURES THAT A CYBER INCIDENT CAN TRIGGER DUE TO INTERDEPENDENCIES WITH OTHER CRITICAL INFRASTRUCTURE SECTORS**



New Zealand's approach is not keeping pace with other countries

New Zealand stands out from other advanced economies in not using dedicated legislative mechanisms to protect critical infrastructure from cyber harm (see Figure 2 for a comparison of global practice).

This damages New Zealand's security and competitiveness. New Zealanders and overseas investors alike need reassurance that New Zealand's critical infrastructure is well prepared to withstand and quickly recover from cyber incidents.

Global monitoring tools reinforce the need to align with close partners and consider regulatory action to improve the cyber security of New Zealand's critical infrastructure:

- The National Cyber Security Index ranks New Zealand 49th in the world and the lowest of the Five Eyes partners.[7] New Zealand ranks particularly poorly on factors relating to the cyber security of our critical infrastructure and cyber crisis management.
- The Global Cybersecurity Index measures the adequacy of countries' approaches to cyber preparedness. New Zealand ranks in the third tier, as compared to Five Eyes partners and peers in the Asia-Pacific region, who rank in the first tier.[8]

FIGURE 2: **INTERNATIONAL COMPARISONS**

Australia regulates its critical infrastructure through the Security of Critical Infrastructure Act 2018, which requires entities to register their assets, report cyber incidents, implement a risk management plan (including cyber standards) and comply with government assistance powers in response to serious incidents. Enhanced cyber security obligations also apply to systems of national significance.

The European Union uses the NIS2 Directive to require critical infrastructure entities to implement risk management measures, report cyber incidents, maintain incident response capabilities and have a designated officer.

In the UK, the Cyber Security and Resilience Bill was recently introduced to Parliament to set more robust cyber security requirements akin to the NIS2 Directive, enhance incident reporting obligations and establish executive powers to issue directions in response to cyber threats.

In Singapore, the Cybersecurity Act 2018 established a framework to protect critical information infrastructure against cyber threats. Regulated entities must implement standards, conduct regular audits and risk assessments, report incidents, participate in cyber exercises, appoint a chief information security officer and share threat intelligence.

In Canada, Bill C-8 was recently introduced to Parliament to create a cyber security regime for federally regulated critical infrastructure. It will require designated operators to establish a cyber security programme, mitigate supply chain and third-party risks, report cyber incidents and comply with cyber security directions to protect a critical cyber system.

[7] e-Governance Academy of Estonia. (2025). *National Cyber Security Index – Countries.* https://ncsi.ega.ee/ncsi-index/?order=rank&type=c

[8] New Zealand is the only developed economy listed in Tier 3. See International Telecommunication Union. (2024). *Global Cyber Security Index 2024*. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

What is this consultation about?

This discussion document seeks feedback on two questions:

- **What are the infrastructure services most critical to our economy and communities that they should be safeguarded against harm?**
- **What should the depth of the cyber defences of these infrastructure services be?**

In response to the first question, the Section 1 sets out an approach for defining critical infrastructure in law to create certainty for infrastructure entities and the pubic as to what critical infrastructure is.

In response to the second question, Section 2 sets out **six proposed voluntary and mandatory measures** that could be adopted independently or as a package to enhance the cyber security of the critical infrastructure system (once it is defined).

The measures focus on delivering three outcomes:

- an improved understanding of threats and vulnerabilities by critical infrastructure entities and government (measures 1-4)
- a minimum level of cyber risk management by all critical infrastructure entities (measure 5)
- effective management of cyber threats impacting national security by critical infrastructure entities (measure 6)

Section 3 sets out the proposed approach to monitoring compliance with any mandatory measures that are adopted to ensure that they are having the desired effect.

Consultation[9] and targeted engagement undertaken in 2023 and 2024 informed the development of these measures, as did insights from international partners who have developed and implemented similar regimes – particularly Australia's Security of Critical Infrastructure Act 2018.

Measures have been evaluated against criteria that reflect the objectives and principles of this work. This detail is set out in *Supplementary Document 1: Policy objectives, principles and assessment of measures*, available on DPMC's website. This analysis will be updated based on your feedback to inform final proposals for consideration by Cabinet.

The benefits of enhanced cyber security outweigh the costs of compliance

While there are costs associated with enhancing cyber security, investments in advance of an event are generally acknowledged as being better value for money than enhancing security post-event, when the full costs of disruption are taken into account.

Modelling completed by the Australian Government ahead of introducing similar requirements in Australia indicated that the overall benefit of enhancing the security of critical infrastructure is high, with the benefits of disruptions avoided or mitigated exceeding the costs of implementation.[10]

[9] DPMC. (2024). *Critical infrastructure phase 1 consultation.* https://consultation.dpmc.govt.nz/national-security-group/critical-infrastucture-phase-1-public-consultation/

[10] Department of Home Affairs. (2022). *Regulation impact statement: a risk management program framework for critical infrastructure assets*. https://oia.pmc.gov.au/sites/default/files/posts/2023/02/Impact%20Analysis.pdf

Section 1: Defining critical infrastructure

A principles-based approach to defining critical infrastructure will ensure that we identify the infrastructure services most critical to our economy and communities.

Any new mandatory requirements to enhance cyber security would only apply to **critical infrastructure** – targeting the services that matter most to our economy and communities**.**

To provide clarity on what constitutes critical infrastructure, a new definition is proposed for inclusion in New Zealand law (see Figure 3).

From an initial assessment, the proposed definition could capture approximately 200 of New Zealand's most significant infrastructure entities across seven essential services:[11]

- communications and data
- defence
- energy
- finance
- health
- transport
- drinking water and wastewater.

