



COVERSHEET

Minister	Hon Judith Collins, KC	Portfolio	Space
Title of briefing	Introduction of the High-Altitude Activities Amendment Bill	Date to be published	10 October 2025

List of documents that have been proactively released

Date	Title	Author
July 2025	Introduction of the High-Altitude Activities Amendment Bill	Office of the Minister for Space
17 July 2025	Introduction of the High-Altitude Activities Amendment Bill LEG-25-MIN-0135 Minute	Cabinet Office
9 July 2025	Regulatory Impact Statement: Ground Based Space Infrastructure Regulatory Regime	MBIE

Information redacted

YES / NO

Any information redacted in this document is redacted in accordance with MBIE's policy on Proactive Release and is labelled with the reason for redaction. This may include information that would be redacted if this information was requested under Official Information Act 1982. Where this is the case, the reasons for withholding information are listed below. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Some information has been withheld for the reasons of protecting national security and confidential advice made to Government.



Regulatory Impact Statement: Ground Based Space Infrastructure Regulatory Regime

Decision sought	<i>Final Cabinet decision on the regulatory design for managing risks to ground based space infrastructure</i>
Agency responsible	<i>New Zealand Space Agency within the Ministry of Business, Innovation and Employment.</i>
Proposing Ministers	<i>Minister for Space</i>
Date finalised	<i>9 July 2025</i>

This proposal details a regulatory regime to manage the risks posed by ground-based space infrastructure (GBSI). This will be achieved through an authorisation regime implemented through the Outer Space and High-Altitude Activities Act 2017 (OSHAA).

Summary: Problem definition and options

What is the policy problem?

Ground-based space infrastructure (GBSI) refers to the systems on Earth that track and communicate with spacecraft. Foreign actors that do not share New Zealand's values and interests have attempted to covertly establish or use GBSI in New Zealand. This gives rise to the risk that GBSI sited in New Zealand could be used to support activity that could harm New Zealand's national security or be contrary to our national interests **National security or defence**. To date these risks have been managed primarily through non-regulatory measures, such as education and outreach, however, these measures are not adequate, as interest in New Zealand as a GBSI location is increasing and we currently have no regulatory levers to stop problematic GBSI activity that is already underway.

Consulted GBSI operators supported the establishment of a regulatory regime for GBSI. Through non-regulatory measures, officials have positive relationships with a number of major GBSI operators in New Zealand. So far, this approach has proved effective in preventing malicious approaches, however officials expect approaches to continue and currently do not have the regulatory measures to prevent harmful activity, and/or shut down operations that don't comply with New Zealand's national security/interest.

What is the policy objective?

The regime's objective is to manage national interest and national security risks posed by GBSI through a proportionate regime. The regime will manage these risks by enabling the regulator to:

- Deter – implementing a regime will likely deter malicious actors from attempting to undertake GBSI activities in New Zealand knowing legislation exists.
- Detect – the regime will allow the regulator to detect some illicit or concerning behaviour.
- Deny – the regime's enforcement provision affords the regulator the ability to seize equipment of offending parties

The objectives for a GBSI regulatory regime are based on the principles previously agreed by Cabinet:

- Mitigate the risk GBSI poses to New Zealand's national security and national interests by providing means to deter, detect and deny GBSI activity that presents the highest potential harm to New Zealand's interests, including national security
- Complement (rather than duplicate) existing regulatory and non-regulatory measures that apply to GBSI (e.g., Radiocommunications Act, Overseas Investment Act, MBIE's relationships with commercial providers and universities).
- Impose minimal costs on the regulated entities and on agencies involved in administering the regime while providing adequate information to inform decision making.
- Remain durable and flexible to keep pace with rapidly changing technologies.
- Provide a sufficient level of certainty, predictability and transparency to regulated entities.
- The success, or failure, of the regime will be measured by the presence of GBSI activity that is contrary to New Zealand's national interest/security.

What policy options have been considered, including any alternatives to regulation?

Four options were considered:

- Option one – counterfactual: continued use of non-regulatory measures to try to manage increasing risks.
- Option two – a notification and call-in regime: GBSI operators would be required to notify the regulator of their GBSI use, and the regulator would have the power to "call in" the notification for further assessment.
- Option three **[PREFERRED]** – an authorisation regime: GBSI operators would need to apply to the regulator for authorisation of their GBSI use and would be subject to ongoing monitoring and reporting requirements.
- Option four – a licensing regime: GBSI operators would need to apply for a licence to undertake in-scope GBSI activity in New Zealand.

An authorisation regime is preferred as it delivers the best balance between effectively managing risks while ensuring the costs of the regime are proportionate.

What consultation has been undertaken?

A targeted consultation with domestic GBSI operators was undertaken to seek their views on the scope and options for the design of the regime. The industry was provided with a discussion document for consultation, with several weeks to consider and provide comments. Officials also offered meetings with known GBSI

RESTRICTED

operator, with participating operators offered the opportunity to comment on the scope of the regime.

Stakeholders that responded broadly supported the proposed regime scope and no stakeholders were opposed to the recommended authorisation regime for GBSI.

Engagement was further sought with all relevant agencies (Ministry of Foreign Affairs and Trade, Department of Prime Minister and Cabinet, Government Communications Security Bureau, New Zealand Security Intelligence Service, Land Information New Zealand, Ministry of Defence, New Zealand Defence Force, Ministry of Justice, Office of the Privacy Commissioner). Agencies are supportive of the proposed GBSI regime.

Is the preferred option in the Cabinet paper the same as preferred option in the RIS?

Yes

Summary: Minister's preferred option in the Cabinet paper

Costs (Core information)

Outline the key monetised and non-monetised costs, where those costs fall (e.g. what people or organisations, or environments), and the nature of those impacts (e.g. direct or indirect)

Compliance with the regulatory regime for applicants will require a relatively minimal upfront administrative cost to apply for authorisation. There will be ongoing costs to set up and maintain due diligence and protective security systems, should they not already exist.

We anticipate an estimated cost of two FTEs at MBIE to resource the regime, plus additional costs for potential compliance and enforcement action. Confidential advice to Government

Confidential advice to Government

Benefits (Core information)

Outline the key monetised and non-monetised benefits, where those benefits fall (e.g. what people or organisations, or environments), and the nature of those impacts (e.g. direct or indirect)

Managing the risk that GBSI could be used to harm New Zealand's national security or be used in ways that are contrary to New Zealand's national interest will have the ongoing benefit of making New Zealand safer.

Protective security and due diligence requirements will likely have ongoing benefits for GBSI operators beyond regulatory compliance, e.g., protecting their business, mitigating reputational risks, protecting intellectual property, protecting physical property from theft or damage. The regime also provides certainty about how to identify and manage risks. Less reliance on non-regulatory measures and a better understanding of how to apply non-regulatory measures will lessen the burden on agencies implementing these measures and provide access to a broader suite of tools to respond to risks.

Less reliance on non-regulatory measures and a better sense of how best to apply non-regulatory measures will lead to an ongoing reduction in burden on agencies

implementing these measures and provide access to a broader suite of tools to respond to risks.

Managing the risks that GBSI in New Zealand that could be used to harm New Zealand's interests **National security or defence** will likely enhance New Zealand's reputation as a trusted space partner and support the international space relationships we rely on.

Balance of benefits and costs (Core information)

Does the RIS indicate that the benefits of the Minister's preferred option are likely to outweigh the costs?

