

Trusted Business

Protective security guidance for the New Zealand business sector



PSR

Protective Security
Requirements



Te Kāwanatanga o Aotearoa
New Zealand Government



Contents

Protecting your business	4
Business in New Zealand	5
What is espionage and foreign interference?	6
Why could you or your business be at risk?	8
Specific aspects of your business that could attract foreign interest	10
How espionage and foreign interference can affect your business	12
Examples of how espionage and foreign interference may present in business	14
Minority ownership, but control over your business	15
Access to your business, personnel, and systems	16
Managing espionage and foreign interference risks	21
Do your due diligence	22
Build your security culture	22
Use legal frameworks	24
Overseas Investment Act	28
Utilise the Protective Security Requirements (PSR)	30
Resources	32

Protecting your business

This guide is designed to help the business sector in Aotearoa New Zealand get the best out of international business relationships while protecting intellectual property (IP), sensitive research, data, information, and employees.

Ensuring the integrity of New Zealand business is vital to the ongoing success of domestic and international business, trade, and export.

This guide:

- outlines the potential risks to New Zealand business from espionage and foreign interference
- helps businesses, government, and industry partners to have confidence in international collaboration and make informed decisions about potential risks
- explains how to protect your business from espionage and foreign interference.

Protective security is the responsibility of everyone in an organisation including leaders, employees, contractors, and temporary staff. Strengthening the overall security capability and culture of your organisation will enable it to function effectively and better manage a broad range of risks.

Business in New Zealand

New Zealand is a global trading nation, and the business sector attracts customers and partnerships from around the world. A significant amount of economic success is derived from New Zealand's international business relationships and agreements:

- New Zealand has an open business sector that values the independence and innovation of individuals and businesses
- New Zealand welcomes international trade, investment, and business opportunities
- the New Zealand government actively supports building strong international relationships and removing barriers to trade and business.

There may be risks associated with international partnerships that businesses should identify and manage to prevent damage to reputation, loss of revenue, loss of IP, loss of markets, or harm to the national interests of New Zealand. National interests include economic prosperity and resilience, international relations, or broader policy settings and values.



When building trusted business connections, you need to understand if potential partners and relationships may be associated with:

- organisations from authoritarian or repressive regimes, which could take punitive measures in response to actual or perceived grievances
- countries that engage in espionage or foreign interference activities to benefit their national interests, at the expense of other countries.

What is espionage and foreign interference?


Espionage refers to various intelligence activities involving the clandestine collection of information, materials, or capability for the purpose of gaining an advantage over a rival.

Espionage can come from foreign states (state-sponsored espionage) or from non-government organisations (industrial espionage).

The New Zealand business sector may present opportunities for foreign states and organisations to collect data and information which is not otherwise publicly available. This may be used to interfere with the national and economic interests of New Zealand, or to further foreign interests.

Foreign states may also target New Zealand businesses as a way to target the supply chains of New Zealand's critical infrastructure, the economy, or government.

Industrial espionage is like state-sponsored espionage except it is undertaken for financial gain, such as to go to market with a new product before a competitor. An organisation may use similar methods to those used by states to target a business.



Foreign interference is an act by a foreign state, often acting through a proxy, which is intended to influence, disrupt, or subvert New Zealand's national interests by deceptive, corruptive, or coercive means.

All countries and businesses use foreign influence to gain access to foreign markets and products. These efforts may include routine diplomatic or commercial activities that promote their political or economic interests.

However, these efforts become a serious concern for businesses and government when the activities are deceptive, corruptive, or coercive.

When this occurs, foreign influence becomes foreign interference. Foreign interference can be divided into two main forms: political and societal. Societal interference refers to acts by foreign states that are intended to influence, disrupt, or subvert New Zealand's communities and non-government sectors, including businesses, by deceptive, corruptive, or coercive means.

Foreign interference is undertaken to further a country's own political, economic, military, or commercial interests or advantage.

Why could you or your business be at risk?

Foreign states may have an interest in you, your business, or your industry sector to help meet their strategic goals. These goals can include:

- furthering their international relations and global standing
- innovating and driving their economic growth
- modernising or enhancing their military.