Some critical infrastructure components are so integral to the functioning of New Zealand to warrant more robust protection against cyber threats. To enable additional obligations to apply to these components, a very small subset of critical infrastructure would be designated as **critical infrastructure of national significance** (CINS).

Designating critical infrastructure

Likely using regulations, thresholds would be set to clarify the type and level of service provision that meets the definition of critical infrastructure. Draft thresholds are set out on the following pages.

Entities that provide essential services at or above the stipulated threshold – with components located within New Zealand – would be required to notify the government of their status. The government would keep a list of critical infrastructure entities informed by these notifications and use this information to help map New Zealand's critical infrastructure system (including dependencies and interdependencies).

Thresholds will not always account for the important dependencies that underpin New Zealand's prosperity or security. Similarly, thresholds could capture components or entities that result in unintended or perverse consequences, undermining the regulation's intent.

The Minister responsible[12] would therefore have powers to:

- designate certain components or entities as critical infrastructure
- exempt entities that meet the definition of critical infrastructure from all or some of the legal obligations of the proposed regime.

Once a decision to designate or exempt an entity has been made, the Minister responsible would be required to table a statement of reasons in Parliament.

.

[11] Definitions of essential services and essential infrastructure are included in the Emergency Management Bill, see: https://legislation.govt.nz/bill/government/2025/0236/latest/LMS1022328.html.

[12] The Minister with responsibility for the proposed regime. This portfolio allocation has not yet been made.

Designating critical infrastructure of national significance

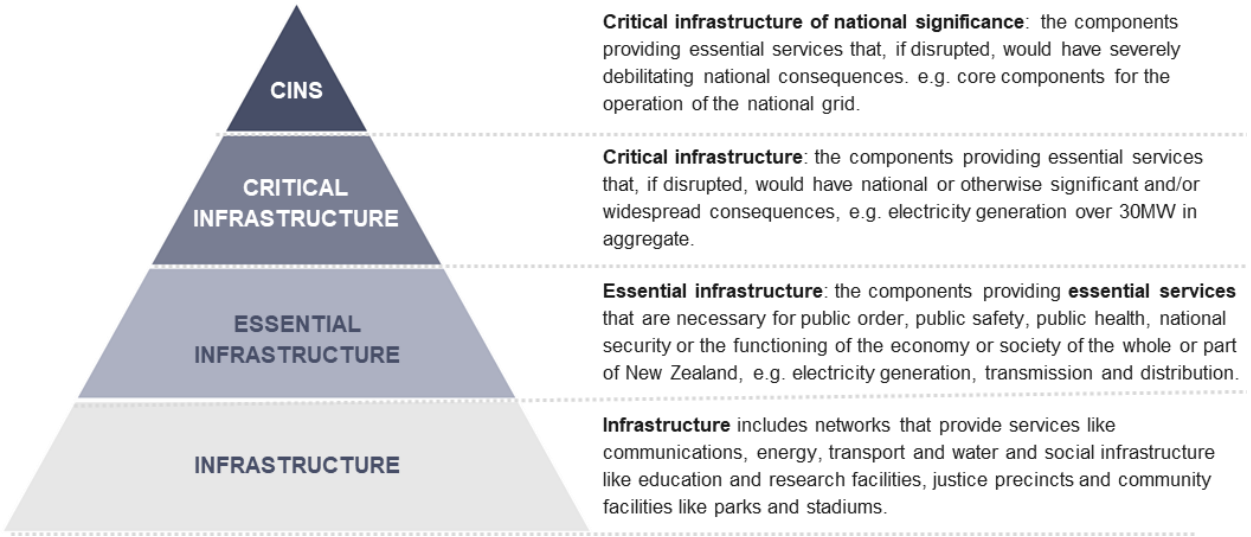
The potential number of components that would be designated as critical infrastructure of national significance is not possible to estimate at this time. This is because designation would be on a case-by-case basis once government has the necessary information to identify and map interdependencies between critical infrastructure entities.

The power to designate components as critical infrastructure of national significance would be vested in the Minister responsible. Factors considered in making a declaration include:

- the extent of cross-sector interdependencies (and therefore potential for any disruption to have cascading consequences across the critical infrastructure system)
- the severity and extent of harm that may be caused to New Zealand's society, security or economy if the service was degraded, disrupted or otherwise compromised
- other matters considered relevant by the Minister.

Before making any designation, the responsible entity would be notified and given the opportunity to provide feedback. Any designation would be privately declared, rather than disclosed publicly, for reasons of security.

FIGURE 3: **PROPOSED APPROACH TO DEFINING NEW ZEALAND'S CRITICAL INFRASTRUCTURE SYSTEM**



Other key definitions include:

- Components: assets, information, networks, systems, suppliers, people and processes.
- Critical components: the components that are necessary[13] to the delivery of the relevant essential service, as determined by a reasonable person in the same set of circumstances.

[13] The scope of this definition is proposed to align with definitions introduced through the Emergency Management Bill, see https://legislation.govt.nz/bill/government/2025/0236/latest/LMS1022328.html.

Proposed critical infrastructure thresholds

Thresholds would give effect to the principles-based definition of critical infrastructure across different types of essential services.

Your feedback will inform refinement of these critical infrastructure thresholds. For further detail on each essential service and the rationale for the proposed thresholds, see *Supplementary Document 2: Defining critical infrastructure*, available on DPMC's website.

Communications and data

Provision of telecommunications services

- Provision of retail telecommunications services by a network operator (as defined in section 3 of the Telecommunications (Interception Capability and Security) Act 2013) to at least 10,000 customers or provision of wholesale network services (also defined in section 3 of the Act) by a network operator maintaining at least 10,000 wholesale connections.
- Connection of domestic and international submarine cables (as defined in section 2 of the Submarine Cables and Pipelines Protection Act 1996) to land-based telecommunications networks.
- Submarine cables in New Zealand waters (as defined in section 2 of the Submarine Cables and Pipelines Protection Act 1996) for the purposes of telecommunications connectivity and the connection of such cables to land-based telecommunications networks.

