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 | Supplementary document 1 | Policy objectives, principles and assessment of measures

Objectives for enhancing critical infrastructure cyber security

New Zealand businesses and communities must be able to rely on the continued delivery of critical infrastructure services that are resilient to malicious attacks, accidental disruptions and negligent practices.

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

- **protect the lives and livelihoods of New Zealanders** from the real-world impacts of cyber incidents by reducing the risk of outages that can undermine health, prosperity and living standards
- **support economic growth** by maintaining digitally resilient critical infrastructure services to power our economy and mitigate the costs of future incidents, enhancing New Zealand's attractiveness for foreign investment and business formation
- **preserve New Zealand's sovereignty** by reducing the opportunity and likelihood of foreign states gaining leverage over the New Zealand Government, which could constrain its ability to act solely in the interests of New Zealand citizens
- **keep pace with international approaches** to protect against the disruptive impact of new technologies, including a rising threat level and expanded attack surface, which makes critical systems more vulnerable to attack.

Principles underpinning the design of measures

The measures in the discussion document have been selected for their consistency with the principles listed below:

- Any reform would apply to all critical infrastructure equally, irrespective of ownership.
- Any reform would be consistent with the principles of te Tiriti o Waitangi | Treaty of Waitangi, other domestic policy obligations and our international obligations.
- Critical infrastructure entities are best placed to understand and manage the risks facing their organisations, but government has a responsibility to partner with industry to:
  - ensure owners and operators have a good understanding of the cyber risks they face
  - support owners and operators in prioritising targeted investments to enhance their cyber security
  - set minimum requirements in areas where market forces do not deliver a sufficient level of cyber security.
- Cyber security should be enhanced at least cost to businesses, consumers and government, without unduly undermining market competition, by:
  - using non-regulatory mechanisms (such as information sharing), where possible, to better prioritise investments in cyber security and deliver optimal improvements for each dollar spent
  - taking advantage of existing regulatory regimes, where possible, by filling gaps in the existing regulatory landscape rather than replacing or duplicating them
  - developing proposals that build on and complement forthcoming laws, where possible
  - ensuring any new approach is proportionate and dynamic so that legislation does not become rapidly outdated or otherwise no longer fit for purpose.
- The costs of enhancing cyber security should, where possible, be paid for by those benefiting from the investments (the benefit principle) or creating the need for them (the causer principle).

Assessment of measures

Three criteria are used to determine the extent to which specific measures deliver on the objectives of reform and how well they embody the design principles.

DPMC has not attached any weighting to these criteria. Ministers' weighting of these criteria will inform their final decisions. Discounted approaches that scored poorly against these criteria or did not align with feedback received through engagement with industry during 2023 and 2024 have not been taken forward.

Criterion A: How well does the measure better ensure the provision of essential services? This question considers how effectively a measure ensures the continued provision of essential services despite the existence of potentially disruptive threats. It considers the extent to which the measure:

- reduces or supports a reduction in the likelihood and impact of cyber security risks
- encourages, facilitates or requires proportionate investments to enhance cyber security across all critical infrastructure sectors.

Criterion B: How does the measure change the regulatory burden and regulatory certainty for critical infrastructure entities? This question includes consideration of anticipated costs to entities through:

- the cost of compliance
- the degree of certainty that a measure would provide for regulated entities as to their obligations and how to meet them, recognising that navigating uncertainty increases compliance costs for critical infrastructure entities
- any change in the number of regulatory relationships or 'touch points' that a measure would create for critical infrastructure entities, recognising that this would directly increase compliance costs and the regulatory system's complexity.

Criterion C: What costs does the measure impose on central government for implementation and ongoing administration? This question considers increased costs to government through:

- any additional expenses the government may incur to administer a measure on an ongoing basis, including expenses associated with a need for additional coordination between government regulators
- any costs associated with a measure's implementation.

The discussion document sets out the measures that have been identified that meet the objectives and principles and could work together to enhance the cyber security of New Zealand's critical infrastructure system.

Measures have been scored against the criteria above, and a summary of this analysis is presented in the following tables to display the relative costs and benefits.

Based on feedback, these scores will be updated and compared against each other to inform a net benefit assessment and final recommendations to Cabinet on preferred measures.

Table 1: Assessment of the costs and benefits of defining critical infrastructure

	Principles-based definition in legislation and thresholds to give effect to the definition in regulations
Criterion A: Ensures the continued provision of essential services	**Strongly positive** Updates New Zealand's approach to defining critical infrastructure. The definition would remain current and comprehensive because thresholds can be more easily amended.
Criterion B: Changes to regulatory burden and certainty for critical infrastructure entities	**Slightly negative** The split between legislative instruments would reduce certainty and require entities to periodically review the regulations. This cost would be partially offset by the ability to adjust thresholds, which reduces the risk of capturing entities that do not provide nationally significant services.
Criterion C: Cost to government	**Slightly negative** Essential services and thresholds would need to be periodically reviewed.

