NEW ZEALAND SPACE AGENCY

Protective security guidance for ground-based space infrastructure

What is protective security?

Protective security is a series of risk management measures designed to help organisations and communities protect their people, information and assets. Effective security enables organisations to work together securely in an environment of trust and confidence.

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 an operator intending to operate a GBSI to submit to MBIE a declaration stating that they have protective security arrangements in place that:

- identify the security risks associated with the activities that they propose to carry out under the authorisation
- establish reasonable measures to manage those risks.

Section 49D of the Act requires authorisation-holders to provide MBIE with an annual report confirming that their protective security arrangements continue to meet the requirements.

The purpose of the protective security requirements in the Act is to ensure that operators manage the physical, information and personnel security risks associated with operating GBSI, and ensure regular review of their settings to ensure they remain fit for purpose.

Operators should use the below guidance in setting up and reviewing their protective security measures.

What are my vulnerabilities?

There are a number of methods malicious actors may use against you and your assets. It is important to know your potential vulnerabilities:

- **Insider access** – Your people are your greatest asset, but in some cases, they can pose a risk of insider threat.
- **Cyber access** – Insecure IT can provide an easy way for your business to be exploited.
- **Physical access** – Tangible or digital assets could be stolen directly from your place of work.
- **International travel** – State actors can operate more easily overseas than in New Zealand.
- **Investment** – Investment can be used to gain access to, and influence over, your company.
- **Overseas jurisdictions** – International expansion exposes you to security risks from local laws and foreign business practices.

- **Supply chain** – Vulnerable or malicious suppliers could compromise your business.

Take the time to understand and think through how different threats can impact your business.

What protective security arrangements should I put in place?

Protective security settings should be proportionate to the potential risks. However, as a starting point, you should consider the following in relation to your security settings:

- **Ownership** – who will lead and be accountable for your security?
- **Identification** – which assets are most critical to your success?
- **Assessment** – What's your level of security risk?
- **Mitigation** – How can you lower your risk level?
- **Foundations** – How can you make security part of your business?

New Zealand government advice on how to consider these questions is available in the Secure Innovation Guidance: Secure-Innovation-Security-Advice-for-Emerging-Technology-Companies.pdf

Where can I find more information?

The New Zealand Protective Security Requirements framework (Home | Protective Security Requirements) provides useful guidance to GBSI operators on protective security settings. The requirements are designed for New Zealand Government agencies, so operators should consider which of the requirements are appropriate and proportionate for their business.

There are a range of other resources available that outline things to consider in relation to your protective security settings:

- Trusted Research Guidance (psr-trusted-research-guidance-spreads.pdf)
- National Cyber Security Centre, Cyber Security Framework (NCSC Cyber Security Framework)
- National Cyber Security Centre Guidance, Protect Yourself from Ransomware (Protect your organisation against ransomware)

There is also a range of resources to help you understand the security risks relevant to ground-based space infrastructure. Each year the New Zealand Security Intelligence Service (NZSIS) publishes a Threat Environment Report. The report provides insight into national security risks in New Zealand and is designed to support decision-making or facilitate discussions on what impact these risks may have on your business.

- New-Zealands-Security-Threat-Environment-2023.pdf
- New-Zealands-Security-Threat-Environment-2024.pdf
- New-Zealands-Security-Threat-Environment-2025.pdf

There are some general resources that, although are not specific to GBSI, provide additional context on the potential risks to space activities:

- Center for Strategic and International Studies, Space Threat Assessment 2025 (2025 Space Threat Assessment)
- European Union ENISA – Space Threat Landscape (incl. mapped controls) (From Cyber to Outer Space: A Guide to Securing Commercial Satellite Operations | ENISA)
- NASA Space System Protection Standard (SPACE SYSTEM PROTECTION STANDARD | Standards)
- NASA Space Security Best Practice Guide (7.22 - Space Security: Best Practices Guide - SW Engineering Handbook Ver D - Global Site)
- Cybersecurity and Infrastructure Security Agency (CISA):
    - Space Systems and Service (Space Systems and Services | CISA)

- Recommendations to Space Systems Operators for Improving Cybersecurity (Recommendations to Space System Operators for Improving Cybersecurity | CISA)
- Space System Security and Resilience Landscape: zero trust in the space environment (Space System Security and Resilience Landscape: Zero Trust in the Space Environment | CISA)

Operators should report any cyber incidents on the NCSC website. Operators should report any other national security concerns on the NZSIS website.

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