



23 July 2026

Ref: OIA-2026/27-0002

Tēnā koe

Official Information Act request relating to National Security, Sovereignty, and Strategic Risk Assessment of Data Centre Expansion

Thank you for your Official Information Act 1982 (the Act) request, which was transferred to the Department of the Prime Minister and Cabinet (DPMC) by the Minister of Defence on 30 June 2026. You requested:

Strategic Infrastructure

Please advise whether data centres are regarded as strategic infrastructure for national-security purposes. If so, what oversight mechanisms apply?

Foreign Ownership and Control

Please advise whether assessments have been undertaken regarding:

- Foreign ownership;
- Foreign control;
- Strategic dependency risks;
- Concentration of infrastructure ownership.

National Resilience

Please advise whether assessments have been undertaken regarding:

- Cybersecurity risks;
- Systemic vulnerabilities;
- Emergency response capability;
- Resilience during national crises.

Digital Sovereignty

Please advise whether the Government has assessed:

- Dependence upon foreign cloud providers;
- Strategic implications of offshore control;
- Long-term impacts on New Zealand's digital sovereignty.

Artificial Intelligence Infrastructure

Please advise whether any assessment has been undertaken regarding the national-security implications of rapidly expanding AI-related computing infrastructure.

Request for Evidence

Please identify all relevant risk assessments, security reviews, intelligence assessments, Cabinet papers, departmental advice, and expert reports relied upon.

Where such assessments have not been undertaken, please explain how the Government can be satisfied that current expansion aligns with New Zealand's long-term strategic interests and national resilience objectives."

On 12 July 2026, you refined your request (see Appendix 1). As we assessed that your refined request remained overly broad, we sought further refinement and invited you to

respond on or before 21 July 2026. As we have not heard from you, we have proceeded to respond to your refined request. While your refinement provides a timeframe, the request remains very broad. It spans multiple complex subject areas, a wide range of document types, several DPMC business units, and information that may have originated from, been received from, or referred to other agencies, including but not limited to MBIE, DIA, NZSIS, GCSB, Treasury and NEMA.

Information to be refused

Responding to the request as framed would require DPMC to search across multiple work programmes and information management systems, identify potentially relevant material, and assess whether each item relates to one or more of the matters listed in your request, and determine whether it was received, considered, relied on, summarised or referenced. This would require substantial collation and research.

DPMC has considered whether charging or extending the timeframe would enable the request to be met, as required by section 18A of the Act. DPMC has also considered whether further consultation would assist you to make the request in a form that would remove the reason for refusal, as required by section 18B. Given the breadth of the request and the extent of the searches and assessment that would be required, DPMC does not consider that charging, an extension, or further consultation would enable the request to be met without substantial collation or research. Your request is therefore refused under section 18(f) of the Act, as the information requested cannot be made available without substantial collation or research.

As advised in our consultation with you, some potentially relevant DPMC material is already publicly available and may assist you to make a more targeted request. This includes New Zealand's Cyber Security Strategy 2026–2030, the discussion document on enhancing the cyber security of New Zealand's critical infrastructure system, supplementary material on defining critical infrastructure, and related proactively released Cabinet material:

- [New Zealand's Cyber Security Strategy 2026 – 2030 - February 2026 - Department of the Prime Minister and Cabinet](#)
- [Discussion document: Enhancing the cyber security of New Zealand's critical infrastructure system - February 2026 - Department of the Prime Minister and Cabinet](#)
- [Supplementary document 1: Policy objectives, principles and assessment of measures - February 2026 - Department of the Prime Minister and Cabinet](#)
- [Supplementary document 2: Defining critical infrastructure - February 2026 - Department of the Prime Minister and Cabinet](#)
- [Proactive Release FPS-26-SUB-0004: New Zealand Cyber Security Strategy 2026-2030 and Enhancing the Cyber Security - April 2026 - Department of the Prime Minister and Cabinet](#)
- [Response to Official Information Act request OIA-2024/25-0655: Various documents regarding critical infrastructure and resilience - April 2025 - Risk and Systems Governance Group; Department of the Prime Minister and Cabinet](#)

If you wish to make a new request, DPMC suggests narrowing it to a specific topic, document type and timeframe. For example, you may wish to request formal DPMC advice to Ministers during a defined period on a single topic, such as critical infrastructure or cyber security.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on the DPMC website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Nāku noa, nā



Julian Grey
Acting Deputy Chief Executive
National Security and Resilience

Proactively Released

Appendix 1 – Refinement of 12 July 2026

Tēnā koe,

Thank you for your email of 9 July 2026 and for the opportunity to clarify my request.

