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

Proactive Release

The following document has been proactively released by the Department of the Prime Minister and Cabinet on behalf of Rt Hon Christopher Luxon, Minister for National Security and Intelligence:

New Zealand Cyber Security Strategy 2026-2030 and Enhancing the Cyber Security of Critical Infrastructure

The following documents have been included in this release:

Title of minute: Report of the Cabinet Foreign Policy and National Security Committee: Period Ended 20 February 2026 (CAB-26-MIN-0047 refers)

Title of minute: New Zealand Cyber Security Strategy 2026-2030 and Enhancing the Cyber Security of Critical Infrastructure (FPS-26-MIN-0004 refers)

Title of paper: New Zealand Cyber Security Strategy 2026-2030 and Enhancing the Cyber Security of Critical Infrastructure (FPS-26-SUB-0004 refers)

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

Key to redaction codes:

- Section 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand
- Section 9(2)(f)(iv), to maintain the confidentiality of advice tendered by or to Ministers and officials

Some annexes enclosed in the released paper were considered in draft form and have been superseded by final versions. These drafts are omitted from this proactive release. The final versions of these annexes can be found at the links below:

- Annex A: New Zealand's Cyber Security Strategy 2026 – 2030
- Annex B: New Zealand's Cyber Security Action Plan 2026 – 2027
- Annex E: Discussion document: Enhancing the cyber security of New Zealand's critical infrastructure system

Cabinet

Minute of Decision

Report of the Cabinet Foreign Policy and National Security Committee: Period Ended 20 February 2026

On 23 February 2026, Cabinet made the following decisions on the work of the Cabinet Foreign Policy and National Security Committee for the period ended 20 February 2026:

FPS-26-MIN-0004	**New Zealand Cyber Security Strategy 2026-2030 and Enhancing the Cyber Security of Critical Infrastructure** Portfolio: National Security and Intelligence	CONFIRMED

[Not in Scope]

Rachel Hayward
Secretary of the Cabinet

Cabinet Foreign Policy and National Security Committee

Minute of Decision

New Zealand Cyber Security Strategy 2026-2030 and Enhancing the Cyber Security of Critical Infrastructure

Portfolio **National Security and Intelligence**

On 18 February 2026, the Cabinet Foreign Policy and National Security Committee:

1 **noted** that threat assessments from domestic agencies, clos partners, and industry point to a worsening cyber threat environment that is negatively affecting New Zealand through the impact of espionage, cybercrime, and disruption to ritical infrastructure;

2 **agreed** to the content and public release of the New Zealand Cyber Security Strategy 2026-2030 (the Strategy), and supporting Action Plan for 2026-2027 (the Action Plan), attached to the submission under FPS-26-SUB-0004;

3 **noted** that two actions in the Action Plan 2026-2027 directly address the need to strengthen the protection of personal data, as evidenced by the Manage My Health cyber incident;

4 **noted** the indicative direction f future actions, as set out in the attached Annex C, and the need to regularly r fresh the Action Plan to keep pace with the threat;

5 **noted** that enhancing th cyber security of New Zealand's critical infrastructure is a key initiative of the Strategy and Action Plan;

6 **agreed** to the p blic release of the discussion document, *Enhancing the cyber security of New Zealand's critical infrastructure system* (the discussion document), attached as Annex E, which outlines a package of proposed measures to drive a consistent and effective appro ch to managing cyber risks across the critical infrastructure system;

7 **authorised** the Minister for National Security and Intelligence to approve any necessary editorial, minor, or technical amendments to the wording of the Strategy, the Action Plan, and the discussion document before publication.

Jenny Vickers
Committee Secretary

Attendance: (see over)

Present:
Rt Hon Christopher Luxon
Rt Hon Winston Peters
Hon David Seymour
Hon Nicola Willis
Hon Judith Collins KC

Officials present from:
Officials Committee for FPS
Office of the Prime Minister
Office of the Chair of FPS
Office of the Minister of Defence

Office of the Minister for National Security and Intelligence

Cabinet Foreign Policy and National Security Committee

New Zealand Cyber Security Strategy 2026-2030 and Enhancing the Cyber Security of Critical Infrastructure

Proposal

1. This paper seeks Cabinet agreement to:

   a. Approve New Zealand's Cyber Security Strategy 2026-2030 and its supporting Action Plan 2026-2027.

   b. Release a discussion document on enhancing the cyber security of New Zealand's critical infrastructure, which is a key action under the Strategy and Acti n Plan.