Operation of domain name system (DNS) service

- Management of New Zealand's country code top-level domain.

Provision of data storage or processing services

- A data centre facility or data services provider that stores or processes data that is integral to the delivery of essential services by a critical infrastructure entity.

Provision of managed services

- Management of IT infrastructure, devices, systems, networks or applications where the IT is integral to the delivery of essential services by a specified number of critical infrastructure entities.

Provision of cloud computing services

- Provision of on-demand computing services that are integral to the delivery of essential services by a specified number of critical infrastructure entities.

Provision of emergency broadcasting services

- Provision of Radio New Zealand and Television New Zealand broadcasting (as defined in section 2 of the Broadcasting Act 1989) in an emergency (as defined in section 4 of the Civil Defence Emergency Management Act 2002).

Provision of positioning, navigation and timing (PNT) services

- Ground-based PNT infrastructure, where PNT services are integral to the delivery of essential services by a critical infrastructure entity.

Defence

Delivery of Defence outputs

- Infrastructure that the New Zealand Defence Force (NZDF) has defined as time-critical to the delivery of Defence outputs (as defined in the most recent NZDF Output Plan).

Energy

Production, processing, transmission, distribution and storage of petroleum products

- Operation of bulk storage facilities (as defined in section 4 of the Fuel Industry Act 2020) with aggregate storage capacity of more than 50 million litres.
- Transmission of petroleum through pipelines (as defined in section 2 of the Health and Safety in Employment (Pipelines) Regulations 1999).

Generation, transmission and distribution of electricity

- Electricity generators (including stations, batteries and other storage) with generation capacity greater than or equal to 30 megawatts and connected to a wholesale electricity market.
- Operation of the national grid (as defined in section 5 of the Electricity Industry Act 2010).

- Coordination of electricity supply and demand by the system operator (as defined in section 5 of the Electricity Industry Act 2010).
- Operation of New Zealand's wholesale trading and information system for spot market electricity.
- Electricity distribution services (as defined in section 54C of the Commerce Act 1986) with greater than 25,000 installation control points (ICPs).

Production, transmission, distribution and storage of gas

- Natural gas producer (as defined in section 2 of the Gas Act 1992).
- Natural gas pipeline services (as defined in section 55A of the Commerce Act 1986) that convey gas at a volume greater than 500,000 gigajoules per annum.

Finance

Taking deposits and processing domestic payments

- Registered banks (as defined in section 2(1) of the Banking (Prudential Supervision) Act 1989) that have been identified as domestic systemically important banks by the Reserve Bank of New Zealand.

Operation of financial market infrastructures

- Domestic financial market infrastructure designated as systemically important under section 20 of the Financial Market Infrastructures Act 2021.

Operation of securities markets

- The NZX, as the primary domestic licensed market operator (as defined under section 6 of the Financial Markets Conduct Act 2013).

Health

Provision of human health services

- Operation of a hospital care institution (as defined in section 58(4) of the Health and Disability Services (Safety) Act 2001) with an intensive care unit.

Transport

Roading

- National and high-volume roads as classified under the One Network Road Classification.
- M1 and M2 roads as classified under the One Network Framework.

Rail

- Management, operation and maintenance of priority and secondary rail freight lines (as defined by KiwiRail) and rail corridors that carry MetroPort services.

Aviation

- Management, operation and maintenance of specific airport companies and airport services (as defined in section 56A of the Commerce Act 1986).
- Air traffic control services (as defined in section 5 of the Civil Aviation Act 2023) at the designated airports.

Maritime

- Management, operation and maintenance of a maritime port (as defined in section 2 of the Port Companies Act 1988) that handles more than 4 million tonnes of combined bulk and container import and export freight per annum, averaged over five years, excluding outlier years linked to global trade shocks.
- Management, operation and maintenance of major inland ports, currently South Auckland Freight Hub and Ruakura Inland Port.
- Management, operation and maintenance of ports that facilitate Cook Strait freight connectivity.
- Operation of interisland freight ferry services.
- Maintenance of New Zealand Distress and Safety Radio Service NAVAREA XIV.
- Maritime navigational aids provided for the operation of any port (as defined in section 200(2) of the Maritime Transport Act 1994) meeting the definition of critical infrastructure.

Drinking water and wastewater

Provision of drinking water services (water treatment plants, reservoirs, distribution systems, pump stations and trunk water mains)

- Networks that supply drinking water to at least 25,000 connections, plus the drinking water schemes operated by Queenstown Lakes District Council (which would be designated by the Minister).

Collection, treatment and disposal of wastewater (wastewater treatment plants, pump stations, trunk sewers, wastewater pipes and pipe bridges)

- Networks that collect and treat wastewater to at least 25,000 connections, plus the reticulated wastewater service operated by Queenstown Lakes District Council (which would be designated by the Minister).

Section 2: Agreeing the depth of the cyber defences of critical infrastructure

Improving information sharing and collection on threats and vulnerabilities

A shared understanding of the interdependencies across the critical infrastructure system and the cyber threats they face is key to reducing cyber risks and minimising the impact of incidents.

A systemic view is necessary to understand the threat environment in which we operate, how disruptions may cascade across the economy and the type of support that critical infrastructure entities need to ensure the ongoing delivery of essential services. This is vital to tackle cyber threats that are constantly evolving, growing in sophistication and increasingly difficult to detect. The more information that is shared, the better prepared New Zealand's critical infrastructure will be to defend against malicious cyber activity.