I appreciate your advice regarding its scope. My intention is not to seek every document relating to data centres, but rather to identify the principal assessments, advice and decision-making documents relied upon by Government in considering the national security, resilience and sovereignty implications of the expansion of large-scale data centre and AI computing infrastructure in New Zealand.

For the purposes of this request, please interpret my reference to "strategic infrastructure" as including "critical infrastructure", where that is the terminology used by DPMC. To assist with processing, I refine my request as follows. This clarification is intended to reduce the scope of the request only. It should not be taken as withdrawing or limiting any of the substantive matters raised in my original request.

Timeframe

Please limit the search to documents created or received between 1 January 2024 and 21 June 2026, being the date of my original request.

Documents requested

For the avoidance of doubt, this request extends to all information held by DPMC that falls within the scope of this request, including documents that originated from another agency (including NZSIS, GCSB, MBIE, Treasury, NEMA, DIA, or any other department or agency) where those documents were received, considered, relied upon, summarised, referenced, attached to briefings, or otherwise informed advice or decision-making within DPMC.

Please provide copies of, or where appropriate identify by title, date and reference number:

- Cabinet papers and Cabinet minutes;
- Briefings or formal advice to Ministers;
- Departmental reports or policy papers;
- Risk assessments;
- Security reviews or security assessments;
- Strategic, resilience or dependency assessments;
- Intelligence assessments (where releasable or capable of being identified without prejudice to security interests); and
- Expert reports or independent advice commissioned by, or relied upon by, DPMC.

These documents are requested insofar as they relate to one or more of the following matters concerning data centres and associated AI computing infrastructure in New Zealand.

1. Critical infrastructure

Whether data centres are regarded as critical infrastructure (or otherwise strategically significant infrastructure) for national security purposes, and what governance, oversight or risk management mechanisms apply.

2. Foreign ownership and control

Any assessments relating to:

- foreign ownership;
- foreign control;
- strategic dependency risks;
- concentration of infrastructure ownership; or
- risks arising from reliance upon overseas-owned operators.

3. National resilience

Any assessments relating to:

- cyber security risks;
- systemic vulnerabilities;
- emergency response capability;
- continuity of essential services; and
- resilience during national emergencies or crises.

4. Digital sovereignty

Any assessments relating to:

- dependence upon foreign cloud providers;
- strategic implications of offshore ownership or control;
- long-term impacts upon New Zealand's digital sovereignty; or
- the Government's ability to maintain sovereign control over nationally significant digital infrastructure.

5. Artificial intelligence infrastructure

Any assessment concerning the national security, resilience or strategic implications arising from the expansion of AI-related computing infrastructure and associated hyperscale data centres.

Decision-making evidence

Please provide any advice, briefing, assessment, report, Cabinet paper, aide-mémoire, memorandum or other document that records how Ministers or officials satisfied themselves that the above matters had been adequately considered when developing or supporting Government policy relating to the expansion of data centre infrastructure.

If such documents were relied upon in whole or in part, I request copies or, where withholding grounds apply, sufficient particulars to identify each document.

If DPMC does not hold documents addressing one or more of the above matters, please confirm that no such documents are held in respect of those matters.

If any information is withheld, I request that each document withheld be identified separately together with the relevant provision of the Official Information Act relied upon, and the reasons for withholding.

I trust this clarification provides sufficient particularity to enable the request to proceed. If any aspect of the request remains unclear, I would appreciate DPMC providing reasonable assistance under section 13 of the Official Information Act to further refine the request, rather than refusing it under section 18.

For the avoidance of doubt, where any requested document is withheld in full, does not exist, or cannot be released, I still request that DPMC identify the document, where possible, by its title, date, author or originating agency, reference number (if any), and a brief description of its subject matter, unless that identifying information is itself withheld under the Official Information Act.

Thank you for your assistance. I look forward to your response within the statutory timeframe.

Nāku noa, nā,