Based on Cabinet's direction to design a regime to manage significant risks relating to GBSI, the proposed regime meets the criteria and the RIS suggests that the benefits in risk management will outweigh the costs of resourcing the regime.

The regime has been designed specifically to minimise costs while still effectively managing risks, as we expect more GBSI activity over time, and thus ongoing costs. One of the key pillars of design for the regime was proportionality – to ensure the implemented regime manages the risk without overburdening the sector.

We expect there to be administration costs for regulated entities, however this means that there will be fewer costs over the lifetime of operations. For the regulator, an authorisation regime with an assessment function lowers the requirement for additional resources for up front assessments.

Implementation

How will the proposal be implemented, who will implement it, and what are the risks?

The proposal will come into effect in July 2025. The regime applies to all GBSI operators conducting activities in scope of the regime, including those that were underway before the regime was established. The regime will be implemented by MBIE with the Minister for Space as the regulatory decision maker. There is currently no funding identified to support the implementation of the regime.

There may be some limited overlap with a small number of existing and proposed regulatory regimes, such as the radio spectrum management regime, and the GBSI regime. However, we will deconflict any regimes that may have overlap with GBSI.

Limitations and Constraints on Analysis

Uncertain implementation costs

It is difficult to accurately predict the amount of GBSI that might be established in New Zealand in the future with limited underlying data. Officials have attempted to identify GBSI operators currently operating in New Zealand, however we cannot know exact numbers until authorisation is implemented as not all GBSI are required to go through other regulatory regimes.

As a result, the GBSI regime implementation costs for the regulator are based on a very rough estimate. The potential impact of this is reduced through our preferred option, as it seeks to minimize the burden on the regulator, but there is still some residual uncertainty.

RESTRICTED

I have read the Regulatory Impact Statement and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the preferred option.

Responsible Manager(s) signature:

Andrew Johnson
Manager – Space Policy and
Sector Development



9 July 2025

Quality Assurance Statement	
Reviewing Agency: MBIE	QA rating: Meets
Panel Comment: MBIE's Quality Assurance Panel has reviewed the Regulatory Impact Statement prepared by the MBIE Space Policy and Sector Development Team and considers that it meets the quality assurance criteria.	

Section 1: Diagnosing the policy problem

What is the context behind the policy problem and how is the status quo expected to develop?

Background

Ground-based space infrastructure is an essential part of space operations

1. Ground-based space infrastructure (GBSI) is used to communicate with, operate and track spacecraft (e.g., satellites) from Earth.
2. GBSI covers a wide range of infrastructure including satellite aerals, receiving stations, radars, and optical and radio telescopes.

New Zealand is an attractive location for GBSI and demand for GBSI is increasing

3. GBSI is vital to maintaining communication between the Earth and satellites, making it an essential part of satellite systems. Many satellite applications rely on near-continuous communication between space and Earth, which requires access to a global network of GBSI to ensure there are sufficient opportunities for data to be transmitted to and from satellites as they orbit Earth.
4. New Zealand's geographic location makes it well positioned for offering relatively rare Southern Hemisphere GBSI coverage. [REDACTED] National security or defence [REDACTED] New Zealand can be the first or last significant landmass sighted by an orbiting satellite. Combined with an advanced fibre relay network and clear skies for making space observations, New Zealand is a sought after, and in some cases integral, location for GBSI.
5. The number of satellites in Earth orbit has increased considerably over recent years, leading to growing demand for satellite data relay and transfer capability.

6. [REDACTED] National security or defence [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Context

Great power competition is playing out in space

7. Space is contested and competitive, leading to an increasingly prevalent view of space as a geopolitical domain, as countries seek to use space technologies to further their military and security ambitions.
8. Modern militaries rely heavily on space-based systems for intelligence, surveillance and reconnaissance; communications; and position, navigation and timing.
9. [REDACTED] National security or defence [REDACTED]
[REDACTED]
[REDACTED] Diverging views in multilateral negotiation processes continue to prevent consensus on appropriate international rules and norms to regulate responsible behaviour in relation to space capabilities.

RESTRICTED

GBSI can give rise to risks to New Zealand's national security and broader national interests

10. Like most space technology, GBSI is dual use in that it can be used to carry out both civilian and military functions. It can, therefore, be used to further the military interests of states that do not share New Zealand's values.

11. **National security or defence**
- [Redacted]

12. Foreign actors that do not share our values and interests could use GBSI in New Zealand to undertake activities that present a risk to our national security and broader interests through:

- a. **National security or defence**
- [Redacted]

- b. **National security or defence**
- [Redacted]

13. There are two categories of GBSI – radio and optical. Radio GBSI uses radio waves to communicate with satellites, while optical GBSI uses light to monitor satellites. Both types of GBSI could give rise to the risks outlined above. Of particular concern is GBSI carrying out:

- a. Telemetry, tracking and control: GBSI receives data on a satellite's status and location and gives commands to the satellite. This typically refers to GBSI communication with a cooperative satellite.
- b. Space object surveillance and identification: GBSI is used to observe, identify and track space objects. This can be used for uncooperative satellites **National security or**
- c. Data reception: GBSI receives data collected by the satellite's sensors, for example, Earth-observation images **National security or defence** and position, navigation and timing applications.

14. Having the above activity take place in New Zealand by entities from states that do not share our values and interests could have serious consequences for our national security. **National security or defence**
- [Redacted]

Status quo

15. Currently GBSI risks are managed through a combination of regulatory and non-regulatory measures as outlined in Table 1. There are a number of gaps in the current approach which limit the effectiveness of managing risk in this way.

RESTRICTED

Table 1: current measures for managing GBSI national interest and national security risks

	Telemetry, tracking and control (TT&C) (Radiofrequency based)	Telemetry, tracking and control (TT&C) (Optical)	Space object surveillance and identification (SOSI) (Radiofrequency based)	Space object surveillance and identification (SOSI) (Optical)	Data reception (Passive radiofrequency or optical)
Radiocommunications Act	Regulates transmission to manage interference. National interest managed through a Government Policy Statement, and national security in secondary legislation.	No coverage	Regulates transmission to manage interference. National interest managed through a Government Policy Statement, and national security in secondary legislation.	No coverage	No coverage
Overseas Investment Act	Partial coverage – only in cases involving foreign ownership which meets thresholds/criteria in the Overseas Investment Act.				
Outer Space and High-altitude Activities Act	No coverage – only requires launch and high-altitude licence holders to disclose details of spectrum authorisation for GBSI used to transmit to the launch or high-altitude vehicle				
Non-regulatory measures	Partial coverage – where the activity is enabled by an established provider with whom the Government has a relationship				

The Radio Communications Act does not manage national interest and national security risks

16. The Radiocommunications Act 1989 regulates radiofrequency transmission from GBSI through a range of bandwidths, depending on operator needs. However, the Act's purpose is protection from radio frequency interference, so there is national interest provision in the Radiocommunications Act (although the Radiocommunications Regulations 2001 do allow for revocation of radio licences on the basis of national security). There are also gaps in GBSI coverage under the Radiocommunications Act:
 - a. No licence is necessary for downlink (reception of data from a satellite) unless the operator chooses to apply for protection from radio interference. A receive-only station can collect large amounts of satellite data.
 - b. The optical part of the electromagnetic spectrum is not covered by the Radiocommunications Act at all. Optical GBSI is therefore, currently unregulated.
17. In 2021 and 2023, further measures were established to manage GBSI risks as a stop-gap measure. Statements of Government Policy and Directions were released which established the Government's radiocommunications policy objectives under the Radiocommunications Act.
18. Pursuant to these objectives, the Statement included direction to seek national security advice from the New Zealand Security Intelligence Service and the Government Communications Security Bureau in relation to issuing licences for satellite ground stations and to have regard to the impact of approving or declining the application on New Zealand's national security and/or national interest.

