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

31 March 2026

Sam Brown
fyi-request-33468-f6fe4ceb@requests.fyi.org.nz

Tēnā koe Sam

Official Information Act request

Thank you for your Official Information Act 1982 (OIA) request of 8 January 2026 to the Government Communications Security Bureau (GCSB) seeking information about national security assessment of satellite communications infrastructure dependencies. I apologise for our response not meeting the statutory deadline due to reduced capacity while we recruit to fill vacancies in our official correspondence team.

Response

While we are not able to provide information at an unclassified level in response to your request, I would like to provide some context about the role of the GCSB when providing national security risk assessments and advice to policy and decision makers.

Under Part 3 of the Telecommunications (Interception Capability and Security) Act 2013, the GCSB undertakes national security risk assessments to provide advice to decision makers to keep New Zealand's public telecommunications network secure. Any network operator providing telecommunications services in New Zealand, when they meet the prescribed thresholds, must engage with the GCSB for this purpose.

Similarly, the GCSB provides national security advice to decision makers in relation to issuing licences for satellite ground stations under the Radiocommunications Act 1989.

My responses to your questions are as follows.

***1. Any unclassified or partially declassified threat assessments, risk analyses, or security evaluations regarding**:*

> *- New Zealand's increasing dependency on foreign-controlled satellite communications systems for essential services, government operations, or critical infrastructure*
>
> *- Signals intelligence vulnerabilities when New Zealand internet traffic is routed through satellite systems controlled by foreign entities*
>
> *- Data sovereignty implications of satellite internet providers routing traffic through foreign jurisdictions*

- National security considerations of critical infrastructure (emergency services, healthcare, education, business operations) depending on single foreign-owned connectivity provider

The GCSB has no unclassified assessments on satellite internet service providers. Your request is therefore refused under s18(e) of the OIA, as the information does not exist.

The GCSB would undertake a national security risk assessment where this technology meets the criteria for assessment under specific regulatory regimes, for example the Telecommunications (Interception Capability and Security) Act 2013.

***2. Any unclassified guidance, standards, or recommendations provided to government agencies regarding**:*

- Appropriate use cases for satellite internet versus terrestrial connectivity for handling sensitive information

- Security requirements for connectivity used by government agencies or critical infrastructure operators

- Risk mitigation measures when using foreign-controlled communications infrastructure

- Whether satellite internet services meet Government security requirements for official purposes

The New Zealand Information Security Manual (NZISM) details processes and controls for the protection of all New Zealand Government information and systems. This includes requirements relating to connectivity used by government agencies.

In 2024 the National Cyber Security Centre joined the Australian Cyber Security Centre and other international partners to support the release of guidance on cyber security for operational technology (OT).

The guidance includes creating and maintaining a definitive view of an agency's OT architecture – Principle 4 provides guidance on (amongst other things) Exposure, Redundancy, and Availability of connectivity for Operational Technology used by critical infrastructure.

Secure connectivity principles for Operational Technology (OT) provides more comprehensive guidance on connectivity for Operational Technology used by Critical Infrastructure.

While not specific to satellite internet providers, this guidance provides government agencies with the tools to consider a range of issues to consider when assessing if satellite internet is the most appropriate connectivity for their purposes.

The NZISM is available here: nzism.gcsb.govt.nz

3. Any assessment (at unclassified level) of scenarios where:

- Foreign government threatens to, or directs satellite provider to limit, terminate, or monitor New Zealand communications

- Satellite provider experiences technical failure, service withdrawal, or degradation affecting New Zealand essential services

- Entire communities or regions lose connectivity simultaneously due to single-provider dependency

- Geopolitical tensions affect availability or integrity of satellite communications services

GCSB holds no information in scope of this question. Your request is therefore refused under s18(e) of the OIA, as the information does not exist.

4. Any correspondence with other government agencies or Ministers regarding:

- Security implications of policy decisions that increase dependency on foreign-controlled satellite communications

- Whether security considerations have been incorporated into rural connectivity policy or funding decisions

- Concerns about infrastructure resilience when terrestrial alternatives are eliminated

- Whether GCSB security assessments or recommendations have informed telecommunications policy development

GCSB holds no information in scope of this question. Your request is therefore refused under s18(e) of the OIA, as the information does not exist.

5. Any coordination with Five Eyes intelligence partners regarding:

- Security posture or threat assessments of commercial satellite communications providers

- Recommendations for security standards or usage restrictions for satellite services

- Intelligence sharing implications when allied nations' communications route through foreign-controlled satellite networks

A guidance publication titled *Securing Space – Cyber security for low earth orbit satellite communications* is publicly available here: https://www.ncsc.govt.nz/protect-your-organisation/low-earth-orbit-satellite-communications/

The document was authored by the Australian Signals Directorate and co sealed by GCSB's National Cyber Security Centre and other international partners. It is relevant to both Network Operators and Internet Service Providers.

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.

Ngā mihi

Andrew Clark
Te Tumu Whakarae mō Te Tira Tiaki
Director-General, GCSB