New Zealand does not have a centralised or consistent approach to sharing or reporting information related to the cyber security of critical infrastructure. While some voluntary information-sharing arrangements are in place, these have trade-offs:

- Most existing forums are sector-specific and therefore do not foster cross-sector dialogue to address common cyber risks.
- Entities have limited incentives to share sensitive information that reveals their vulnerabilities and exposure to cyber threats.
- Entities are concerned about real and perceived barriers to sharing information, including the potential to create legal liabilities (e.g. breaching regulated service quality standards or anti-trust legislation) or harm competitiveness (e.g. information disclosed being used to damage their reputation or gain a competitive advantage).

Only a small proportion of cyber incidents are currently reported, either voluntarily or to meet sector-specific requirements. A number of sectors that provide essential services are not regulated at all, and therefore government has no legislative levers to encourage reporting.

While some information is shared voluntarily with government (e.g. to the NCSC or other regulators), this is typically to seek support in responding to cyber incidents. Some entities may be reluctant to report incidents to government where:

- the information reveals poor security processes or organisational weaknesses
- sharing information could breach legislative or contractual requirements
- there are limited guarantees about how the information will be protected.

There are four measures that could be adopted independently, or as a package, to introduce a new way of working between government and industry to understand and manage the cyber risks to the critical infrastructure system.

Measure 1 addresses the need for a common operating picture of the critical infrastructure system, including who owns and controls critical infrastructure in New Zealand. This type of information would be required at the time an entity meets the definition of critical infrastructure or when there is a material change to an entity's operations and therefore the information previously provided.

Measure 1: Allow government to collect specific information from critical infrastructure entities

Measure 1 would grant the Minister responsible the power to require a critical infrastructure entity to provide certain information to government in a required form at specified intervals. A failure to provide requested information would be an offence.

Initially, the information required could include:

- a description of the critical infrastructure entity's operations, including critical components
- information on the entities and individuals that own and control the critical infrastructure entity
- mapping of key dependencies and interdependencies.

Specific requirements would be set in regulations to allow flexibility in the information that is collected.

Measure 2 would establish a legal framework and forum to facilitate voluntary information sharing, including setting out how any information shared would be protected.

Measure 2: Establish a voluntary information exchange

An information exchange would help connect entities across the critical infrastructure system with each other and with government to coordinate cyber security efforts. This engagement would support a collective response to cyber incidents that have cascading consequences. It would also provide a secure, non-competitive environment for government and industry to work together to tackle cyber threats, mitigate cyber risks and develop solutions to shared cyber security challenges.

The exchange would create a cross-sectoral mechanism for engagement, recognising interdependencies and connections between critical infrastructure entities and sectors.

Measure 3 addresses the need for critical infrastructure entities to share information with each other that may be commercially sensitive but is mutually beneficial to exchange.

Measure 3: Require critical infrastructure entities to share certain information with each other

Measure 3 would allow the Minister responsible to require critical infrastructure entities to share certain information with each other at a prescribed interval. This could include, for example, information on projected restoration times.

In the first instance, this would likely apply only to critical infrastructure of national significance, with a focus on better understanding interdependencies. This would help government identify pressure points across the system and the priority issues that need addressing to mitigate the cascading impacts of cyber incidents.

How would information be protected?

To foster trust and transparency, information shared or collected would be held in strict confidence.

The government would legally only be able to use and share information obtained subject to the following constraints:

- Information could only be used consistent with the purpose of enhancing critical infrastructure security or preserving New Zealand's national security or public order.
- Information could only be disclosed by the critical infrastructure regulator(s) with specified government agencies that have a role in ensuring the security and ongoing operation of the critical infrastructure system.
- Information could only be disclosed to other organisations if there are reasonable grounds to believe its disclosure is necessary to preserve national security or public order.

Any breach of these protections by a government agency would be an offence.

Measure 4 would require critical infrastructure entities to report cyber incidents with the goal of building a more accurate picture of the threat environment and scale of cyber harm experienced by New Zealand's critical infrastructure system.

Measure 4: Require critical infrastructure entities to report cyber incidents

Measure 4 would establish reporting requirements for cyber incidents by critical infrastructure entities to the NCSC and the critical infrastructure regulator(s)[14], including:

- regularly reporting all cyber incidents (with the frequency of reporting to be set in regulations).
- reporting significant cyber incidents as soon as practicable. This would include an initial early warning not later than 24 hours after the incident was detected, and the full report not later than 72 hours after the incident was detected.

Rapid reporting of significant incidents would also allow the NCSC to help entities respond to high-impact cyber incidents so they can recover as soon as possible with minimal disruption to the delivery of essential services.

How could a significant cyber incident or a cyber incident be defined?

A significant cyber incident would be defined as an event involving an information system that has had or, is likely to have, serious impact[15] on:

- the confidentiality, integrity or availability of information, or
- the delivery of essential services.

A cyber incident would be defined in the same way, without reference to the incident's materiality.

How could reporting on cyber incidents be used?

Incident reports would be subject to the same protections proposed for other types of information sharing and collection set out on page 13.

The government's priority upon receiving an incident report is swift remediation and recovery, rather than immediate compliance action. Onward sharing of information reported to the NCSC in the context of incident response and remediation would be limited, so it would not be used for regulatory purposes.

This would reduce the risk that entities do not report incidents, delay reporting, or limit the detail they provide out of concern that the information will be used for regulatory action.

This limited use obligation would not provide a safe harbour from legal liability or prevent a regulator from acquiring the same information directly from the entity.

Australia has also legislated a limited use obligation but only with respect to voluntary reporting of incidents to the Australian Signals Directorate (Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024) or its National Cyber Security Coordinator (Cyber Security Act 2024).