RESTRICTED

The Overseas Investment Act doesn't capture most GBSI activity in New Zealand

19. The Overseas Investment Act 2005 (OIA) would capture GBSI if an overseas person requires consent to establish GBSI in New Zealand because it requires investments in sensitive land or a significant business asset (as defined in the OIA).
20. That investment may also be subject to a national interest or national security and public order risk assessment if:
 - a. There is investment by an overseas person in a GBSI business that involves dual-use technology. Dual-use technology is defined in the OIA as goods listed in the strategic goods list and any technology which could pose a significant risk to national security and public order and is within a class of technology set out in regulations; or,
 - b. The investment involves a non-New Zealand government investor who has a 25% or more ownership and control interest; or,
 - c. The Minister of Finance decides to 'call in' the transaction to assess if there are reasonable grounds to believe that the proposed investment could pose risks to New Zealand's national security or public order or have outcomes that would be significantly inconsistent with or could hinder delivery of other Government priorities.
21. Although this will capture some GBSI, gaps still remain:
 - a. While some GBSI is included on the strategic goods list, not all types of GBSI are covered.
 - b. The OIA only applies to overseas investments, so it will not capture overseas persons who have responsibility for operating GBSI that they do not own.
 - c. The OIA will not cover services provided to foreign customers or collaborators by New Zealand owned and operated GBSI e.g., customers of a commercial GBSI service.

Non-regulatory measures are used where there are regulatory gaps

22. We lack regulatory levers to detect and make a risk assessment of all GBSI activity that could give rise to national interest and national security risks. Over the past few years, we have identified and managed these risks by relying on government relationships with GBSI operators, through:
 - a. GBSI providers coming to relevant agencies with information on approaches by potential customers or collaborators that could pose risks.
 - b. Agencies using this information to undertake a risk assessment and make a recommendation to GBSI operators about the best course of action.
23. This process relies on the government maintaining relationships with New Zealand entities (e.g., commercial GBSI operators, Crown Research Institutes, universities and local government) and the goodwill of these operators to take advice provided by the government to reject approaches by high-risk foreign actors

Counterfactual - expected development of the status quo if no action is taken

Non-regulatory measures to manage risk are becoming unsustainable on their own due to increasing GBSI activity

24. [REDACTED] National security or defence [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
25. A number of factors could create challenges for continuing to rely primarily on non-regulatory measures, particularly relying on relationships with GBSI operators:
- a. Increasing global space activity, coupled with the desirability of New Zealand as a location for hosting GBSI, is expected to result in increased GBSI activity in New Zealand. This will likely lead to more activity outside of host organisations the government has a relationship with, limiting the government's ability to manage risks through non-regulatory measures.
 - b. There may be GBSI operators that the government does not have a relationship with, either now (operators we are unaware of currently) or in the future.
 - c. [REDACTED] National security or defence [REDACTED]
[REDACTED]
[REDACTED]
 - d. Technology development will make some types of GBSI more easily accessible than they have previously been, which could lead to more GBSI being established in New Zealand.
 - e. Where there are gaps in coverage by the regimes noted above, there are no regulatory levers to stop New Zealand-sited GBSI from being used in ways that would be contrary to New Zealand's interests, even if this activity was discovered.
26. In the absence of a regulatory regime to support the deterrence, detection and denial of high-risk GBSI activity, we expect some of the risks posed by GBSI to our national interest and national security, outlined above, will go unmanaged.
27. With risks going unmanaged, New Zealand could inadvertently allow a foreign government or entity, that does not share our values, to install or use GBSI equipment in New Zealand with a military or intelligence function. This could have serious consequences for New Zealand's sovereignty, national security and international reputation.

Relevant government decisions

Cabinet has agreed to the development of a regulatory regime to manage GBSI risks

28. In December 2022, Cabinet agreed to the following principles to inform the design of a GBSI regulatory regime [ERS-22-MIN-0057 refers]:
- a. Capture GBSI that creates a significant risk to New Zealand's national security and national interest.
 - b. Mitigate risk related to foreign military and security beneficiaries of GBSI located in New Zealand.

RESTRICTED

- c. Complement existing regulatory and non-regulatory measures (e.g., Radiocommunications Act, Overseas Investment Act, MBIE's relationships with commercial providers and universities).
 - d. Impose minimal costs on the regulated entities and on agencies involved in administering the regime while providing timely and comprehensive information to inform decision making.
 - e. Remain durable with regard to rapidly changing technologies.
 - f. Provide a sufficient level of certainty, predictability and transparency to regulated entities.
29. In July 2024, Cabinet agreed in principle to the following outcomes sought by introducing a new regime for regulating GBSI, in line with the aim to capture significant GBSI risks through regulation [ECO-24-MIN-0115 refers]:
- a. Preventing the operation of GBSI contrary to New Zealand's national security and national interests.
 - b. Ensuring the security of GBSI operations in New Zealand.
 - c. Addressing gaps that exist within the current regulatory regimes.
30. Cabinet also agreed that a regulatory regime for GBSI will be established under the Outer Space and High-altitude Activities Act 2017 (the OSHAA).
31. The OSHAA currently regulates launches into outer space, launch facilities, space payloads and high-altitude activities. It includes national interest and national security provisions, amongst other requirements.

Managing GBSI risks aligns with New Zealand's National Security Strategy and the countering foreign interference work programme

32. The National Security Strategy, published in 2023, describes the country's security outlook and sets out the 12 core issues that directly impact New Zealand's national security interests. Foreign interference and espionage, and space security are both included as core issues.
33. The Strategy prioritises acting early to prevent national security threats and build resilience by taking a proactive approach to anticipating and identifying threats.
34. The government is also undertaking a 'countering foreign interference' work program to build domestic resilience to the risks of foreign interference, coordinated by the Department of Prime Minister and Cabinet. The work seeks to enhance New Zealand's security through a combination of:
- a. boosting awareness and capability in entities that face foreign interference risks
 - b. stronger policy and regulatory settings
 - c. promoting greater transparency of foreign state activity.
35. These initiatives recognise that a combination of regulatory and non-regulatory responses are helpful for addressing national security risks.

International context

36. [REDACTED] National security or defence [REDACTED]
[REDACTED]
[REDACTED]
37. Like New Zealand, many countries regulate radiofrequency based GBSI to manage interference. However, New Zealand is the only country from the Five Eyes that does not regulate receive-only space-to-Earth communications.
38. [REDACTED] National security or defence [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
39. However, as GBSI risks continue to grow, some likeminded countries, [REDACTED] National security or defence are contemplating how to better manage these risks and may decide to implement GBSI regulatory regimes in the future.
40. Other countries have existing national security legislation that, while not specific to GBSI, would provide regulatory levers to prevent high-risk GBSI activity from taking place in their countries, negating the need for a GBSI-specific regulatory regime for managing risks.
41. [REDACTED] National security or defence [REDACTED]
[REDACTED]
42. Officials will continue to engage with [REDACTED] National security or defence [REDACTED] on the development of policy and regulation to manage GBSI risks.