Individuals and businesses could be targeted to gather personal data, research data, commercially sensitive information, IP, or to gain access or control over assets or organisations. In addition, there is sometimes intent to discredit, coerce, or punish businesses whose actions or statements are perceived as subversive by the foreign government.

Foreign states or their proxies can:

- use a relationship with your business to gain legitimacy
- gain access to your brand and your reputation – this could be used to advance interests and agendas of groups that don't align with your business interests or the national interests of New Zealand
- gain access to your IP, steal proprietary information, and potentially impact your markets, profits, and in some instances, impact the national economy
- exploit an investment or relationship that your business has with a private entity or individual to gain access to sensitive information
- seek to own, control, or have access to the business infrastructure or assets of New Zealand e.g. a foreign state-linked minority investor could have reporting requirements to provide its parent or country with information and data regarding the operation of business infrastructure or assets
- seek opportunities to develop a base for research and innovation that increases its economic, military, and technological advances over other countries.

◆ Case study

Foreign legislative and political regimes

Some foreign states have legal, regulatory, or administrative structures which ensure government control over entities based in that country. This could take the form of a statute requiring a company to hand over information or provide assistance to a state's intelligence services.

For example, the People's Republic of China (PRC) 2017 National Intelligence Law stipulates that all PRC citizens and entities, regardless of where they are located or operating, must assist the PRC's intelligence agencies.

This law also applies to PRC-based foreign entities. If information of potential interest to an authoritarian state is shared with a company based in PRC territory, there is a risk that the company will be forced to pass that information to the foreign government.





Specific aspects of your business that could attract foreign interest

Any of the following could make your business a more desirable target of espionage and foreign interference:

- your direct or indirect access, ownership, or control of critical infrastructure or a unique New Zealand economic asset
- your access to sensitive proprietary, political, commercial, or economic data and information for private and public entities, especially if that data and information is aggregated
- your unique or high value IP, including innovation and research work in development
- your market position or direct competition with foreign businesses
- your business and personal relationships that could be used to exert soft power, including your networks and supply chain, particularly where these are exclusive or provide access to influential individuals
- your brand and reputation – having a relationship with you would provide legitimacy and build credibility.



◆ Case study

Targeting New Zealand organisations

In recent years, New Zealand organisations have been approached by a small number of entities seeking to develop space infrastructure in our territory. These entities claimed the infrastructure would be used for civilian research purposes, but it was subsequently found in each case that what was proposed could have assisted foreign military activity that could have harmed New Zealand's interests.

The full capabilities, and some of the affiliations of these entities, were deliberately hidden. If these projects had gone ahead, we would have inadvertently allowed another country to install equipment in New Zealand with a plausible military or intelligence function. To have done so would have risked New Zealand's sovereignty.

By hiding their affiliations, the foreign entities attempted to undermine New Zealand's ability to make informed decisions based on our national security and national interest.



How espionage and foreign interference can affect your business

Foreign interference can manifest in many forms, from gaining influence and control through business activity to using espionage to collect data and information. It can also include economic coercion, such as disrupting trade to and from New Zealand.

Protecting your assets is important to your business and forms a part of the assurances you offer your business partners. When you recognise espionage or foreign interference as a potential threat, you can identify the risks to your business, consider your risk appetite and identify ways to treat those risks.

Not mitigating potential risks could lead to:

- negative impact or damage to your reputation in New Zealand or overseas, and a loss of trust
- loss of IP
- loss of control of your business
- financial losses
- increased risk to your employees.

Due to behaviours of some foreign states, you could also risk:

- inadvertent support for countries that do not share the values or interests of New Zealand to develop their military or security capabilities
- being complicit in human right abuses, such as use of forced labour/modern slavery.

Protective security advice

Simple steps can protect you and your business from espionage and foreign interference:

Be vigilant

Is interest in your business suspicious, ongoing, unusual or persistent compared to your regular interactions? If behaviour is deceptive, corruptive, or coercive, it should be reported to the NZSIS.

Check identity and connections to foreign governments

Research unknown individuals or businesses online to check their credentials and confirm their organisation exists.

Take a trusted colleague with you when meeting someone new

Having someone else around can make it harder for you to be compromised.



Examples of how espionage and foreign interference may present in business

Foreign states can use a range of methods to interfere in New Zealand businesses. Foreign states can target three main aspects of a business to achieve this: **ownership**, **control**, and **access**.