Table 2: Assessment of the costs and benefits of measures to enhance the cyber security of critical infrastructure

	Measure 1: Allow government to collect specific information from critical infrastructure entities	Measure 2: Establish a voluntary information exchange	Measure 3: Require critical infrastructure entities to share certain information with each other	Measure 4: Require critical infrastructure entities to report cyber incidents	Measure 5: Develop, implement and maintain a risk management programme aligned with an internationally recognised cyber security framework	Measure 6: A power to direct the management of cyber threats for national security reasons
Criterion A: Ensures the continued provision of essential services	**Moderately positive** Provides government with vital information to understand threats and vulnerabilities in critical infrastructure, revealing dependencies and interdependencies.	**Slightly positive** Increases confidence to share and ability to manage risks but less useful if essential services providers do not participate or share sensitive information.	**Slightly positive** Greater sharing of information on matters such as levels of service, shared risks and interdependencies would help manage cascading failures to restore essential services and inform investment planning.	**Moderately positive** Grants the NCSC visibility of significant threats that could impact other entities in close to real time, informing guidance and other interventions. Regular reporting would also provide trends of threats. There is a degree of uncertainty around effectiveness as it is unclear how many cyber incidents are not being reported.	**Strongly positive** Sets clear objective legal tests around what risks to address in the most material parts of an entity's operations as well as the level of treatment required. The risk management programme would drive strategic, entity-led, investment in cyber security.	**Moderately positive** Enhances government's ability to support entities to manage cyber threats to national security and reduce impact from disruptions. Legal indemnity protections would increase the likelihood of entities taking necessary actions.

	Measure 1: Allow government to collect specific information from critical infrastructure entities	Measure 2: Establish a voluntary information exchange	Measure 3: Require critical infrastructure entities to share certain information with each other	Measure 4: Require critical infrastructure entities to report cyber incidents	Measure 5: Develop, implement and maintain a risk management programme aligned with an internationally recognised cyber security framework	Measure 6: A power to direct the management of cyber threats for national security reasons
Criterion B: Changes to regulatory burden and certainty for critical infrastructure entities	**Slightly negative** Reporting across the system adds regulatory burden and cost, but costs would be minimised by requiring information only when it can't be accessed in another way.	**Neutral** Voluntary involvement means there is no prescribed additional cost burden on entities. However, participation (through attendance and information contribution) in any network will require time and resource.	**Slightly negative** Adds burden to generate, assure and share information, but this is limited by constraints on required information.	**Moderately negative** Reporting soon after an event is detected would place burden on already stressed entities. This would be managed by minimising the amount of information required. Similarly, regular reporting of all incidents would place a burden on entities that would be managed by ensuring only necessary information was required.	**Strongly negative** Annual risk management processes and reporting would have material ongoing costs, in addition to the investments required to implement measures to enhance cyber security. There would also be one-off costs associated with developing systems and capabilities initially. These are unlikely to be significant given compatibility with leading practice.	**Slightly negative** Could create greater compliance costs for entities depending on the specific direction and actions needed. A legally binding direction would provide entities with greater certainty on necessary actions compared to voluntary advice. Legal indemnity would remove disincentive to act due to conflicting legislative or regulatory obligations.

	Measure 1: Allow government to collect specific information from critical infrastructure entities	Measure 2: Establish a voluntary information exchange	Measure 3: Require critical infrastructure entities to share certain information with each other	Measure 4: Require critical infrastructure entities to report cyber incidents	Measure 5: Develop, implement and maintain a risk management programme aligned with an internationally recognised cyber security framework	Measure 6: A power to direct the management of cyber threats for national security reasons
Criterion C: Cost to government	**Slightly negative** Government would need to establish processes to ensure that legal protections are met. Collection of information may also require additional resources to process and analyse in order for the data to have the desired impact.	**Slightly negative** Government would incur expenses setting up and providing the platform, hosting meetings and sharing information. There would be one-off costs to establish processes to ensure protections are met.	**Slightly negative** Government would incur some expense in establishing regulations and monitoring compliance, but ongoing costs would be minimal.	**Moderately negative** Could increase demand for NCSC resources, depending on how often significant cyber events occur and the level of support required. Would require additional resourcing to ensure that the information provided through regular reporting was analysed in a way to generate meaningful insights.	**Moderately negative** Government would need to build additional capacity and capability to provide guidance on the risk management programme and assess compliance on an ongoing basis.	**Slightly negative** Would impose some additional burden associated with consultation and other requirements before the power can be exercised, but those costs would be offset by the fact that the power is expected to be used very rarely.