What is the policy problem or opportunity?

Policy problem

43. GBSI could be used to support the aspirations of countries that do not share New Zealand's values and interests. If GBSI was to be established or used in New Zealand for this purpose, it could be harmful to New Zealand's national security and broader national interests, [REDACTED] National security or defence [REDACTED].
44. The government primarily relies on the non-regulatory measures described above to manage GBSI risks due to regulatory gaps (Table 1). However, due to growing interest in New Zealand as a location for hosting GBSI, officials no longer have confidence that these non-regulatory measures will be sufficient for managing the risks posed by GBSI.

Scale and scope of the problem

45. [REDACTED] National security or defence [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
46. While it is important for a GBSI regime to manage these risks, there is a challenge in designing a regime to identify a small number of high-risk GBSI activities while imposing minimal costs on GBSI activity that poses low or no risk. This is because there are a large number of types of equipment that could be considered GBSI, many potential uses for GBSI, and a number of GBSI users, as outlined below.

RESTRICTED

Types of infrastructure

47. Radio GBSI includes:

- a. Radio telescopes
- b. Space object tracking radars
- c. Global Navigation Satellite Systems (e.g., GPS) receivers
- d. Satellite phones
- e. Domestic satellite broadband installations
- f. Satellite communications gateways
- g. Domestic satellite dishes for household television
- h. Global Navigation Satellite Systems (GNSS) calibration antennas
- i. Some telecommunications networks.

48. Optical GBSI includes:

- a. Laser terminals
- b. Optical telescopes.

GBSI use cases

49. Both radio and optical GBSI can support a wide range of use cases:

- a. Telemetry, tracking and control of spacecraft.
- b. Space surveillance and identification of spacecraft.
- c. Satellite data reception, including but not limited to:
 - i. Commercial telecommunications activity
 - ii. Private telecommunications activity
 - iii. Provision of broadband and television
 - iv. Emergency and safety of life services
 - v. Position, navigation and timing.
- d. Radio and optical astronomy.

GBSI users

50. There is also a wide range of potential GBSI users in New Zealand:

- a. Commercial 'GBSI as service' operators
- b. Telecommunications companies
- c. Private telecommunications network operators
- d. General public
- e. Hobby astronomers
- f. Academic tertiary institutes
- g. Crown Research Institutes

- h. Private research institutes
 - i. New Zealand government
 - j. Foreign governments.
51. If the regulatory regime is extended too broadly, it could capture low risk equipment, activity (e.g., optical telescopes for amateur astronomy, satellite phone usage) and users (e.g., hobbyists and the general public). This would increase regulatory costs considerably.
52. Conversely, a regime scoped too narrowly may lead to high-risk GBSI equipment, activity or users not being captured by the regime, particularly in the future as GBSI technology develops.

What objectives are sought in relation to the policy problem?

53. The objectives for a GBSI regulatory regime are based on the principles previously agreed by Cabinet:
- a. Mitigate the risk GBSI poses to New Zealand's national security and national interests by providing means to deter, detect and deny GBSI activity that presents the highest potential harm to New Zealand's interests, including national security.
 - b. Complement (rather than duplicate) existing regulatory and non-regulatory measures that apply to GBSI (e.g., Radiocommunications Act, Overseas Investment Act, MBIE's relationships with commercial providers and universities).
 - c. Impose minimal costs on the regulated entities and on agencies involved in administering the regime while providing adequate information to inform decision making.
 - d. Remain durable and flexible to keep pace with rapidly changing technologies.
 - e. Provide a sufficient level of certainty, predictability and transparency to regulated

What consultation has been undertaken?

54. MBIE approached 21 known GBSI operators to provide them with the opportunity to give feedback on the scope and design of a GBSI regulatory regime.
55. This included an initial discussion with GBSI operators (those that responded) on the scope of the regime. Following this, the same GBSI operators were provided with a consultation document which set out options for the design of the regulatory regime for feedback.
56. Three GBSI operators responded to the consultation document, which made it challenging to get a consensus view across GBSI operators. Two of the operators that responded supported an authorisation regime for GBSI, while one operator felt the choice of regime design would not be consequential as they would expect to receive a high level of scrutiny under any regime due to offering GBSI services to foreign third parties.

RESTRICTED

57. Consulted stakeholders highlighted the importance of a flexible regulatory regime, a regime that is not overly burdensome for GBSI operators and a regime that is scoped appropriately to ensure only high-risk GBSI is captured.

Section 2: Assessing options to address the policy problem

What criteria will be used to compare options to the status quo?

58. Based on the objectives above, the following criteria has been used to compare policy options:
- a. *Effectiveness* – the regime should enable deterrence, detection and denial of GBSI activity that presents the highest potential harm to New Zealand's interests.
 - b. *Cost* – the regime should not impose unnecessary compliance costs on the regulated entities and agencies involved in administering the regime.
 - c. *Certainty and predictability* – the regime should be easily understood by applicants and agencies responsible for its implementation.
 - d. *Flexibility* – the regime should provide enough flexibility to keep pace with technological advancement.

What scope will options be considered within?

Previous Cabinet decisions

Cabinet has agreed to the development of regulatory measures for managing risks

59. Cabinet has agreed to the development of legislative measures to manage GBSI risks due to non-regulatory measures no longer being adequate for managing national interest and national security risks, therefore, non-regulatory measures are not considered in scope. Relevant Cabinet decisions are summarised in paragraphs 28 – 30.

Protective security and due diligence requirements have already been agreed

60. Subject to stakeholder consultation, Cabinet has agreed that GBSI operators would be required to have due diligence systems in place to know who they are providing services to (e.g., customers or collaborators) and the purpose of their customers' or collaborators' GBSI operations. The regulator would not make an upfront assessment of the GBSI operators' customers to determine whether they pose any significant risks.
61. A limitation of this approach, however, is that primary responsibility for identifying and managing potential risks will sit with GBSI operators. Even with a best practice due diligence system, they may not identify sophisticated covert customers or collaborators that could give rise to risks. Non-regulatory measures, including intelligence reporting, regular engagement and strong relationships with the sector will need to continue to manage any residual risk.
62. Options three and four set out below include protective security and due diligence requirements, however, we did also explore an option without these requirements (option two below).

Cabinet has agreed that the regime will focus on regulatory gaps for significant risks

63. As noted in paragraph 24, Cabinet has agreed that the regulatory regime will only capture GBSI that poses significant risk to New Zealand's national security and national interest and will complement existing regulatory measures that apply to GBSI. This narrowed the scope of options to only those that filled regulatory gaps.