Once they have some degree of ownership, control, or access, they may not act negatively for a significant period.

This means businesses need to consider the long-term implications of their investment decisions, and the potential harm if factors change in the future.



Remember

The covert nature of foreign interference or espionage can make it hard to identify

Minority ownership, but control over your business

Soft power may be used to exert influence over your business. This soft power can come from a minority stake in a dispersed shareholding, or another form of ownership that provides a significant degree of undue or coercive influence (e.g. bespoke control arrangements attached to a minority shareholding, or some form of state/government control that can steer future decision making and policy).

A person or entity in control can act in a similar way to a majority owner to determine the course of your business. Dependant on the goals of the foreign state investor, minority ownership may provide sufficient influence over the business to achieve the state's strategic goals, such as disruption to the New Zealand economy. These outcomes are contrary to the national interest of New Zealand.



Access to your business, personnel, and systems

Foreign states may attempt to target your business in different ways to gain access:

01

Goods and services your organisation relies on

They may seek to own or control physical or cyber control systems, or physical facilities that enable your business to function or deliver goods and services.

02

Direct attacks or indirect attacks

They may attack you directly or target you to indirectly attack another business. Consider where you are in a supply chain and the services you provide. You may be targeted to achieve greater effect elsewhere, such as upstream or downstream in a procurement chain.



Collaboration/cooperation with overseas groups

Foreign states may use your overseas academic or research partnerships and business talent recruitment programs to access people, IT networks, IP, and research which may include sensitive or dual-use technology. Find more advice on protecting your sensitive research on our website:

www.protectivesecurity.govt.nz/trusted-research

03

Foreign states may also seek to visit your business premises to sustain collaboration and partnerships. You can find advice on how to manage visits from foreign delegations on our website:

www.protectivesecurity.govt.nz/inwards-visits

Personnel

Covertly placing people in your organisation can enable access to your information or assets. Corrupting or co-opting employees (wittingly or unwittingly) can cause similar risks, creating an **insider threat risk**. Insiders can offer ongoing access to sensitive information. You can read guidance for minimising insider threat, including when travelling, on our website:

www.protectivesecurity.govt.nz/campaigns/it-happens-here

04

05

Overseas travel

Overseas business engagement provides an easy route for foreign states to gain access to you when working abroad or travelling to attend corporate events such as conferences.

When you or your staff do business overseas, you may be subject to exploitation by foreign states. Find out how you can protect yourself while travelling on our website:

www.protectivesecurity.govt.nz/overseas-travel

06

Online



You may be targeted through a cyber-attack, such as via a phishing email. Foreign states may attempt try to trick you into revealing sensitive information, send you links to a malicious website, or use an infected attachment. Find out how to minimise online risk on the National Cyber Security Centre (NCSC) website: **www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-guidance-for-high-profile-Individuals-09-24.pdf**

The NCSC works with a broad range of partner organisations to build cyber defences including in New Zealand's private sector. Cyber security resilience is centrally important to ordinary business operations and, during incidents, the NCSC works with the suppliers to the affected organisations as they restore their services. Further information can be found on their website: **www.ncsc.govt.nz**



◆ Case study

Online recruitment

Some foreign states use online recruitment platforms or job advertisements as a means to collect sensitive or proprietary information, including against New Zealand. The prevalence of remote working has made this a more attractive avenue for foreign intelligence services. In early 2024, an online advertisement for a New Zealand-based intelligence analyst was posted on LinkedIn, likely by a foreign intelligence agency. The job was advertised as part-time and remote, with exaggerated remuneration and requirements to have access to geopolitical information of interest to a foreign state – all of which were indicators that it was an attempt to recruit an intelligence source online.

Along with online advertisements, some foreign states will specifically target individuals. Individuals who share information online about their employment, including access to, or knowledge of, sensitive technology or geopolitical insights could be susceptible to this type of approach.

Practical advice:

Educate your staff on the risks associated with recruitment platforms and ask them to consider what they put online about their employment and expertise. For more information, please see:

www.protectivesecurity.govt.nz/campaigns/think-before-you-link

Managing espionage and foreign interference risks

New Zealand has an open economy and conducts business with individuals, commercial entities, organisations, universities, and researchers within New Zealand and internationally.