Relation to government priorities

2. Lifting New Zealand's approach to cyber security supports the Government's objective of rebuilding and growing the economy. The safe and s cure operation of New Zealand's critical infrastructure underpins our economic growth, stability and prosperity.

Executive Summary

3. New Zealand's economic growth relies n our ability to promote and defend a free, open and secure cyberspace. However, New Zealand is exposed to persistent, pervasive and escalating cyber threats. To prosper s a nation and protect our national security, we must increase our efforts to counter these th eats. This paper seeks Cabinet agreement to:

   a. approve New Zealand s Cyber Security Strategy 2026-2030 and supporting Action Plan for 2026-2027; and

   b. release a discussion d cument on measures to enhance the cyber security of New Zealand's cri ical infrastructure system, which is a key initiative in the Strategy and Action Plan.

4. The urrent Cyber Security Strategy dates back to 2019. We are in a different context now The 2019 Strategy does not provide a plan for managing the cyber risks of today's h ghly olatile, complex, and interconnected environment. Attacks from hostile states and cybercriminals continue to mount, and their techniques continue to evolve, revealing a growing gap between the scale of threats and our capacity to defend ourselves from them. This weakness poses a significant threat to New Zealand's economic security.

5. To recalibrate our approach, a new Strategy and Action Plan have been developed. They are focussed on making New Zealand safer now and more resilient in the future, by strengthening the foundations of our cyber security and ensuring New Zealand has the right cyber capabilities and tools to advance our national security interests. The Strategy, and its Action Plan, have been developed based on domestic and international assessments of the cyber threat environment, and targeted engagement with industry. The

Action Plan includes a range of measures that would make New Zealanders safer and New Zealand more resilient to cyber threats now and into the future.

6. A key initiative under the Action Plan 2026-2027 is to improve the cyber security of our critical infrastructure, which is being repeatedly targeted by malign cyber actors, both for strategic advantage and financial gain. To manage the heightened threat level, we need to strengthen the cyber defences of our critical infrastructure so it is well-prepared to withstand and quickly recover from cyber incidents without disrupting provision of essential services. Australia, Canada, the European Union, the United Kingdom, the United States, Singapore and other partners are all progressing regulatory reforms in thi area.

7. Over the past two years, we have been working with industry which tells us that the cyber security of our critical infrastructure is not where it needs to be, and requires s me form of intervention. I propose to release a discussion document to test a package of proposed measures to do this, including voluntary and mandatory information sharing on threats and vulnerabilities, mandatory reporting of cyber incidents and minimum cyber risk management requirements for our most important infrastructure assets, and a power for the government to direct the management of cyber threats for national security reasons. The measures in the discussion document have been dev lop d through initial public consultation and targeted engagement with industry and ocal government reference groups.

Cyber risks are rising and pose a serious threat to New Zealand's national security

8. The security of cyberspace continue to d ter orate amid heightened geostrategic competition, protectionism, trade tensions and conflict. We are not immune to the growing threat as evidenced by a se ies of direct attacks on our people, government and critical infrastructure networks, including:

    a. the Waikato DHB ransomw re attack in 2021 that interrupted healthcare services for 400,000 people;

    b. ongoing industrial scale cybercrime coming from nations such as Myanmar, Laos and Russia, where law enforcement is tolerant or unable to act;

    c. the 2021 compromise of Parliamentary networks by an actor associated with the People's Republic of China's (PRC) Ministry of State Security;

    d evidence of Salt Typhoon, a PRC-affiliated advanced persistent threat, targeting organisations in New Zealand as part of an expansive global espionage campaign against telecommunications and broader critical infrastructure networks; and

    e. the Manage My Health cyber attack and extortion in late 2025 that compromised the personal information of around 100,000 patients.

