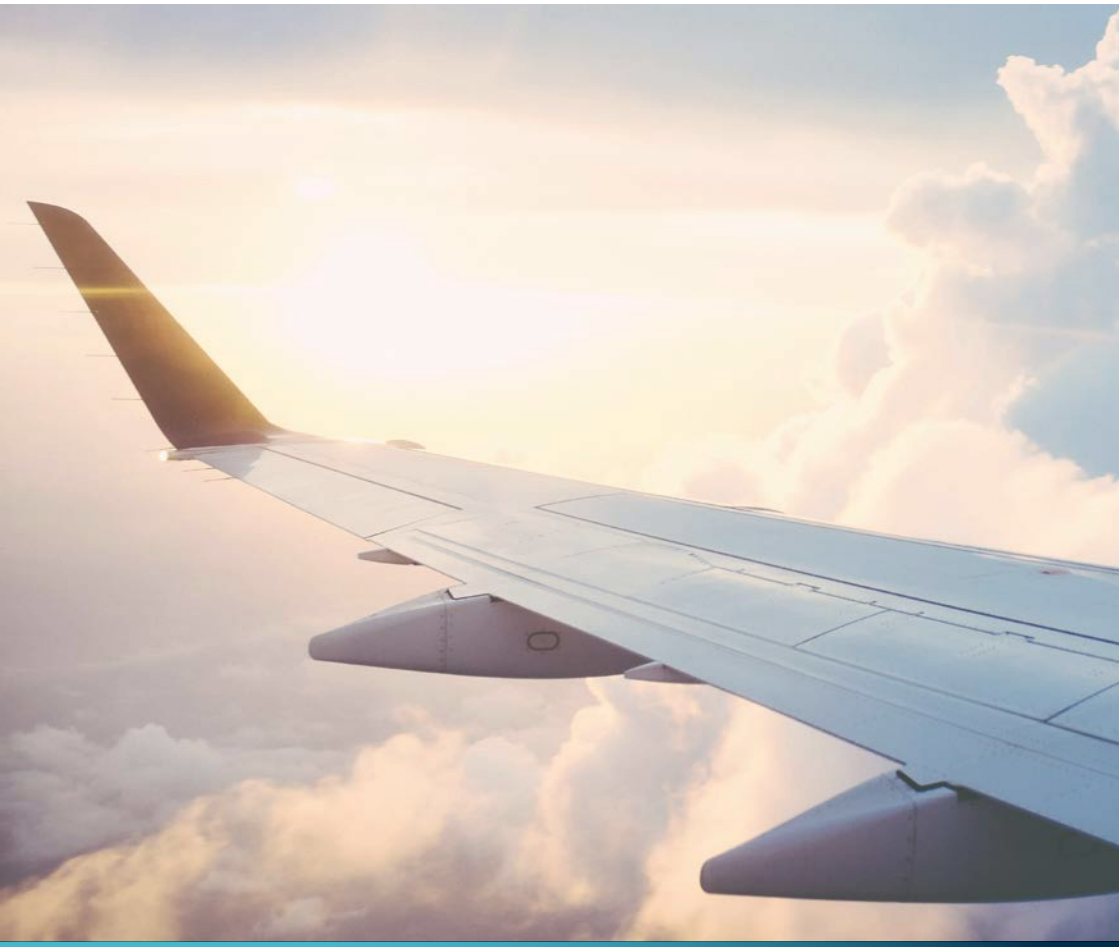
Travelling overseas on business

Protective security guidance for New Zealand travellers



PSR | Protective Security Requirements

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

Protecting yourself when overseas is important whether you are travelling as a government official or representing your business.

The relationships you have and your access to people and information can make you of interest to foreign governments.

Foreign government organisations may target you to get access to information, gain an advantage, or to influence, circumvent, or undermine New Zealand's open democracy and interests. Espionage and foreign interference can happen to all types of travellers, including those from:

- central and local government
- business and technology sectors
- research and education institutes
- iwi entities.