If you or your organisations are considering international business arrangements or collaborations, you should:

- evaluate the research, investment, or business opportunity and the associated risks
- assess the benefits, considering ethical issues with the opportunity itself or the partner involved
- review your IP management systems.

While many overseas business, investment, and research relationships will be assessed as providing an overall benefit, others may involve more risks and may need more consideration.

Do your due diligence

Due diligence is a systematic assessment of the risks associated with any business, research, or investment decision with a potential new partner or collaborator. It also applies throughout the lifecycle of a business relationship, partnership, or investment.

The purpose of due diligence is to:

- avoid causing or contributing to adverse impacts on people, the environment, and society
- prevent adverse impacts directly linked to operations, products, or services through business or research relationships.

Find more information about due diligence assessments on our website: **www.protectivesecurity.govt.nz/due-diligence**

Build your security culture

Developing and maintaining a strong security culture is crucial for organisations to effectively manage their protective security. A strong security culture includes security values and practices, where employees recognise security as an enabler that is crucial to success. Alongside this recognition, a strong security culture leads to a workforce that takes ownership for security issues and is therefore more likely to think and act in a security-conscious manner.

Practical steps you can take

Build security awareness

People are much more likely to engage in your security culture if they understand the credible security risks that face your business. Develop security training to help people understand they have important security responsibilities and what those responsibilities are.



Publish clear communications about security

Everyone needs access to clear policies and procedures that explain the reasons for your organisation's security instructions and ensure people understand their responsibilities.



Manage concerning behaviour

Ensure your business has tools and policies to identify, support, and manage people who display concerning behaviour to do with security, poor performance, or unacceptable conduct.



Encourage a reporting culture

Raising legitimate security concerns should be encouraged and your business should have a process in place to respond to these appropriately.



Use legal frameworks

To use legal frameworks correctly and protect your business, consider any relevant export controls and legislation including the Privacy Act and the Overseas Investment Act.

Know about export controls that apply to your business

The New Zealand export controls regime controls the export of sensitive technology or strategic goods (military or dual-use goods), with the aim of:

- preventing the spread of weapons of mass destruction and stopping undesirable entities from developing other military capabilities (this is inclusive of controlling the export of catch-all goods)
- countering international threats such as terrorism
- protecting sensitive research and innovation.

The controls apply to the New Zealand business and research communities.

Controls may touch on several areas of industrial exchange, particularly areas that might enable technology to be transferred, either physically or electronically. Failure to get a licence to export controlled goods or technology is an offence.

Routine business activities that could be covered by export controls include:

- transferring (exporting) research undertaken as part of an international collaboration
- taking presentations to international conferences which contain sufficient detail to materially contribute to the development, production, or use of weapons/dual-use technologies
- exporting certain materials, organisms, devices, machines, or other goods.

It is important to find out if your business is subject to export controls. Your organisation's legal department, or other relevant corporate services function(s), should be able to help with advice on export control issues.

The Ministry of Foreign Affairs and Trade (MFAT) Exports Control Office can also advise on whether a particular export may be covered by export controls. Specific enquiries can be emailed to **exportcontrols@mfat.govt.nz**, and more information can be found at:

www.mfat.govt.nz/en/trade/trading-weapons-and-controlled-chemicals



Be aware of legal obligations in foreign jurisdictions

If you are collaborating with international partners or investors, there may be laws and regulations in their country that you need to comply with.

Most countries will maintain some form of export control. They may have laws which restrict the ability for businesses to share data or research outcomes, and their legal protections around IP may differ from the protections that exist in New Zealand.

Do not assume that your business partner will take responsibility for legal compliance and be aware of any requirements that may affect your collaboration.

As mentioned earlier in this guide, your international partners may also be subject to intelligence laws that could compel them to share their data or research with military or intelligence personnel in their country.

Understand your legal obligations to protect personal information

Know and uphold your responsibilities for protecting the privacy of data and information you handle while conducting business.

The Privacy Act 2020 sets out the framework for how New Zealand organisations collect, use, disclose, store, and give access to personal information in New Zealand. Ensure that all data containing personal information is protected in compliance with the Privacy Act.