[14] Decisions at to the entity(s) who would have responsibilities as the critical infrastructure regulator(s) have not been taken.

[15] This threshold is based on the categorisation of cyber security incidents in the New Zealand Information Security Manual section 7.2.14. It will likely be for entities to determine what constitutes serious impact through the application of a reasonable person test. https://nzism.gcsb.govt.nz/ism-document#Section-13120

Introducing minimum cyber risk management requirements across the critical infrastructure system

Good risk management is key to enhancing the cyber security of our critical infrastructure system. It is important that minimum requirements for cyber risk management are set consistently for all critical infrastructure entities to ensure they work towards a common level of security. The New Zealand Government must play a role in setting and enforcing these.

Minimum requirements are designed to empower critical infrastructure entities to identify the most cost-effective measures to manage their cyber risks. This recognises that critical infrastructure entities know their businesses, supply chains and value chains best. It also allows entities to leverage any existing measures they undertake to prevent or protect themselves from cyber risks.

The requirement to align with a cyber security framework recognises that capability is limited in some entities and sectors, and it may be more effective to implement a structured set of standards, practices and security controls. It would further ensure consistency in approaches to cyber security across the critical infrastructure system.

While it is not proposed that an exhaustive list of accepted frameworks would be provided by government, entities would be required to justify their chosen cyber security framework as well as confirm compliance.

Requiring other entities that have operational control over critical components, such as suppliers or contractors, to support critical infrastructure entities to meet their risk management obligations is intended to help ensure consistent alignment with cyber security frameworks throughout the supply chain and manage any risks that have the potential to disrupt critical infrastructure.

Measure 5: Require critical infrastructure entities to develop, implement and maintain a risk management programme aligned with an internationally recognised cyber security framework

Measure 5 would require critical infrastructure entities to develop, maintain and implement a risk management programme that:

- identifies components that are critical to the delivery of essential services
- identifies cyber risks that are material to those critical components as determined by a reasonable person in the same set of circumstances
- treats cyber risks that are material to the critical components as far as reasonably practicable
- complies with a cyber security framework that is endorsed by the NCSC or recognised internationally, such as the US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) or ISO/IEC 27001:2022.

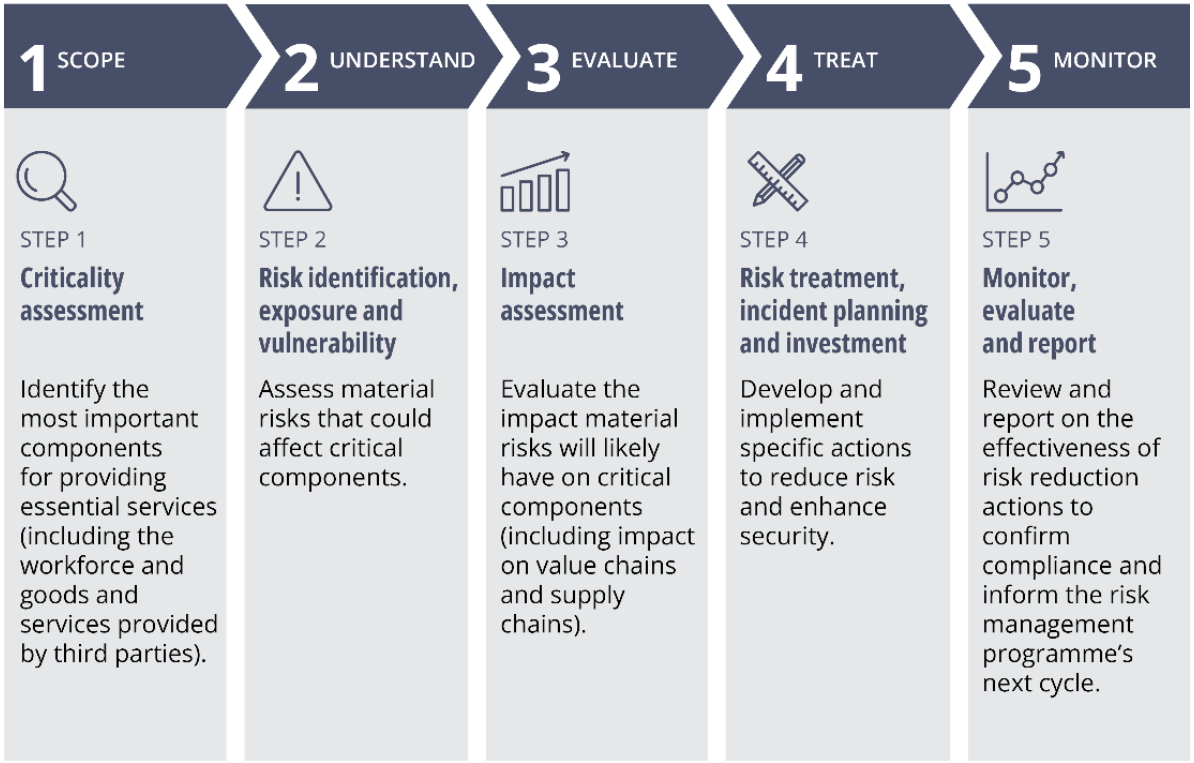
Figure 4 on page 16 summarises the key steps entities would be expected to complete in developing and implementing the risk management programme.

To support critical infrastructure entities fulfil their risk management programme obligations, other entities that have operational control over critical components would be required to support critical infrastructure entities as far as practicable.

In addition, the Minister responsible would be able to:

- specify any additional measures that entities may need to undertake as part of the risk management programme
- require entities (or a subset of entities such as critical infrastructure of national significance) to take prescribed actions to manage a specific risk or set of risks.