This guide will help you understand why you may be at risk from espionage and foreign interference, how these risks may occur, and how you can protect yourself and your organisation's interests while travelling overseas on business. At the back is a handy checklist to help you plan and manage your travel securely.

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.

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).

Why could you be targeted?

Some foreign governments are seeking to target New Zealand and our interests. These attempts are more effective when they have a “home ground” advantage, so they find it easier to collect intelligence from New Zealanders travelling overseas.

Foreign governments may be interested in New Zealand travellers for several reasons, including our:

- innovations in science and technology
- sensitive intellectual property and business data
- foreign investment opportunities in sectors such as agriculture, energy, and primary industries
- influential international relationships and partnerships
- government policies, particularly on international issues such as trade agreements
- defence, security, and intelligence capabilities.

Foreign government organisations aren’t just interested in government travel or classified information. You may also be of interest because of what you know, your personal opinions and statements you’ve made, your ability to make or shape decisions, or the access you have to other people of influence.

They also seek out privileged, public, or private sector information that will give them a fresh insight or provide a strategic or commercial advantage for their country. Information that may seem harmless to you may form part of a bigger picture for a foreign government organisation.

How could you be targeted?

Foreign government organisations may know about your travel in advance. They could find out about your travel plans through visa applications, foreign ministries, or even flight manifest data provided by airlines. Your travel plans may already be public due to a press release or social media post from you, your organisation, an overseas partner, or family and friends. In some cases, they might extend an invitation to you to visit and organise your travel arrangements and agenda on your behalf.

During your travel, foreign government organisations may attempt to gain influence or access to information they can use to their advantage. Many of their approaches or interactions will seem like normal social networking opportunities. You may be completely unaware you're speaking with an intelligence officer (or someone working on their behalf either wittingly or unwittingly). In some cases, they may be more overt and try to exert pressure on you or put you in a stressful or compromising position to compel you to do something you don't want to do.

Eliciting – seeking to gain information of value through targeted conversation.

Enticement – providing you with gifts, goods, or services at discounted rates, or suggestions of "preferred" merchants or service providers.

Talent spotting – attempting to build trust and rapport with you so they can assess whether you might give them information or have access to people of influence.

Intercepting public and private Wi-Fi connections and phone networks.

Eavesdropping – listening to your private and potentially sensitive conversations.

Physically interfering with possessions such as documents and electronic devices, including at airports and in hotel rooms.

Cyber exploitation – remotely accessing information on your electronic devices using techniques such as spear phishing email campaigns or by gifting exploited devices such as USB drives.

Setting up surveillance, both physical and technical. For example, placing listening devices in hotel rooms and vehicles.

Managing the risks

Before you go

Know the destination

Do your due diligence on your destinations to understand any associated security and personal safety considerations. Register with SafeTravel to receive up-to-date travel advice including potential security risks from violent protest or extremism, and contact details of the nearest consulate.

https://www.safetravel.govt.nz

Another useful resource is New Zealand's Security Threat Environment report released annually by the New Zealand Security Intelligence Service which includes real case studies of foreign government organisations conducting espionage and foreign interference.

https://www.nzsis.govt.nz

Know the value of your information

Before you head overseas, know what you need to protect.

- What is your potential value as a target — what information, knowledge, and access do you have?
- Do you or your travelling companions have any potential vulnerabilities which could be exploited?

To minimise the risk, ensure you only take information and devices essential to your travel and consider the potential impact of your information being compromised. Have a plan in place if you think you have been targeted or your organisation's information compromised.

Manage your electronic devices

All electronic devices that transmit are vulnerable to interception, manipulation, and/or information extraction; and can provide an entry point into your organisation's network. The risk of your electronic devices being compromised is heightened when travelling overseas.

Leave your devices at home and purchase a 'clean' mobile device to take overseas which doesn't hold any personal information or data, and only holds contact details required for your travel. If this isn't possible, ensure both personal and work issued devices:

- have up-to-date security and application patches
- are protected by strong authentication such as multi-factor authentication
- have any sensitive government or business information removed.