9. These incidents show the cyber threat level has continued to increase across the full range of our national security interests, while our national cyber security has not kept pace. Malicious actors are growing more numerous and capable, including cybercriminals that have disruptive capabilities that rival some states. The latest Global Cybersecurity Index

ranks New Zealand in the third tier of cyber performance, grouped with developing countries still establishing good cyber security practices.[1] This is unacceptable, and highlights the level of risk that New Zealand is currently carrying. It also exemplifies how far we have fallen behind countries such as Australia, India, the Netherlands, Singapore, the UK and the United States, who rank in Tier 1 as 'role-modelling'.

A new Cyber Security Strategy would support prosperity and security

10. The current Cyber Security Strategy dates back to 2019 and does not provide a useful guide for dealing with current and future threats. New Zealand's strategic environment has changed, and the nature of the threat has evolved. We need a results-driven plan that addresses the cyber risks of today's highly volatile, complex and interconnected world. Since 2019 a gap has grown between the mounting cyber threats we face and our nati nal cyber resilience. This undermines New Zealand's economic security.

11. Reporting from domestic and international sources, including from industry nd the intelligence community, shows a clear increase in the scale and sophistication of the cyber security threats New Zealand is facing. All sources point to a need for New Zealand to have a growing and more effective cyber security capability across the government and private sector.

12. Cyber harm can cascade across our economy and have a crippling impact that is keenly felt by New Zealanders. Theft of intellectual property o trade secrets can erode our technological advantage. Disruption to businesses can propagate through supply chains, preventing access to critical goods and services, and causing loss of market confidence. Our citizens also continue to experience direct financial loss, with online threats costing New Zealanders at least $1.6 billion in 2024[2]

13. Strengthening our cyber defences is integral to protecting our economic security and ensuring that New Zealand is a s fe and secure place to do business. I am proposing a new Cyber Security Strategy for 2026-2030 (see Annex A) that sets a clear vision and elevates cyber security s a critical enabler for New Zealand's economic growth.

14. The Strategy would be supported by a series of Action Plans that take a broad national security approach. The first Action Plan for 2026-2027 (attached as Annex B) prioritises immediate a tions that can be delivered within agency baselines. Actions include:

    a. establishing a single point for cyber security incident reporting to improve the quality of data and make it easier to access advice, guidance and support;

    b developing a range of actions with industry to enhance the cyber security of critical infrastructure and raise cyber resilience across the economy (including the release of the discussion document on these actions which is outlined further below);

    c. managing public service use of high-risk products, services or vendors to reduce risk to government-held data; and

[1] New Zealand is the only developed economy listed in Tier 3. See United Nations' International Telecommunications Union, www.itu.int/epublications/publication/global-cybersecurity-index-2024

[2] Research found 54% of adult New Zealanders had experienced an online threat in the last six months and 830,000 had experienced some financial loss.

d. updating legislative powers to enable New Zealand's defence and security agencies to use cyber capabilities and tools to advance our national security interests.

15. The Manage My Health cyber incident is front of mind at present. The Action Plan includes two actions to enhance the security of New Zealanders' personal information and to deter the misuse of stolen data:

a. develop advice on incentives for protecting personal information from cyber threats, such as introducing a civil pecuniary penalty regime to the Privacy Act 2020; and,

b. a potential new offence targeted at people who view or disseminate personal information when they are aware it has been illegally obtained.

16. This advice will take account of the reviews of this incident being undertaken by Ministry of Health, Health New Zealand, and the Office of the Privacy Commissio er.

17. s6(a) [redacted]

18. New Zealand needs to position itself to keep pace with the rapidly evolving threat environment. The Action Plan 2026-2027, which is fully funded within agency baselines, includes essential measures for lifting our cyber security. But these actions on their own will not lift New Zealand's cyber capability and resilience to a level commensurate with the threats we face and will face in the future as the threat landscape evolves, there will be more we can and should consider doing.

19. The Strategy therefore commits to regularly reviewing the Action Plan, including during 2026-2027. These review will enable us to adapt our priorities, including as the threat changes, including potentially adding initiatives. To provide an indicative direction of future actions ut to 2030, Annex C sets out a non-exhaustive list of initiatives, some of which are already under development, and others that are in the preliminary scoping stage for consideration in the 2026/27 financial year and later Action Plans. This paper is not seek ng in principle approval of these initiatives – rather, it is illustrative of potential future a tions, subject to future analysis.