FIGURE 4: **KEY STEPS REQUIRED WHEN DEVELOPING CYBER RISK MANAGEMENT PROGRAMME**



Reporting compliance with minimum requirements

Directors of critical infrastructure entities (or equivalent) would be responsible for ensuring compliance with minimum requirements. Including cyber security as a core element of fiduciary duty for directors across New Zealand's critical infrastructure system would help elevate board attention and investment in managing cyber risks.

Regulations would be used to confirm reporting requirements, and these would likely strengthen over time. Initially, responsible entities could be required to attest to their compliance with minimum requirements (i.e. sign a formal declaration that the requirements have been met).

After a period of the regime being in force, responsible entities would likely be required to complete a short report documenting how requirements have been met. This would provide the government with more information to assess whether requirements are having the intended impact, including whether any related guidance needs to be adjusted or attention given to managing certain risks.

While the government could require responsible entities to obtain a third-party audit to demonstrate compliance, this is unlikely in the medium term due to the significant cost for critical infrastructure entities and the market's limited capacity and capability to support this type of audit.

Accounting for compliance with other regulatory regimes

Many critical infrastructure entities already manage cyber risks, whether to address the recommendations of the NCSC, to meet sector-based guidelines or requirements, to satisfy prudent governance, or for commercial reasons.

The existence of good practice, including compliance with any current or future regulations, would not exempt a critical infrastructure entity from the obligation to comply with, and report on, minimum requirements. It could, however, affect what additional activities an entity would need to take in order to comply.

In this way, minimum requirements are designed to fill gaps rather than duplicate, and allow for sector-based requirements to evolve as the stewards of those systems see fit over time.

If a set of responsible entities were managing cyber security to the level required as part of complying with sector-based regulations, the critical infrastructure regulator(s) would be empowered to issue a determination noting that all relevant entities are managing cyber risk to the level required. However, this is expected to be rare, at least initially.

Wherever an entity is meeting the requirements through adherence to sector-based regulations, the relevant sector regulator would remain responsible for monitoring compliance. If requirements were not met, this would breach the requirements of both regimes. Details on how this would be managed in a way that avoids double jeopardy is provided on page 19.

For entities subject to price-quality regulation by the Commerce Commission, any investments required to comply with minimum requirements could be able to be offset with additional revenue.

Enhanced minimum requirements for critical infrastructure of national significance

Two elements of minimum requirements that could be enhanced for critical infrastructure of national significance are:

- the risks to be treated and the level of treatment
- the type of reporting required to demonstrate compliance.

Minimum requirements would include the power to require critical infrastructure of national significance to take a specific action to manage a risk or set of risks to a particular level. This could include following an additional process such as complying with a particular cyber security framework or more prescriptive actions.

Reporting requirements could be enhanced for critical infrastructure of national significance more quickly than for other responsible entities (e.g. moving from attestation to a short report more quickly than other critical infrastructure entities).

Both of these approaches to calibrating minimum cyber security requirements for critical infrastructure of national significance reflects the importance of these assets to New Zealand and would only be used where the risks faced outweigh the additional costs of compliance.

Ensuring effective management of cyber threats impacting national security

Critical infrastructure entities could be better supported to remediate, recover and learn from cyber incidents and cybercrime.

It is not realistic or proportionate to expect critical infrastructure entities to manage all cyber threats on their own, particularly if they are of such severity as to pose a significant threat to national security. New government powers would help ensure rapid and decisive action to protect critical infrastructure. This recognises that:

- the government's access to classified information and specialist capabilities put it in a unique position to understand national security threats and support entities to manage them
- state-sponsored threat actors have much greater ability and incentive to invest in exploiting one vulnerability than any potential target could invest to reduce all of its vulnerabilities
- even where an entity could manage a cyber threat, there may be statutory or contractual requirements that serve as a barrier to them doing so (e.g. contracts with a third-party provider).

The executive power proposed would improve the government's ability to help critical infrastructure entities respond effectively to significant cyber threats or incidents. Compliance with the power would be mandatory.

The power would only be exercised as a last resort for national security reasons. There would be no ability for entities to seek damages or financial compensation for any reasonable costs incurred as part of compliance.

Measure 6: A power to direct the management of cyber threats for national security reasons

Measure 6 would grant the Minister responsible the power to direct a critical infrastructure entity to do, or refrain from doing, anything necessary to manage a cyber threat for national security reasons. A direction would specify the period within which this must occur.

Direction under the power could include, for example, requiring critical infrastructure entities to accept support from the NCSC to help resolve cyber incidents that are a threat to national security.

Entities subject to the power would have the following legal and natural justice protections available of:

- the ability to appeal to the Minister
- a right to statutory review
- indemnity against legal liability
- limits on the acquisition of property.

Protections around the use of government powers

Reflecting the significance of the proposed power, the Minister responsible could only use it to support the management of threats to critical infrastructure entities (rather than threats to all essential services). The Minister responsible would also need to be satisfied that:

- the national security threat is significant
- adequate and good-faith consultation with the relevant entity or entities has occurred
- the proposed action to manage the threat is proportionate, reasonably necessary and has a reasonable likelihood of success
- there is no alternative to the proposed action that would satisfactorily address the national security threat.

Once the incident has been resolved, a summary of the measures taken and rationale for invoking the power would be published unless there were reasonable grounds to withhold this information under the Official Information Act 1982.

Section 3: Ensuring mandatory requirements improve the cyber security of the critical infrastructure system

Compliance is key to delivering an uplift in the cyber security of New Zealand's critical infrastructure system. The proposed approach combines efforts to promote voluntary compliance with a range of tools for addressing non-compliance.