Understand your visit programme, objectives and outcomes

If your visit is being hosted by an international partner, know who you will be meeting and understand any pre-agreed actions or expectations before you travel.

- Has the proposed programme been shared with you and are you comfortable with all elements? Do you know who you will be meeting and understand the objectives and expected outcomes of each engagement?
- Will you be asked to formalise contracts, statements, memoranda of understanding (MoUs), or other agreements? If so, have you been provided with draft text in advance and undertaken due diligence, including legal review?
- Will your visit include publicity such as a joint press release, media appearance, or public statement? Is this in line with your organisation's brand and interests?
- Could any elements of your visit cause harm or reputational damage or disadvantage to you, your organisation, or New Zealand's national interests?

Do not feel pressure to agree to all proposed programme elements or any last-minute programme "surprises" from your host. Ask to take proposals away for further consideration.

The **Managing Inwards Visits guide** provides further detail on espionage and foreign interference risks that may arise through visit programmes and is a good resource even when you're the one travelling.

https://www.protectivesecurity.govt.nz/inwards-visits

While you're away

Secure your information and electronic devices

Maintain physical control of your information and electronic devices at all times, including in carry-on luggage during transit. Don't leave your information or devices unattended in hotel rooms and safes. Keep your personal devices and any work-issued devices separate.

- Maintain physical control of all your devices, including laptop and mobile phone chargers, at all times; if you lose sight or physical control, consider your device as compromised
- Avoid using a charger that someone else offers you and don't charge your electronic devices at public charging stations or via USB charging outlets
- Avoid using public Wi-Fi, including in hotels – talk to your IT team about hotspotting
- Disable wireless and Bluetooth functions when not in use
- Turn your devices off during any sensitive conversations
- Where devices can't be taken into an engagement such as meetings or break-out discussions, designate a staff member outside of the meeting to maintain positive control of your device(s) and ensure no physical material is left unattended.

Check your organisation's policies and procedures for use of electronic devices while travelling for business. If there are none, these should be established. For further advice, review the National Cyber Security Centre's guidance for high profile individuals.

www.ncsc.govt.nz/resources/cyber-resilience-guidance/guidance-for-high-profile-individuals

Personal physical security

Ensure that you follow country specific advice and guidance for travellers on the SafeTravel website as well as your organisation's health, safety and security policies and guidance.

Gifts and hospitality

International travel often involves the acceptance of gifts and hospitality, and in many cases, this is culturally required.

If you are gifted an electronic device including USB drives or other memory storage devices, don't plug them into government, organisational, or personal IT systems or devices. In the first instance, you should hand in any gifted devices to the part of your organisation that is responsible for security.

Persistent or extravagant gifts or social events with plentiful alcohol, may be an attempt to compromise you or gain favour. When travelling overseas, including when at events, stay alert to any approaches that may be suspicious, part of an ongoing pattern, unusual, or persistent. If travelling with others, ensure that you are not separated from them during social events.

When you return

We all have a part to play in keeping New Zealand's interests safe. Your experiences may not be in isolation and may form part of a bigger picture of foreign intelligence activity.

Report any concerns to your organisation's security lead or team. Depending on the size and nature of your organisation, this could be a designated Chief Security Officer, or someone with an IT or personnel security function.

Things to report may include:

- Official or social contact that seemed suspicious, ongoing, unusual, or persistent in any way
- Unusual incidents you experienced
- Electronic devices you suspect may have been compromised (including if your phone or laptop were out of your sight and control, even if temporarily)
- Written material that may have been compromised. For government officials, this includes any protectively marked material
- Any gifts including electronic devices such as USB drives
- Concerns relating to potential violent protest or violent extremism.

If you or your organisation's security lead suspects you have been targeted by a foreign intelligence service, report this via the New Zealand Security Intelligence Service website:

https://www.nzsis.govt.nz

If you travelled independently, you are still encouraged to report using the same portal.