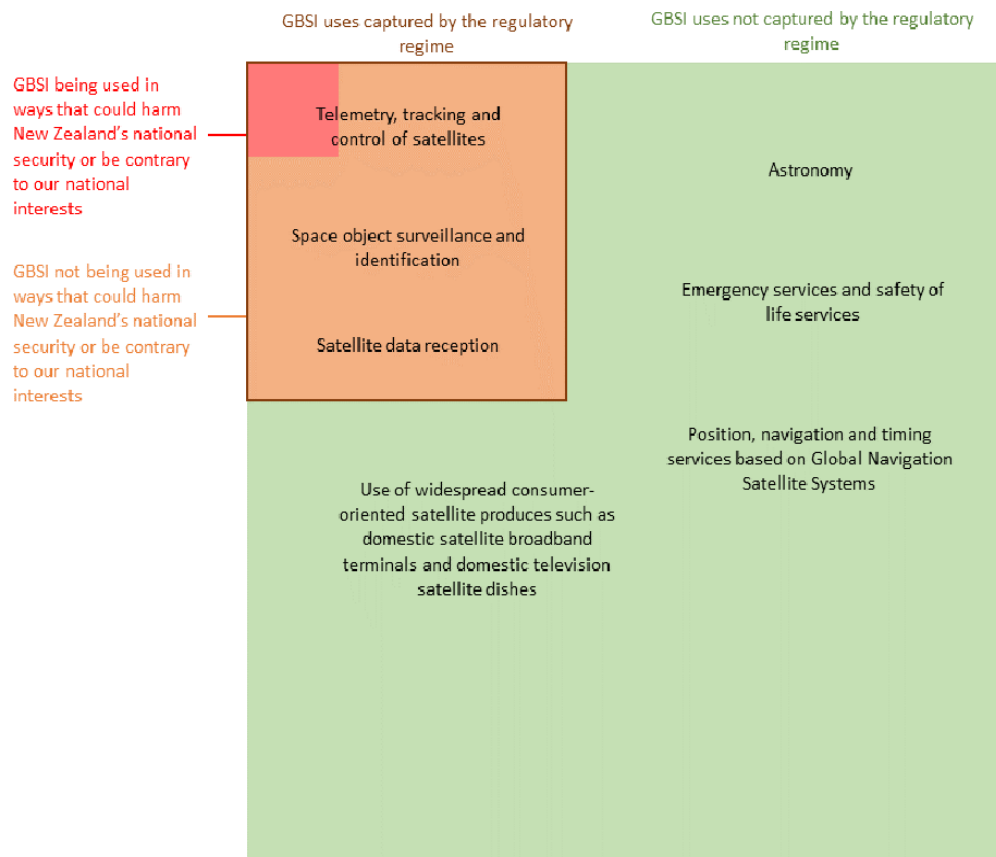
Regime scope

64. A GBSI regulatory regime needs to be appropriately scoped to capture GBSI activity that gives rise to significant risk, while to the extent possible, avoiding capturing GBSI activity that poses minimal or no risk. This requires decisions on what uses of GBSI and which entities to regulate. On the basis of Cabinet's decision to focus the regime on significant risks, we propose a regime that is narrowly scoped to focus on GBSI activities that can poses a significant risk (i.e. not regulating low-risk users or activities like hobby astronomy).
65. A more broadly scoped regime was considered and discarded due to imposing an unjustifiable regulatory cost on low-risk GBSI users and the regulator. On this basis, no further options analysis is provided for regime scope.
66. The GBSI regime should apply to the following GBSI uses:
- a. Telemetry, tracking and control (including capability that could degrade or disrupt satellite operations) of spacecraft (including, for example, geodetic infrastructure)¹.
 - b. Satellite data reception.
 - c. Space surveillance and identification of space objects.
67. GBSI uses that would not be captured by the regime are:
- a. Any infrastructure or other equipment of a type that is made or supplied primarily for personal, domestic, or household use (Including television satellite dishes, satellite and other mobile phones and internet access terminals).
 - b. Any infrastructure or other equipment of a type that is made or supplied primarily for the purposes of safety, navigation, calibration of measuring instruments, positioning, or timing and is not capable of sending information to a space object.
 - c. Emergency Locator Beacons.
 - d. Use of widespread consumer-oriented satellite products such as domestic satellite broadband terminals and domestic television satellite dishes.
68. Members of the general public that observe satellites as a hobby should be exempt from the regime.
69. With respect to which responsible entity to regulate, we consider that the GBSI regime should target GBSI operators, rather than owners or hosts. This is because operators are responsible for the GBSI activity undertaken and will interact directly with customers and collaborators. **National security or defence**
70. Operators are entities that manage, or make decisions on:
- a. The nature of activities that the GBSI will be used for, and;

¹ Satellite geodesy is the science of using satellites to measure and map the Earth's shape, gravity field, and orientation in space. It includes satellite navigation systems like the Global Positioning System

RESTRICTED

- b. If services are to be provided to a third party, whether to provide services, and;
- c. if the operator hosts a third party, whether or not to host that other party. The diagram below highlights that in capturing high-risk GBSI (represented by the red box), the dual use nature of these technologies means that low-risk GBSI uses will also be captured by the regime (represented by the orange box). Ideally, there should be minimal costs imposed on those operators that fall within the scope of the regime but are assessed to be undertaking low-risk activity.



71. The regime will apply to all in-scope GBSI use in New Zealand, including by GBSI established prior to the regulatory regime being established. National security or defence
72. Provision 6(2) in the OSHAA exempts the New Zealand Defence Force from having the OSHAA apply to it. We intend for this carve out to apply to the GBSI regulatory regime. The GBSI regime will not apply to the New Zealand Defence Force, or to any person or body [whether in New Zealand or overseas] that assists or provides services to or is working in a relevant partnership with the New Zealand Defence Force.
73. We also propose that the GBSI regime does not apply to the intelligence and security agencies when they are performing their statutory functions, or to any person or body [whether in New Zealand or overseas] that assists or provides services to the intelligence and security agencies in relation to the performance of the agencies' functions.

Regulatory decision maker

74. In line with the OSHAA, MBIE will serve as the regulator, with regulatory decisions to be made at Ministerial level (the Minister for Space is currently the decision maker).

What options are being considered?

Regime design

75. Three options were considered for the design of the GBSI regime alongside the counterfactual:
- a. *Option one* – Counterfactual.
 - b. *Option two* – A notification and call-in regime for GBSI.
 - c. *Option three* – An authorisation regime for GBSI.
 - d. *Option four* – A licensing regime for GBSI.
76. As described above, two rounds of targeted stakeholder consultation with GBSI operators were undertaken in 2024, which included consultation on the policy options including the scope and design and of the regulatory regime.
77. All options are designed to be complemented by the use of ongoing non-regulatory measures, consistent with the past management of GBSI risks in New Zealand.

Option one – Counterfactual

78. Under this option there would be continued reliance on non-regulatory measures for managing risks posed by GBSI to New Zealand's national security and national interests. This is expected to be ineffective over time due to a predicted increase in GBSI activity in New Zealand, as outlined in paragraphs 21 – 23.
79. Existing regulatory gaps will remain and, in some cases where no other laws apply, foreign entities will be able to lawfully use GBSI in New Zealand in ways that could harm or undermine New Zealand's security or national interest.
80. The likely ineffectiveness of continued reliance on non-regulatory measures for managing GBSI risks means it does not meet the policy objectives outlined above.
81. This option is not feasible for effectively managing risks from GBSI, nor does it provide certainty or predictability for GBSI operators given the ad-hoc nature of some of the non-regulatory measures applied. It is also not in line with Cabinet's direction to develop a regulatory regime for GBSI.

Option two – Introduce a notification and call-in regime for GBSI

Description of option two

82. This option is similar to the notification and call-in regime implemented under the Overseas Investment Act. Entities or individuals intending to undertake GBSI activity that is in-scope of the regulatory regime would be required to notify the regulator of their proposed activity.
83. The regulator would have the power to "call in" the proposal for further assessment and decline the proposal if it was determined to be contrary to the national interest (including for national security reasons).