The proposed approach to compliance would aim to provide the critical infrastructure regulator(s) with mechanisms for:

- **monitoring and supervision** such as regular reporting, inspections and performance assessments
- **compliance and enforcement**, which would range from awareness-raising and education in the first instance to fines, enforceable undertakings and civil and criminal penalties for non-conformance.

These mechanisms would be:

- fair, consistent and proportionate to the severity of the breach and degree of harm caused
- efficient and as simple as possible to administer
- easy to understand.

Ensuring a proportionate approach to compliance

The critical infrastructure regulator(s) would have access to a comprehensive suite of compliance and enforcement tools, including:

- compliance notices directing a breach be fixed within a specified time period
- legally binding agreements (enforceable undertakings) between the regulator and a non-compliant party that the regulator would not prosecute or apply a penalty if the non-compliant party agrees to certain actions
- non-criminal monetary penalties imposed by the courts
- criminal prosecution.

Table 1 on page 20 provides examples of how potential breaches could be matched with compliance tools. In some instances, tools could be combined where necessary to ensure compliance. Use of deterrent and punishment measures would be carefully calibrated to the nature of the breach – with more severe breaches matched with stronger compliance tools.

Entities and individuals would not be held responsible for offences where the contravention:

- was necessary to save or protect life or health or prevent serious damage to property
- was beyond the person's or entity's control, could not reasonably have been foreseen, and steps could not reasonably have been taken to prevent it from occurring
- was due to reasonable reliance on information supplied by another person, or
- was not known about by the person and they could not reasonably have known.

The responsible party would not be punished twice for breaching more than one regulatory regime. Where a breach is punishable under multiple regulatory regimes, the more stringent of the two penalties would apply, unless otherwise mutually agreed by both regulators.

A staged approach to compliance

During the first few years of the regime's operation, regulatory requirements would likely come into force in a phased manner, recognising the lift in skills and capability that would be required across the critical infrastructure system to achieve compliance.

The approach to compliance would be staged – with a one-year grace period between requirements coming into effect and any enforcement action being considered. During this period, there would be a focus on providing regulated entities with information, guidance materials and other support to make complying with legislated requirements as simple and clear as possible.

TABLE 1: **EXAMPLES OF BREACHES AND COMPLIANCE TOOLS**

CATEGORY OF BREACH	EXAMPLE OF BREACH	EXAMPLE COMPLIANCE TOOLS
Minor breach	• Late or incomplete provision of information in accordance with an information-collection power or reporting on minimum cyber security requirements (strict liability, entity only). • Late or incomplete sharing of required information with other critical infrastructure entities (strict liability, entity only).	• Targeted education. • Written warning. • Increased monitoring assessments. • Administrative fine of up to $50,000.
Minor to moderate breach	• Failure to provide information in accordance with an information-collection power (strict liability, entity only). • Failure to share required information with other critical infrastructure entities (strict liability, entity only).	• Compliance notice or enforceable undertaking. • Increased monitoring assessment. • Information request or inspection. • Civil pecuniary penalty of up to $100,000.
Moderate breach	• Failure to report on minimum cyber security requirements. • Using or disclosing protected information without authorisation. • Failure to comply with a compliance notice or enforceable undertaking.	• Compliance notice or enforceable undertaking. • Civil pecuniary penalty of up to $200,000. Aggravating factors of negligently, recklessly or knowingly breaching requirements would be considered in determining penalty quantum.
Serious breach	• Negligently, recklessly or knowingly failing to review progress against minimum cyber security requirements within specified timeframes or failing to comply with specified rules when adopting or reviewing requirements (criminal offence, entity or directors). • Knowingly or intentionally abusing protected commercial information such as for sabotage or financial gain (criminal offence, entity or directors). • Negligently, recklessly or knowingly (for an entity) or negligently or recklessly (for a director) failing to comply with an information request related to compliance or the prospective use of a power (criminal offence, entity only). • Negligently, recklessly or knowingly submitting false or misleading information (criminal offence, entity or directors).	• Compliance notice or enforceable undertaking. • Criminal penalty of up to $2 million or up to 1 percent of annual turnover, whichever is greater (for an entity). • Criminal penalty up to $100,000 (for a director).
Critical breach	• Negligently, recklessly or knowingly failing to meet minimum cyber security requirements. • Negligently, recklessly or knowingly failing to comply with instructions made under a national security power direction. • Negligently, recklessly or knowingly obstructing an investigation or inspection.	• Compliance notice or enforceable undertaking. • Criminal penalty of up to $5 million or up to 2 percent of annual turnover, whichever is greater (for an entity). • Criminal penalty up to $500,000 (for a director).

How to have your say

We want to hear views from individuals and organisations on the ideas and measures set out in this document.

Consultation is open from 27 February to 19 April 2026.

This discussion document is primarily aimed at the owners and operators of critical infrastructure who would be directly affected by potential regulatory reform. We also welcome input from individuals, businesses and communities who are directly affected by the security of our critical infrastructure.

Ways to provide feedback:

- Attend an online or in-person meeting (details available on DPMC's website)
- Complete a written submission online on DPMC's website, email it to criticalinfrastructure@dpmc.govt.nz or post it to:
  National Security and Resilience Group
  Department of the Prime Minister and Cabinet
  Level 8, Executive Wing, Parliament Buildings
  Wellington 6011

To guide your feedback, a list of questions to consider is provided on pages 22-24. However, you should not feel restricted to answering these questions or using this format.

You can find more information about this work programme, consultation meetings and making a submission on DPMC's website at https://www.dpmc.govt.nz/our-programmes/national-security/critical-infrastructure, including:

- Supplementary Document 1: Policy objectives, principles and assessment of measures
- Supplementary Document 2: Defining critical infrastructure
- Summary of Phase 1 Consultation.