Checklist

Before you go

Share a detailed itinerary of your travel plans with your security lead, manager, and colleagues	
Consult your organisation's security lead to see if you need a security briefing	
Register with **safetravel.govt.nz** and note the contact details of the New Zealand embassy or consulate nearest your destinations	
Know your security responsibilities to meet organisation policies and procedures while travelling	
Arrange to take minimal electronic devices and ensure they are clean. Your organisation may be able to provide these	
Remove non-essential data e.g. apps, accounts, contacts, emails, and files from any devices you do travel with	
Clear your web browsing history	
Enable encryption on electronic devices or ask your organisation's security lead to do it for you	
Set complex passwords and enable MFA for your electronic devices	
Know and agree to any visit programme and expected objectives or outcomes. Ensure you are comfortable with what is being asked of you and prepare ways to gracefully decline anything that raises alarms for you	
Do due diligence on things you may need to sign or agree to, including legal reviews	
Know what information you can share, and what needs to be protected	
Prepare responses for any tricky questions or sensitive issues that may come up	
Make yourself familiar with local laws and customs	
Consider any health and safety or security risks specific to your travel, and plan for specific contingencies in advance e.g. what will you do if you become sick while overseas?	

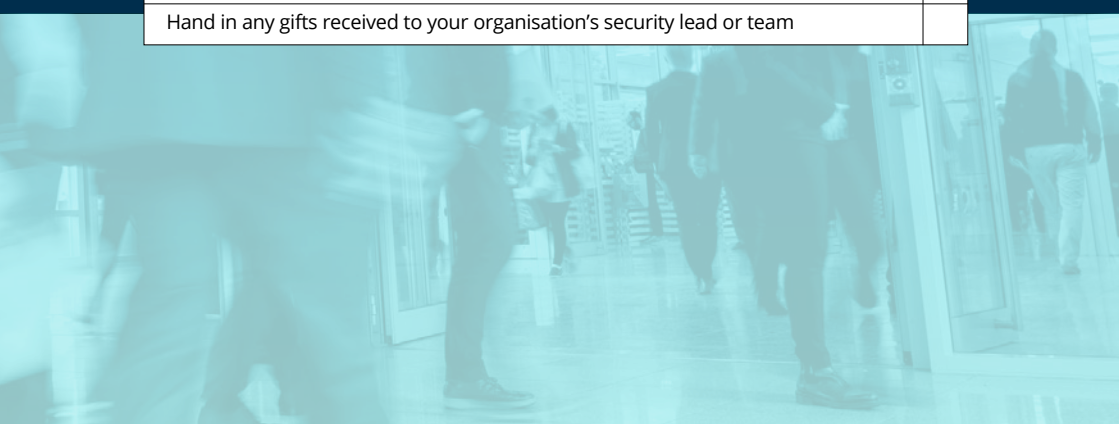
Checklist

While you're away

Always maintain physical control of your electronic devices and official documents. Consider using tamper evident bags or envelopes and don't leave your electronic devices and chargers unattended in hotel rooms, including in safes	
Don't talk about sensitive matters in locations which could be compromised. For government officials, only discuss classified matters in suitably secure facilities within NZ diplomatic posts	
Be cautious about giving your personal email, social media accounts, or phone numbers to people you meet. For government officials, only give out your official contact details	
Be wary of drinking alcohol and lowering your inhibitions at social events. These events give foreign government organisations opportunities to learn more about you or your organisation	
If you're connecting to the internet, use a trusted data network rather than an open Wi-Fi network. When not required, turn off Bluetooth, GPS, and other location settings on all devices	
Only use your own chargers. Do not use a charger that someone else offers you and don't charge your electronic devices at public charging stations or via USB charging outlets	
Don't open unsolicited emails, attachments, or messages from unknown sources	

When you return

Report any concerns to your organisation's security lead or team	
Hand in any gifts received to your organisation's security lead or team	



For more information, go to:

www.protectivesecurity.govt.nz

psr@protectivesecurity.govt.nz

PSR | Protective Security Requirements

Te Kāwanatanga o Aotearoa
New Zealand Government