RESTRICTED

84. If the proposal was not called in within a specified timeframe, it could proceed. If a called in proposal was not declined within a specified timeframe, it could also proceed.
85. This option would not create ongoing monitoring requirements for the regulator, such as inspections or assessments or ongoing reporting requirements for regulated entities. However, regulated entities would need to update the regulator should any of the details provided to the regulator change, e.g., ownership change for a commercial GBSI service provider.
86. This option would not require GBSI operators to implement protective security and due diligence systems for vetting customers or collaborators as creating these obligations without the means to monitor them would not be advisable.
87. If the regulator determined through information supplied by the GBSI operator or gathered from other sources that a GBSI operator was carrying out activity that was contrary to the national interest (including security interests), it could provide advice to the decision-making Minister that the notification should be withdrawn, which would prevent the GBSI activity from legally continuing. Without an ongoing monitoring requirement through the regulatory system, it is likely that this decision would need to be made on the basis of information gathered through non-regulatory measures (e.g., intelligence).

Analysis of option two

88. As the least stringent of the options considered (aside from the counterfactual), this option imposes the least regulatory cost to both regulated entities and the regulator, while still providing the government with a list of in-scope GBSI operators. This would help with targeting GBSI operators for the ongoing implementation of non-regulatory measures.
89. Although this option represents a relatively light touch regulatory regime, we still expect it would have some impact as a deterrent for the type of GBSI activities we are looking to prevent from occurring in New Zealand.
90. Without ongoing monitoring obligations, it would be challenging for this option to provide effective risk management over time. GBSI operators could gain new customers or collaborators that would not be known when they notified the regulator of their activities, and this could change the risk profile of a GBSI operation. However, the regulatory decision maker could prevent GBSI activity from continuing at any time, which is an improvement over the counterfactual.
91. We do not consider that option two would be effective enough at managing GBSI risks particularly over time.

Option three – Introduce an authorisation regime for GBSI

Description of option three

92. Entities or individuals intending to undertake GBSI activity that is in-scope of the regulatory regime would be required to be authorised to control, operate or provide GBSI services. An authorisation regime would require GBSI operators undertaking in-scope GBSI activities to:
 - a. authorise – requiring provision of information on who owns the GBSI, the type of GBSI and what it is used for, what services (if any) are provided to third parties, whether services are provided to foreign entities

RESTRICTED

- b. have an adequate due diligence system in place for understanding who their customers or collaborators are, based on guidance supplied by the regulator
 - c. have a protective security plan in place for managing personnel, physical and information security, based on guidance supplied by the regulator
 - d. provide information on customers or collaborators to the regulator via regular reporting
 - e. Notify the regulator of any breach of personnel, physical, or information security or of any decision to discontinue the provision of services to an existing customer or collaborator
 - f. update their authorisation if there is a change in any information provided
 - g. confirm once a year that the information provided in the authorisation is current.
93. The regulator would not make an upfront assessment of the authorisation beyond ensuring the declared requirements have been met, the required information has been provided, and that the GBSI use is in-scope of the regulatory regime. Instead, the regulator would recommend that the decision-making Minister grant authorisation if the applicant provided all required information and declared that it had the required protective security and customer due diligence systems in place.
94. The regulator would provide guidance to regulated entities on protective security and customer due diligence requirements. This guidance would be largely based on the government's existing published guidance in these areas, e.g., the New Zealand Security Intelligence Service's (NZSIS) publication *Secure Innovation: Security Advice for Emerging Technology Companies*, with tailoring for GBSI applications.
95. The decision-making Minister would be able to suspend, withdraw or impose conditions on a GBSI authorisation on national interest or national security grounds. Conditions could include preventing an authorised entity from providing GBSI services to a specified third-party. To inform decisions on an authorisation, the regulator may:
- a. undertake inspections and assess authorised operators' due diligence and protective security systems
 - b. consider any other information that has been made available by other government agencies (e.g., information provided by security agencies), the registrant, or that is in the public domain
 - c. consider any instances of non-compliance with regulatory requirements, including conditions imposed on an authorisation.
96. To support this, the regulator would be able to share all information provided by a authorised GBSI operator to the regulator with security agencies, and other government agencies where relevant (e.g., where there are national interest concerns that relate to New Zealand's international reputation, the regulator may share information with and seek advice from MFAT).
97. Additionally, a disposal order will allow the Minister responsible for space to direct a non-compliant operator to divest themselves in their rights/interest to the infrastructure in cases of national interest (including national security) risks. If the operator still does not comply, the enforcement officers may be able to apply to a district court to for forfeiture of assets.

Analysis of option three

98. Ongoing monitoring requirements (including assessment powers, requirement that GBSI operators provide regular reporting on partners they provide services to e.g., customers) mean that an authorisation regime is more effective at managing changing risks over time than option two – a notification and call-in regime.
99. Option three imposes a higher cost on regulated entities than option two, through greater up front information requirements, ongoing reporting requirements and requirements to implement protective security plans and implement customer due diligence system systems. It also imposes a higher cost than option two on the regulator due to ongoing monitoring requirements.
100. The benefit of these additional requirements, including ongoing monitoring, is that an authorisation regime will be more effective at managing changing risks over time than option two – a notification and call-in regime.
101. A limitation of an authorisation regime for risk management, is that it does not include an upfront assessment of whether the GBSI activity can proceed. Non-regulatory measures would need to continue to support identification of high-risk activity, along with assessments and regular reporting requirements. Not including an upfront assessment of GBSI activity decreases the cost imposed on regulated entities and the regulator.

Option four – Introduce a licensing regime for GBSI

Description of option four

102. A licensing regime for GBSI would require operators of in-scope GBSI activities to apply for authorisation to operate GBSI in New Zealand.
103. The decision-making Minister would need to be satisfied that certain threshold tests were met, including that the proposed GBSI use must not be contrary to New Zealand's national interest (including national security).
104. A licensing regime would require GBSI operators undertaking in-scope GBSI activities to:
 - a. apply for a licence, with requirements to supply enough information for the regulator to provide advice to the decision maker on whether or not the activity is contrary to the national interest
 - b. have an adequate due diligence system in place for understanding who their customers or collaborators are, based on guidance supplied by the regulator
 - c. have a protective security plan in place for managing personnel, physical and information security, based on guidance supplied by the regulator
 - d. provide a list of existing customers or collaborators to the regulator, with quarterly reporting of new customers and reporting of third parties the operator opted not to work with following due diligence
 - e. notify the regulator of any breach of personnel, physical, or information security or of any decision to discontinue the provision of services to an existing customer or collaborator
 - f. update the regulator if there is a change in any information provided

- g. confirm once a year that the information provided in the authorisation is current.
105. Unlike option three, under a licensing regime, the regulator would make an upfront assessment of whether or not the proposed GBSI activity should proceed or not, on the basis of national interest and national security considerations. This would include an assessment of the adequacy of a licence applicants protective security and due diligence systems.
106. As with option three, to inform regulatory decisions the regulator may:
- a. undertake inspections and assessments of authorised operators' due diligence and protective security systems
 - b. consider any other information that has been made available by other government agencies (e.g., information provided by security agencies), the licence applicant, or that is in the public domain.
107. The regulatory decision maker would decide whether to grant or decline a licence application and could impose conditions on a licence, either when the application is initially granted or at any point that it is necessary. The regulatory decision maker could also suspend or revoke a licence at any time on national interest or national security grounds.
108. The regulator could also place conditions on the licence to assist with mitigating any risks identified during the assessment of the licence application.