20. There are also several lines of effort that agencies are already progressing to improve New Zealand's cyber defence and capability, but require further policy work to determine scope, scale, and affordability beyond redeployment of existing baseline. As future Action Plans are developed, Cabinet may be invited to consider any key policy shifts or new lines of effort.

Enhancing the cyber security of the critical infrastructure system

21. To immediately progress a key initiative of Action Plan 2026-2027, I also propose to release a discussion document on a package of measures to enhance the cyber security of New Zealand's critical infrastructure system (see Annexes D and E).

22. The safe and secure operation of New Zealand's critical infrastructure underpins our economic growth, stability and prosperity, but is increasingly vulnerable to compromise by malicious cyber activity. Highly-sophisticated campaigns against critical infrastructure have affected many countries including New Zealand over recent years. Consultation and targeted engagement from 2023 to present has shown that the level of cyber security varies within and across sectors, and has not kept pace with the threat.

23. Cyber attacks on critical infrastructure can be debilitating by causing widespread service disruption that can cascade across sectors, such as blackouts, shutdown of health services, intermittent communications, severe transport delays, retail closure, and disr pt a range of lifeline services. This puts New Zealanders' lives at risk, jeopardises the functioning of government and halts productivity, with cascading consequences for our economic and social stability.

24. The critical infrastructure sector tells us that it does not hink it is possible for industry itself to drive a consistent and effective uplift in cybe sec rity across the critical infrastructure system. They argue that government i t vention is essential to set consistent minimum standards across the critical infrastructure system. Industry also argues that a systemic approach is necessary to man ge the dependencies and interdependencies between infrastructures – where a single vulnerability can trigger widespread outages across multiple ssential services. Officials have developed a package of proposed measures that would achieve this, and consider it is important to test possible approaches via a discussion document to ensure these are in the right place. The proposed measures include:

    a. a voluntary mechanism for government and infrastructure entities to exchange information to b ter understand cyber threats and approaches to mitigation,

    b. mandatory reporting of significant cyber security incidents to government to improve our collective understanding of threats and to target government support for response,

    c. mandato y minimum requirements to set a common baseline level of cyber security across all critical infrastructures, and/or

    d last resort powers to allow government to support and direct entities in response to cyber threats for national security reasons.

25. In the event that consultation shows strong support for some mandatory measures, Ministers would be invited to consider adopting requirements that would only apply to entities that meet a new, legislated definition of critical infrastructure. The proposed definition in the discussion document could result in approximately 200 of New Zealand's most important entities being designated 'critical infrastructure' across a range of sectors, including communications and data, defence, energy, finance, health, transport, and water. Any future legislative measures would also look to ensure regulatory

harmonisation with Australia where possible, given it has already improved its resilience in this area.

26. We want our approach to be flexible and responsive to evolving cyber threats, emerging risks and future innovation, while also accommodating differences in operating environments to ensure the impact on business is proportionate. Consultation would seek feedback from industry as to whether the proposed measures appropriately balance the cost of compliance with the economic benefits of enhanced cyber security, minimised disruption to business operations, and overall national security interests.

Implementation

27. Should Cabinet agree to the New Zealand Cyber Security Strategy 2026-2030, agencies will progress the initiatives set out in the Action Plan 2026-2027.

28. Should Cabinet agree to the release of the discussion document, I will r port back to Cabinet by July 2026 on the outcome of public consultation nd the recommended approach to enhancing the cyber security of critical infrastructur .

Implications

29. There are no direct financial costs at this stage. Future de isions on cyber security initiatives, including progressing the proposed measures in the critical infrastructure discussion document, may have financial implications. But these depend on the outcome of industry feedback on the discussion document, and subsequent decisions by Cabinet. There are no other cost-of-living, legal, population or climate implications in this paper.

30. A separate regulatory impact statement (RIS) s not required at this stage as analysis still needs to be completed for any propo ed regula ion. Given the need to acquire further information from industry, the d scussion document will clearly indicate that it is an open-ended consultation and submi sions on alternative ideas are welcome. A full RIS will be completed to accompany later Cabinet policy decisions on any legislative proposals.

31. Engagement with Iwi and Māori raised concerns around data sovereignty, digital inclusion and lit racy, and differing interpretations of what is considered ‘nationally significant . M asures to ensure that cyber security services delivered to the Māori population are fit for purpose are increasingly embedded into agencies’ service delivery planning. Data governance is primarily being addressed by Stats NZ.