For detailed information on the Privacy Act, including circumstances in which you'll have to report a privacy breach, check the Privacy Commissioner's website: www.privacy.org.nz



Overseas Investment Act

Foreign investment into New Zealand may be subject to regulatory approval, particularly investment in entities with access to, or control over, dual-use/military technology or critical infrastructure.



The Overseas Investment Act 2005 defines those New Zealand assets that are sensitive and/or strategically important, making them subject to a range of regulatory controls. A foreign investor acquiring these assets is required to understand its obligations under the Overseas Investment Act and engage with its regulator, Toitū te Whenua – Land Information New Zealand (LINZ), accordingly.

Whilst approvals aren't required in all circumstances; investments can be voluntarily notified by the foreign investor to gain safe harbour from future intervention. If you, as the business receiving foreign investment, have concerns regarding foreign interference risks you can request the investor engages with LINZ where required.



Guidance on who and what assets are covered by the Overseas Investment Act can be found here:

www.linz.govt.nz/guidance/overseas-investment



Specific enquiries from vendors, targets, and foreign investors regarding the Overseas Investment Act can be emailed to **oio@linz.govt.nz** or submitted online via **www.oio.linz.govt.nz/contact-us**



Utilise the Protective Security Requirements (PSR)

The PSR is New Zealand government's best practice security policy framework for security governance and for personnel, information, and physical security. It is a tool that organisations can use to protect what matters, and manage their security effectively and holistically.

As no two organisations are the same, the PSR follows a risk-based approach designed for flexible implementation. Implementing the PSR will help your organisation to protect its people, information, and assets.

More information can be found at: **www.protectivesecurity.govt.nz**



As the security landscape and economy in Aotearoa New Zealand continues to evolve, it is important for all organisations to understand the risks to their IP, sensitive research, data, information, and employees when building international partnerships. Protecting a business from harm is an important enabler for organisations as they carry out their mahi.

Resources

This section includes a range of useful resources to help guide organisations on identifying and managing their threats and risks.



Protective Security Requirements (PSR) website

The website outlines the Government's best-practice framework for how you could manage security governance, as well as personnel, information, and physical security. Find the framework at **www.protectivesecurity.govt.nz**

National Cyber Security Centre (NCSC) website

The NCSC enables the protection, wellbeing and prosperity of Aotearoa New Zealand by providing trusted cyber security services. Find out more at **www.ncsc.govt.nz**



Trusted Research

Aims to help New Zealand's research and innovation sector get the most out of international scientific collaboration while protecting their intellectual property, sensitive research, and, personal information.



Secure innovation

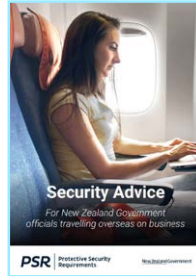
Provides the tech sector with a set of cost-effective measures that companies can take to better protect their ideas, reputation, and future success.



New Zealand's Security Threat Environment

An assessment by the New Zealand Security Intelligence Service which contains insight the reader can use, with a focus on foreign interference, espionage, and violent extremism.

www.nzsis.govt.nz/our-work/new-zealands-security-threat-environment



Security travel advice for government officials

Designed to support travelling officials to protect themselves overseas, but can apply to any individual looking to protect themselves or their organisation's people, information, and assets while out of the country.



Espionage and Foreign Interference Threats

Security advice for members of the New Zealand Parliament and locally elected representatives.



Due diligence

Helps organisations identify and mitigate the risks associated with foreign interference when working with others.



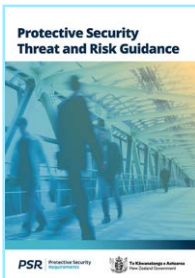
It happens here

This guide explains what insider threat is, how it happens, and what we can all do about it. It also includes case studies that illustrate the risks and consequences of not managing insider threats.



Think before you link

Practical advice on how to identify a malicious online profile, how to respond if approached, and how to minimise the risk of being targeted in the first place.



Protective security threat and risk guidance

Practical step-by-step guidance designed to support New Zealand organisations and community groups to understand, identify and assess threats, and treat and manage risks.



Managing inwards visits

Helps organisations assess possible security risks around visiting delegations from overseas.



For more information, go to:
www.protectivesecurity.govt.nz
psr@protectivesecurity.govt.nz



Te Kāwanatanga o Aotearoa
New Zealand Government

PSR

Protective Security
Requirements