Analysis of option four

109. Compared to options two and three, a licensing regime imposes the highest costs on the regulator as an upfront assessment would be required for all licence applications. It would also impose the highest cost on regulated entities with the highest up front information requirements and an assessment period before activity can take place, beyond that all other obligations on regulated entities are the same for both options three and four.
110. As the most stringent option with an upfront assessment requirement, a licensing regime would provide the highest level of confidence that GBSI risks are being managed.
111. Experience with regulating space activities under the Outer Space and High-altitude Activities Act to date suggests that the existence of a regulatory regime for GBSI will likely be a deterrent for the types of GBSI activity the regime is looking to prevent.
112.

National security or defence

 we do not consider that the costs imposed by a licensing regime would be proportionate to the risks.

RESTRICTED

Comparison of the functionality of regulatory design options

	Option two: notification and call-in	Option three: authorisation	Option four: licensing
Record of GBSI operators	✓	✓	✓
Imposes protective security and due diligence requirements	X	✓	✓
Ongoing monitoring	X	✓	✓
Upfront assurance before activity takes place	X	X	✓

RESTRICTED

How do the options compare to the status quo/counterfactual?

	Option one – counterfactual	Option two – notification and call-in regime	Option three – authorisation regime	Option four – licensing
Effectiveness	<p style="text-align: center;">0</p> <p>This option is not expected to be effective at managing ongoing GBSI risks. It provides no legal basis for preventing the establishment or use of GBSI in ways that would be contrary to New Zealand’s national interest (including national security).</p>	<p style="text-align: center;">+</p> <p>This option allows for improved risk management over the counterfactual, as even basic reporting and transparency requirements will be enough to deter some high-risk GBSI users. However, without ongoing monitoring, there is limited ability to detect or deny high-risk GBSI use, particularly where risk may change or increase over time. A lack of due diligence and protective security requirements also limits effectiveness.</p> <p>This is a light touch approach to regulating GBSI risks, with limited upfront information requirements. This option still allows the regulator to call in any GBSI use that is deemed to be high-risk, allowing the most regulatory scrutiny to be placed where there is the highest risk.</p>	<p style="text-align: center;">++</p> <p>This option has many of the benefits of option two, with low upfront information requirements and immediate authorisation where regulatory requirements have been declared to have been met. The ongoing monitoring requirements, including the option to assess authorised GBSI operators, allows the regulator to focus its oversight over operators that could present the most risk.</p>	<p style="text-align: center;">+++</p> <p>A licensing regime would allow for the most effective risk management as it involves the collection of more upfront information from GBSI operators and the assessment of all applicants to the regulatory regime. It also provides the ongoing risk management benefits of option three.</p>

RESTRICTED

	Option one – counterfactual	Option two – notification and call-in regime	Option three – authorisation regime	Option four – licensing
Cost	<p>0</p> <p>There is not currently a regulatory regime to impose compliance costs on regulated entities and agencies involved administering the regime, however, non-regulatory measures can be resource intensive to implement.</p>	<p>-</p> <p>A notification and call-in regime would impose minimal additional cost for regulated entities and the regulator compared to the status quo. There is no requirement for GBSI operators to undertake due diligence on third parties being provided GBSI services and no ongoing monitoring requirements for the regulator.</p>	<p>--</p> <p>An authorisation regime imposes costs on to regulated entities through the requirement to be authorised, undertake third-party due diligence, implement protective security requirements and provide regular lists of customers and collaborators. The regulator needs to undertake ongoing monitoring including inspections and assessments, supported by intelligence agencies.</p>	<p>---</p> <p>A licensing regime imposes the highest cost onto regulated entities with the biggest upfront information requirement. It is also the most resource intensive option for the regulator. Assessing each licence application, including the adequacy of due diligence and protective security systems add considerable cost over the other options considered.</p>
Certain & predictable	<p>0</p> <p>Non-regulatory measures do not offer certainty or predictability for GBSI operators, as they do not provide clear and consistent requirements.</p>	<p>++</p> <p>Regulated entities will have a clear set of requirements to follow, which provides added certainty over the counterfactual option. The call-in feature may add some unpredictability to the regime.</p>	<p>++</p> <p>Regulated entities will have a clear set of requirements to follow, and authorisation will be quick assuming a registrant declares that requirements are met, and no initial concerns are raised by security agencies. Regulated entities will know the powers the regulator has and the ongoing reporting requirements.</p>	<p>++</p> <p>Regulated entities will have a clear set of requirements to follow to obtain a licence. As with option three, regulated entities will know the powers the regulators have and the ongoing reporting requirements.</p>

RESTRICTED

	Option one – counterfactual	Option two – notification and call-in regime	Option three – authorisation regime	Option four – licensing
Flexible	<p style="text-align: center;">0</p> <p>Non-regulatory measures are not codified into legislation, which provides flexibility to keep pace with technological advancements, however, there is limited flexibility on a course of action where risks are identified.</p>	<p style="text-align: center;">-</p> <p>The one-off nature of GBSI notifications under this option may make it challenging to respond to changing risks over time. It only regulates at a particular point in time. The status quo allows for better on-going management of changing risks.</p>	<p style="text-align: center;">++</p> <p>Ongoing monitoring provides some flexibility to deal with changing risk profiles or circumstances over time and the option to add conditions to an authorisation provides flexibility to manage new risks that emerge.</p>	<p style="text-align: center;">++</p> <p>A licensing regime would allow the regulator to impose licence conditions following a risk assessment for each licence which, alongside the option to include inspections and assessments of GBSI operators, would provide flexibility in managing evolving risks.</p>
Overall assessment	0	1	4	4

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

Authorisation regime for GBSI

113. Option three - an authorisation regime for GBSI is preferred. It provides flexibility to manage changing risks over time and provides adequate certainty to the regulator and regulated entities.
114. While an authorisation regime provides more effective risk management than a notification and call-in regime, it is less effective at managing risks than a licensing regime as outlined in the table above.
115. The reduction in the effectiveness of risk management from a licensing regime to an authorisation regime is traded off for a reduction in the regulatory costs imposed on regulated entities and the regulator that an authorisation regime offers over a licensing regime.

116.

National security or defence

.

117. While we cannot predict the number of these attempts that may occur in the future, we expect that the existence of a GBSI regulatory regime will act as a deterrent.