Consultation

32. Feedback from engagement with industry on the Strategy and the first stage of the critical infrastructure work found participants were supportive of the need to improve New Zealand’s approach to cyber security. There is a risk that the Action Plan 2026-27 is seen by certain parts of industry as lacking ambition.

33. The following agencies were consulted on and are supportive of this paper: Ministry of Foreign Affairs and Trade; New Zealand Security Intelligence Service; Government Communications Security Bureau; Public Service Commission; Ministry of Business, Innovation and Employment; Ministry of Justice, New Zealand Police, Department of Internal Affairs, Ministry of Defence, New Zealand Defence Force, and New Zealand

Customs Service. A wider range of agencies were consulted on the discussion document including, in addition to the above: Civil Aviation Authority of New Zealand, Commerce Commission, Customs New Zealand, Electricity Authority, Financial Markets Authority, Health New Zealand, Maritime New Zealand, Ministry of Culture and Heritage, Ministry of Health, Ministry of Housing and Urban Development, Ministry of Primary Industries, Ministry for Regulation, Ministry of Transport, National Emergency Management Agency, New Zealand Infrastructure Commission, New Zealand Transport Agency, Reserve Bank of New Zealand, Treasury, and Water Services Authority.

Communications and Proactive Release

34. Officials will work with my Office to determine the appropriate timing and form or the release of the Cyber Security Strategy, and the commencement of public consultation on the discussion document. A redacted version of this Cabinet paper and associated documents will be proactively released at an appropriate time following Cabinet decisions.

Recommendations

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

1 **note** that threat assessments from domestic agencies, lose partners and industry point to a worsening cyber threat environment that is negatively affecting New Zealand through the impact of espionage, cybercrime, and disruption to critical infrastructure;

2 **agree** to the content and public release f the attached New Zealand Cyber Security Strategy 2026-2030, and supporting Action Plan for 2026-2027;

3 **note** that two actions in the Action Plan 2026-2027 directly address the need to strengthen the protection of personal data as evidenced by the Manage My Health cyber incident;

4 **note** the indicative direction of future actions and the need to regularly refresh the Action Plan to keep pac with the threat;

5 **note** that enhancing the cyber security of New Zealand's critical infrastructure is a key initiative of the New Zealand Cyber Security Strategy 2026-2030 and Action Plan 2026-2027;

6 **agree** to the public release of the discussion document, *Enhancing the cyber security of New Zealand's critical infrastructure system,* which outlines a package of proposed measures to drive a consistent and effective approach to managing cyber risks across the critical infrastructure system;

7 **authorise** the Minister for National Security and Intelligence to approve any necessary editorial, minor or technical amendments to the wording of the Strategy, its Action Plan and the discussion document before publication.

Rt Hon Christopher Luxon

Minister for National Security and Intelligence

The following annexes contained draft versions of documents. These annexes have been omitted from this proactive release package as finalised versions have been publicly released.

- Annex A: New Zealand's Cyber Security Strategy 2026 – 2030
- Annex B: New Zealand's Cyber Security Action Plan 2026 – 2027
- Annex E: Discussion document: Enhancing the cyber security of New Zealand's critical infrastructure system

Links to the published documents can be found in the cover page at the front of this release package.

ANNEX C
Indicative actions out to 2030

Policy initiatives currently under development

Action Plan 2026-2027 only includes actions that are fully funded within agency baselines.

These actions on their own will not lift New Zealand's cyber capability and resilience to a level commensurate with the threats faced. Agencies are therefore progressing policy wor on the additional initiatives below and will provide Cabinet with options on their scope, scale and cost in due course.

Initiative	Lead agency
s6(a), s9(2)(f)(iv)	

Policy initiatives to be scoped for future consideration

The following initiatives were identified through engagement with agencies and industry as meriting further consideration when developing future action plans. These are still at a preliminary scoping stage, and if progressed, may require changes to current policy settings and new funding.

