NEW ZEALAND SPACE AGENCY

Due diligence guidance for ground-based space infrastructure

What is due diligence?

Due diligence is a systematic assessment of the risks associated with any business, research, or investment decision with a new partner, collaborator or customer. Due diligence should be carried out throughout the lifecycle of a business relationship, partnership, or investment.

Strong due diligence practices not only protects your own intellectual property and assets, but also New Zealand's national security.

Obligations under the Outer Space and High-altitude Activities Act 2017

Section 49A of the Outer Space and High-altitude Activities Act 2017 (the Act) requires ground-based space infrastructure (GBSI) operators that are carrying out a regulated activity to hold a GBSI activity authorisation.

Section 49B of the Act requires GBSI operators to declare that they have internal due diligence processes in place that identify the steps that they will take to verify the identity of any partners and understand the nature of their partners' activities.

Section 49D of the Act requires authorisation-holders to provide MBIE with an annual report confirming their due diligence arrangements, if they have partners.

'Partner' means anyone whose behalf, or for whose benefit, a person operates, or proposes to operate, GBSI to carry out regulated activities (for example, a customer or research collaborator).

The purpose of this requirement is ensure that operators:

- manage the risk that they might inadvertently provide services or infrastructure to entities that may negatively impact New Zealand's national security or national interest, such as actors who are subject to sanctions or involved in espionage or foreign interference. ensure they can carry out an assessment and take action if there are changes in their business relationships with partners, such as a change of ownership in a partner organisation.

The Protective Security Requirements' Due Diligence Assessments prepared for Research Institutes provides some useful information about the kind of risks that may arise with research activities and how to manage them. As similar risks arise with GBSI, this guidance should also be considered alongside this guidance when conducting due diligence.

The level of due diligence required depends on the nature of the activity and the likely risks that are associated with it. Generally due diligence will not require anything more than desktop research to confirm that the information the operator has provided is consistent with publicly available information.

Things to consider as part of due diligence

The degree of due diligence conducted should be proportionate to the potential risks. However, as a starting point, operators should consider the following questions regarding partners and the GBSI itself to help build an approach to due diligence:

Partner ownership and transparency

- Who is the parent company of the partner?
- Who are the primary customers of the partner?
- What is the country of ownership?
- Where does the partner do business?
- Is the partner associated with a country that may not share New Zealand's values or is involved in an international conflict?
- Could the partner be acting on behalf of a foreign state?
- How forthcoming is the partner with providing information?

End use

- What is the intended purpose of the GBSI, and are there any ethical considerations around its use, such as a clear link to international human rights abuses, criminal activity, links to sanctioned entities etc?
- Have you considered all the potential use cases for the GBSI?
- Does the partner have any involvement in working on behalf of a military or police organisation of a foreign government?

Ethical and reputational concerns

- Are there potential reputational or ethical risks associated with the partner, or if your organisation proceeds with a relationship with them?
- Would proceeding with a partner relationship raise potential conflicts with other partner relationships?

Operators should consider the answers to these questions when deciding whether to proceed with a relationship with a particular partner. However, this is not an exhaustive list. There are further questions for consideration in the due diligence guidance links below.

Resources

There are a range of additional resources available that outline things to consider in relation to due diligence processes:

- NZSIS's Security Threat Environment Reports (All years)
- NZSIS published a case study on a security threat affecting GBSI in its 2024 report – NZSIS's New-Zealands-Security-Threat-Environment-2024.pdf (page 21) (https://www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2024.pdf).
- PSR's Secure Innovation Guidance (Secure-Innovation-Security-Advice-for-Emerging-Technology-Companies.pdf)
- PSR's Trusted Research Guidance (psr-trusted-research-guidance-spreads.pdf)
- MBIE's Managing National Security Risks in Procurement (https://www.procurement.govt.nz/assets/procurement-property/documents/managing-national-security-risks-guidance.pdf)

For any national security concerns, operators should report it on the NZSIS website.

If you have any questions about this due diligence guidance, please get in touch with the New Zealand Space Agency at: nzspaceagency@mbie.govt.nz.

If any concerns are identified during a due diligence process, do not proceed with the relationship with the proposed partner, or contact the New Zealand Space Agency at nzspaceagency@mbie.govt.nz for additional guidance.