Consultation questions

The Government is seeking your views on the following questions across all proposed measures:

- Do you have any comment on the potential implications of each of the measures?
- Are you able to quantify the potential cost of compliance with each of the measures?
- Do you think the right measures have been identified?
  - If yes, which of the measures do you prefer and why?
  - If no, what alternative measure(s) would you support and why?

SAMPLE TEMPLATE

When providing information on costs across each measure – particularly minimum cyber risk management requirements – it would be helpful if this could be provided in the following template. This is to ensure information can be collected consistently to support the cost-benefit analysis that will inform final recommendations to Cabinet.

QUESTION	RESPONSE
Is your entity, based on the draft thresholds set out on pages 10 and 11, likely to be a critical infrastructure entity?	
What one-off capital costs do you expect to incur to comply with each measure, if any (e.g. the cost of developing new reporting systems)? Please provide a range between expected costs and highest possible costs.	
What ongoing capital costs do you expect to incur to comply with each measure, if any (e.g. the cost of additional investments in resilience to meet the requirements of the risk management programme)? Please provide a range between expected costs and highest possible costs.	
What ongoing operational costs do you expect to incur to comply with each measure, if any (e.g. the cost of undertaking a risk assessment, as required by the risk management programme)? Please provide a range between expected costs and highest possible costs.	
What assumptions have underpinned these cost estimates?	

In addition to the general questions above, the Government is seeking views on the following questions related to specific sections of the discussion document.

Defining critical infrastructure

- Would you support the proposed approach to defining critical infrastructure and critical infrastructure of national significance, and if not, what changes would you recommend?
- Do you consider any essential services have been included or excluded that should not be? If so, what services are they and why should they be added or removed?
- Do you think the example thresholds for defining critical infrastructure have been set appropriately and provide sufficient clarity as to what level of service provision constitutes critical infrastructure? If not, what alternative thresholds would you support, and why?
- In addition to interdependencies and consequences of a disruption, are there other factors you think should be considered in assessing whether an asset should be declared critical infrastructure of national significance?
- Do you agree that the Minister responsible should have the ability to designate or exempt critical infrastructure entities? In not, what alternative approach would you support, and why?

Improving information sharing and collection on threats and vulnerabilities

- Do you agree with the proposed approach to protecting the data shared? If not, what alternative provisions would you suggest and why?
- If you are likely to be deemed a critical infrastructure owner or operator, what effect would having all essential infrastructure providers participating in the formal information exchange, rather than just other critical infrastructure entities, have on your willingness to participate?
- If the government required regular reporting of all cyber incidents, how frequently do you think this information should be required (e.g. every quarter, every six months)?
- Do you consider the proposed definition of a cyber incident can be given effect within your existing approach to enterprise risk management? If not, what alternative definition would you recommend?
- Would a requirement to report significant cyber incidents make you less willing to report other cyber incidents voluntarily?
- Do you consider using the criteria of serious and above for cyber incidents that should be reported within 72 hours are appropriate. If not, what criteria for reporting would you recommend?
- What impact do you think the requirement to report significant cyber incidents could have on your incident response process? For example, would you need to involve lawyers to determine what incidents to report and when?

Introducing minimum cyber risk management requirements across the critical infrastructure system

- Are any of the specific words proposed to set the requirements of the risk management programme on page 15 likely to conflict with your existing approach to risk management in a way that requires you to make significant changes to these processes, rather than build on what already exists?
- Do you agree that critical components should be defined in a way that aligns with the scope of the requirements in the emergency management system? If not, what alternative scope would you recommend, and why?
- Do you consider that the concept of a risk that is material can be given effect to within your existing approach to enterprise risk management? If not, what alternative approach to defining the level of risk that must be treated would you recommend, and why?
- Do you consider that the threshold for treating risks should be set at so far as reasonably practicable? If not, what alternative language to set the scope of risks to be treated would you recommend, and why?
- Do you support the risk management programme complying with a cyber security framework that is endorsed by the NCSC or recognised internationally?

- Do you agree that government should not prescribe the international internationally recognised cyber security frameworks that are acceptable if compliance with an international cyber security framework were required? If not, what framework(s) would you suggest should be included on such a list, and why?
- Do you consider that a requirement for third-party vendors that have operational control over critical components, to support responsible entities to comply to the extent reasonably practicable, is important to the effective implementation of the risk management programme? Do see any unintended consequences? If so, what do you consider those to be?
- Do you consider that there are alternative ways for the government to recognise that compliance with other regulation is equivalent to the minimum requirements for cyber risk management? If so, what do you propose?
- Do you consider there is a more effective way to ensure compliance than to attach responsibility for minimum requirements for cyber risk management to individual directors? If so, what would you propose?
- Do you have a preference on how responsible entities should demonstrate compliance with minimum requirements for cyber risk management?

Ensuring effective management of cyber threats impacting national security

- When responding to a cyber incident for national security reasons, what support from government is most helpful to aid the restoration of essential services?
- Do you think the thresholds for the use of the last-resort power are appropriate? If not, what changes would you propose?
- Do you think that the protections and rights for entities subject to the last-resort power are appropriate? If not, what changes would you propose?

Ensuring mandatory requirements improve the cyber security of the critical infrastructure system

- Do you consider that the breaches are appropriately mapped to compliance and enforcement tools? If not, what changes would you propose?
- Do you support the proposed approach to compliance and enforcement where an entity breaches requirements across two or more regulatory regimes? If not, what alternative would you propose?
- Do you agree that penalties in respect of compliance with minimum cyber security requirements should apply to the entity's directors as well as to the organisation as a whole? Why or why not?
- Do you perceive any perverse outcomes as a result of directors being individually liable for the most serious breaches of the regime?

ISBN 978-1-0670255-6-4 DIGITAL