Overview of a GBSI authorisation regime

118. GBSI operators, whether based primarily in New Zealand or elsewhere, must authorise to operate a ground station within New Zealand's territory.
119. An assessment of an authorised operator could be triggered by:
- a. the number and nature of customers or collaborators (e.g., an operator providing a GBSI service to a large number of customers, or customers of concern)
 - b. an update to authorisation information (e.g., a change of ownership)
 - c. a breach of physical, personnel, or information security
 - d. information of concern supplied by security agencies (e.g., a customer operating who otherwise should have been rejected by an adequate due diligence system)
 - e. any other information the regulator has, including that supplied by any other agency, that suggests there are unmanaged national security/national interest risks that an operator should be reasonably expected to manage.
120. An assessment may also be undertaken without a specific risk-based trigger.
121. Offences will be modelled off existing offences that appear in the Outer space High-altitude Activities Act (OSHAA) to include that it will be:
- a. An offence to carry out in-scope GBSI activity without being authorised
 - b. An offence to not comply with an assessment
 - c. An offence to not comply with conditions on an authorisation

RESTRICTED

- d. An offence to provide false or misleading information on an authorisation or during the course of an assessment or inspection
 - e. An offence not to comply with a direction given by an enforcement officer.
122. The OSHAA contains existing offences for providing false or misleading information to an enforcement officer that will apply to the GBSI regime, with penalties of up to \$10,000 for an individual or up to \$50,000 for a body corporate. Enforcement officers will carry out assessments and inspections.
123. In the case of failing to follow a direction, the individual may incur a \$5000 fine while a body corporate may incur a \$50,000 fine. These new penalties reflect the level of seriousness in failing to comply with a direction.
124. Enforcement Officers will be appointed by the chief executive of MBIE using the current powers set out in the OSHAA.
125. In line with Section 60 of the OSHAA, in the case of noncompliance with the GBSI regime, Enforcement Officers retain the power to enter the premises and seize equipment and data.
126. The Minister will have the ability to give a disposal order to operators in the case of noncompliance. This power will be available if the Minister believes that the person's operation of the GBSI for a regulated activity poses a national interest (including national security) risk that cannot adequately be managed by imposing GBSI activity authorisation conditions, removing the person's authorisation, or taking enforcement action under the OSHAA.
127. If an operator fails to comply with the disposal order, which will set out the timeliness and way in which their interests must be disposed of, an enforcement officer or a constable can apply to the District Court for a forfeiture order to vest the interest or right that was the subject of the disposal order in the Crown.
128. The regime also introduces a power for the Minister to direct power or internet companies to stop providing services to a GBSI. This inclusion is to ensure that GBSI that continues operating after a disposal order is issued can be prevented from doing so.
129. Penalties will be in line with existing penalties in the OSHAA, which include fines and terms of imprisonment.

RESTRICTED

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups (identify)	Comment <i>nature of cost or benefit (eg, ongoing, one-off), evidence and assumption (eg, compliance rates), risks.</i>	Impact <i>\$m present value where appropriate, for monetised impacts; high, medium or low for non-monetised impacts.</i>	Evidence Certainty <i>High, medium, or low, and explain reasoning in comment column.</i>
Additional costs of the preferred option compared to taking no action			
Regulated entities	One off administration cost to apply for authorisation, though not expected to be particularly burdensome. Regulated entities will be expected to implement and maintain protective security and due diligence systems which will have ongoing associated costs. Regular reporting requirements add ongoing administrative burden.	High	Medium
Regulators	Two additional FTE to manage GBSI authorisations and ongoing monitoring, along with costs for monitoring and compliance. Authorisation numbers are difficult to predict, so more staff may be needed if estimates are inaccurate.	Confidential advice to Government	Low
Total monetised costs		Confidential advice to Government	
Non-monetised costs		Medium	

RESTRICTED

Additional benefits of the preferred option compared to taking no action			
New Zealand	Managing the risk that GBSI could be used to harm New Zealand's national security or be used in ways that are contrary to New Zealand's national interest will have the ongoing benefit of making New Zealand safer.	High	Medium
Regulated entities	Protective security and due diligence requirements will likely have ongoing benefits for GBSI operators beyond regulatory compliance, e.g., protecting their business, mitigating reputational risks, protecting intellectual property, protecting physical property from theft or damage. The regime also provides certainty about how to identify and manage risks. Less reliance on non-regulatory measures and a better understanding of how to apply non-regulatory measures will lessen the burden on agencies implementing these measures and provide access to a broader suite of tools to respond to risks.	Medium	Medium
Agencies involved in implementing non-regulatory measures	Less reliance on non-regulatory measures and a better sense of how best to apply non-regulatory measures will lead to an ongoing reduction in burden on agencies implementing these measures and provide access to a broader suite of tools to respond to risks.	Medium	High

RESTRICTED

Wider government	<p>Managing the risks from that GBSI in New Zealand that could be used to harm New Zealand's interests <small>National security or defence</small></p> <p>will likely enhance New Zealand's reputation as a trusted space partner and support the international space relationships we rely on.</p>	Medium	Low
Partner countries	<p>The GBSI regime will <small>National security or defence</small></p> <p>while having a deterrent effect on foreign actors seeking to use GBSI for purposes contrary to New Zealand's interests.</p> <p><small>National security or defence</small></p>	Medium	Low
Non-monetised benefits		Medium	

130. By comparison, a licencing regime would Confidential advice to Government due to the requirement for more staff to operate the regime and the heightened compliance costs associated with conducting both upfront checks and assessments.

Section 3: Delivering an option

How will the proposal be implemented?

131. The regulatory regime for GBSI will be introduced through an amendment to the Outer Space and High-altitude Activities Act 2017 (OSHAA). The Space Regulatory Systems team within the Ministry of Business, Innovation and Employment will be responsible for administering the regime.
132. In line with the approach taken for other activities regulated by the OSHAA, the Government Communications Security Bureau and New Zealand Security Intelligence Service will provide advice on national security risks.
133. The GBSI regulatory regime will come into effect in 2025. The intention to regulate GBSI was announced publicly by the Minister for Space in December 2024.
134. Implementation of the regime will be supported by published guidance for GBSI operators and information provided through ongoing relationships with GBSI operators.
135. The regime will apply to all in-scope GBSI use in New Zealand, including by GBSI established prior to the regulatory regime being established.
136. There will be a transition period following commencement that will allow in-scope GBSI operators time to meet regulatory requirements before applying for authorisation.
137.

National security or defence

power will be enacted making it possible to stop GBSI activity that poses a risk to New Zealand's national security.

Resourcing

138. The regulatory regime will apply to both new and existing in-scope GBSI activities in New Zealand. It is difficult to accurately predict the number of authorisations that the regulator will receive, however, we estimate approximately 10-15 initial authorisations for existing GBSI, with fewer authorisations over time as new GBSI is established.
139. To accommodate this further resource will be needed for MBIE to administer the GBSI regime, to support two FTE staff and other costs associated with implementation, particularly to support inspection and assessment of GBSI operations.
140.









Confidential advice to Government
141.

Confidential advice to Government

Interface with other regulatory regimes

142. As noted above, in some cases GBSI may be captured by the GBSI regulatory regime and another regime, e.g., the Overseas Investment Act and the Radiocommunications Act. The GBSI regime will be designed in such a way as to reduce duplication between regimes, including allowing for information sharing arrangements between and within agencies.

International engagement

143.  National security or defence 







How will the proposal be monitored, evaluated, and reviewed?

144. A GBSI regulatory regime is relatively novel internationally, and we want to evaluate and review the regime to ensure it strikes the right balance between costs and benefits of the regime.
145. The OSHAA includes a provision for a review of the operation and effectiveness of the Act, three years from commencement. We propose a similar provision be included for a review of the operation and effectiveness of the GBSI regulatory regime, two years after commencement, as we expect this will be an adequate length of time to make a determination about the regime's effectiveness.
146. MBIE routinely seeks post permitting feedback from OSHAA payload permit applicants. A similar approach would be taken with a GBSI authorisation applicant.