



Te Tira Tiaki
Government Communications
Security Bureau

PO Box 12209, Wellington 6144
P +64 4 472 6881, F +64 4 499 3701
www.gcsb.govt.nz

28 July 2025

Wendy McGuinness
[REDACTED]

Tēnā koe Wendy

Official Information Act request

Thank you for your Official Information Act 1982 (OIA) request, partially transferred to the Government Communications Security Bureau (GCSB) from the Department of Internal Affairs on 30 June 2025, as more closely connected to the functions of the GCSB. The parts of your request transferred to the GCSB asked for the following information:

“What is the plan for the GCSB and NZDF dedicated government data centre (mentioned above)? For example, will the new data centre store all New Zealand Government data or only a small portion (please explain roughly the percentage)? When will this new data centre be operational? Who will own the data centre? Will all data currently located offshore be removed from the overseas data centre and moved back to the new dedicated government data centre?”

...

Work is clearly underway to make New Zealand less dependent and more resilient, but we are keen to clarify the extent we are currently vulnerable and what success might look like in the next few years. Can you provide any documents that set out New Zealand's strategy on [the new data centre operated by the GCSB]?”

Response

It may be helpful if I provide some background information about why this data centre, named Mātai, was built. The GCSB is operating the data centre as the government's lead information security agency. This data centre is for a number of New Zealand government agencies to securely store some of their most sensitive data. The design and location of the facility were informed by a number of factors, including our unique environment and New Zealand's specific data storage needs. Security of the data is a key consideration, which is part of why the facility is hosted on a New Zealand Defence Force base.

The plans for this centre arose following a Strategy, Capability and Resourcing Review by the New Zealand Intelligence Community, which was considered by the Cabinet National Security Committee in March 2016. The New Zealand Intelligence Community is comprised of the GCSB, NZSIS, and what was then known as the Security and Intelligence Group at the Department of the Prime Minister and Cabinet. The Cabinet Committee agreed that a tagged capital contingency for the proposed new data centre would be subject to a separate business case. A detailed business case was subsequently considered by the Cabinet

External Relations and Security Committee in May 2019, with construction beginning in September 2022.

We took possession of the data centre on 30 May 2025, the day the centre reached practical completion. The data centre was then officially opened on 27 June 2025 by the Minister Responsible for the GCSB, and Minister of Defence, Hon Judith Collins KC, with an opening ceremony at RNZAF Base Auckland. We plan for this centre to be able to store our government's most sensitive information for at least 25 years.

This centre will not store all of our government's data – it will only store some of the most sensitive information held by a number of our public sector agencies. I am unable to provide the percentage of all public sector data that this represents. The focus of this centre is around the sensitivity of the information it will store, rather than the amount of data it will store across our entire public sector.

I can however advise that there are a number of public sector agencies in New Zealand whose work intersects with national security considerations. The Government's National Security Intelligence Priorities¹ range from countering foreign interference and espionage, to countering malicious cyber activity, to economic security. This centre will therefore store a broad range of agencies' sensitive information, where the information involved in this work can require specific data considerations around handling and storage.

As you alluded to in your request, data sovereignty is an important consideration around the storage of New Zealand's sensitive information. A key requirement for this centre therefore is that the data it stores will be protected in accordance with New Zealand's requirements, namely those in the New Zealand Information Security Manual² and the Protective Security Requirements.³ A key consideration in this guidance is that New Zealand's most sensitive data is already stored within New Zealand, therefore data repatriation is not our focus with this data centre.

Improving resilience has been on our mind throughout this build. With regard to the second part of your request, for strategy documents in relation to our data centre, it is necessary to withhold most of this information under section 6(a) of the OIA, to avoid prejudice to the security or defence of New Zealand or the international relations of the Government of New Zealand. I can however advise that one of these documents was partially titled "Data Centre Strategy", dated April 2016. This noted "*[f]or the purpose of this strategy any solution which involves non-sovereign hosting of data has been excluded.*"

I am also able to provide you with a summary of some relevant information, as allowed for under section 16(1)(e) of the OIA. The Cabinet paper considered by the Cabinet External Relations and Security Committee in May 2019 included the following key points, as summarised below:

Four short-listed location options were outlined, all within the North Island. These shortlisted options were evaluated against criteria relating to cost, benefit and risk. Value for money was a strong factor, as was geographical diversity and resiliency, with a preference for existing Crown land. The evaluation followed Treasury guidelines for situations in which investment objectives – in this case, objectives relating to the

¹ Available online at: <https://www.dpmc.govt.nz/our-programmes/national-security/national-security-intelligence-priorities>

² Available online at: <https://www.nzism.gcsb.govt.nz>

³ Available online at: <https://protectivesecurity.govt.nz>

performance, efficiency, resilience, sustainability and security of data infrastructure – cannot be monetised.

The paper noted the GCSB and the NZSIS participated in this process, as did other key New Zealand government departments, given the need for some of their information to have additional protection against malign actors. To provide additional independent assurance, a specialist consultant was appointed to test how the options were selected and evaluated. A geotechnical consultant was appointed to provide advice on relative levels of risk for different site locations and consequential implications for the resilience of the data infrastructure.

The key finding of the evaluation process was that building at Whenuapai would provide the greatest value for money when taking account of all factors. A data centre built at this location was determined to provide equal or higher levels of resilience and security than any of the other options, and to provide sufficient levels of infrastructure performance.

Review

If you would like to discuss this response with us, please feel free to contact information@gcsb.govt.nz.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that the GCSB proactively publishes OIA responses in accordance with the expectations of Te Kawa Mataaho/the Public Service Commission. We may publish this response (with your personal information removed) on the GCSB website.

Ngā mihi

[Redacted signature block]

[Redacted line]

[Redacted line]

[Redacted line]