Initiative	Lead agency
s6(a), s9(2)(f)(iv)	

ANNEX D

~~IN CONFIDENCE~~ UNCLASSIFIED

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

Enhancing the cyber security of the critical infrastructure system

The case for change: why we need a more modern posture on the cyber security of New Zealand's critical infrastructure

Cyber threats are escalating

- Cyber threats are escalating due to changing technology and a more contested world.
- Criminals are using increasingly sophisticated tools to extort ransoms or exploit data, while state actors are targeting critical infrastructure for espionage, influence and military advantage.
- New Zealand's critical infrastructure has been targeted, including attacks on Waikato DHB in 2021 and the NZX in 2022.
- In 2025, the NCSC identified evidence of Salt Typhoon, a group linked to China's government, targeting New Zealand entities.

Cyber investments are falling short

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

- Cyber security costs are borne directly by entities, but cascading disruption costs are economy-wide.
- Many critical infrastructure providers are monopolies or oligopolies, reducing consumers' power to drive investment.

Current regulatory settings do not address this:

- New Zealand largely relies on voluntary approaches to manage cyber risks to critical infrastructure.
- There is no single piece of legislation to achieve a consistent level of security across the entire critical infrastructure system.

The stakes are high

- New Zealand's critical infrastructure underpins our economy and society.
- It operates as an interdependent system. For example, energy and telecommunications underpin the operation of all other critical infrastructures, including transport, finance and health facilities.
- Beyond economic losses, cyber incidents impacting critical infrastructure could cause public health risks, social unrest, reduced trust in government and erosion of strategic advantage.

Other countries are taking action

- Like-minded countries are adopting legislated definitions of critical infrastructure and are setting requirements to ensure consistent minimum level of cyber security.
- There is a common ANZ market for infrastructure development, delivery and operation. It is important that we harmonise our legislation with Australia s6 a) while scaling any requirements to the New Zealand context.

There is broad support for security uplift, including from industry

- The New Zealand public rate cyber incidents and the failure of critical infrastructure as material national risks – they are both included in the National Risk and Resilience Framework.
- Respondents to DPMC's initial consultation almost universally agreed that New Zealand's infrastructure is not resilient enough, and that government has a role to play to ensure more is done.
- Industry and Local Government reference groups helped to shape the measures included in the discussion document.
- 32 government agencies and sector regulators have been consulted and are supportive of progressing to consultation.

The proposed changes: the draft discussion document engages the infrastructure sector on two questions

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

Identifying the infrastructure services we want to protect

- The draft discussion document sets out a principles-based approach to defining **critical infrastructure** and **critical infrastructure of national significance.** This builds on the definitions developed for the emergency management bill to create a harmonised approach across the infrastructure system.
- The definitions focus on the impact of the disruption of services on the economy and society.
- The discussion document includes draft thresholds across seven sectors:
  - Communications and data
  - Defence
  - Energy
  - Finance
  - Health
  - Transport
  - Drinking water and wastewater.
- Based on the current draft thresholds ~200 of New Zealand's largest and most important entities would be considered critical infrastructure.

Agreeing the depth of the critical infrastructure systems' cyber defences

- The draft discussion document sets out **six measures** which could work together, or individually, to enhance the cyber security of the critical infrastructure system.
- It includes voluntary and mandatory measures, but all would require an agreed definition of critical infrastructure and legislation to give effect to any measures progressed, even if compliance is voluntary. For example, there would need to be a mechanism established for secure voluntary information sharing.
- Measures are designed to deliver three outcomes:
  - an improved understanding of threats and vulnerabilities by critical infrastructure entities and government
  - a minimum level of cyber risk management by all critical infrastructure entities
  - effective management of cyber threats impacting national security by critical infrastructure entities
- The draft discussion document also sets out how government could monitor compliance to ensure that any requirements adopted do lift cyber security across the critical infrastructure system.

Next steps

- Proceeding to consultation does not commit the Government to any measure or action, but signals that the Government considers New Zealand's critical infrastructure system a matter of national security.
- The information gained in response to consultation will inform next steps in the policy process, including developing recommendations for your consideration.
- If we commence consultation early in 2026, we could provide recommendations before the next election, but Cabinet decisions by then are unlikely. Decision-making would likely be deferred until after the election.
- Proceeding to consultation would allow officials to make best use of the resources allocated to this work programme, and place the government in good stead to progress the work programme in the next term.