Security Advice

For New Zealand Government officials travelling overseas on business

PSR | Protective Security Requirements

New Zealand Government

What is the threat to New Zealand when you travel overseas?

When you travel overseas, foreign intelligence services may target you to get access to New Zealand Government information. This threat is constant.

Use this security advice to help protect yourself and New Zealand Government information while travelling overseas.

Why would you be targeted?

Foreign intelligence services have the intent and capability to target New Zealand and our interests.

As a New Zealand Government official, your travel overseas gives foreign intelligence services many opportunities to collect intelligence.

They may be interested in New Zealand Government officials for several reasons, including our:

- position on international issues and agreements such as trade
- strategic perspective and intentions (including domestic policies)
- defence and intelligence capabilities
- innovations in science and technology
- agriculture, energy, primary industries, and other sectors which attract significant foreign investment interest
- alliance with the Five Eyes and other bilateral relationships.

Foreign intelligence services aren't just interested in gaining access to protectively-marked or classified government information. They may also attempt to get access to privileged, public or private sector information, including personal opinions and statements you've made. They may act on behalf of their government or be trying to fulfil their government's obligations to third parties.

They're also interested in collecting information about the identities of other New Zealand government personnel with access to sensitive information or people of influence. For example, your colleagues, managers, or key stakeholders.

Foreign intelligence services may use the information they gather for subsequent intelligence targeting either in their home country, in New Zealand, or in a third country. Even information that seems harmless on its own may be combined with other information to fill intelligence gaps or identify individuals for future targeting.

How would you be targeted?

Foreign intelligence services may be alerted to your travel in advance. They could find out about your travel plans through visa applications, foreign ministries, and even flight manifest data provided by airlines.

They may use several methods 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 intelligence officers.

Methods foreign intelligence services may use to target you:

- 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.
- Eliciting – seeking to gain information of value through targeted conversation.
- Eavesdropping – looking for opportunities to listen in when you and other government officials relax your personal security and discuss sensitive matters in public or social settings.
- Intercepting public and private Wi-Fi connections and phone networks.
- Physically interfering with possessions such as documents and electronic devices, including at airports and in hotel rooms.
- Setting up surveillance, both physical and technical. For example, placing listening devices in hotel rooms and vehicles.
- Using cyber exploitation – remotely accessing information on your electronic devices using techniques such as spear phishing email campaigns and by gifting exploited devices such as USB drives.

Be aware that you may be subject to ongoing targeting when you're back in New Zealand.

Minimising the threat

What to consider when you're travelling overseas:

- Your potential value as a target — what information, knowledge and access do you have? Remember it won't just be protectively-marked material foreign intelligence services are interested in.
- Do you or your travelling companions have any potential vulnerabilities which could be exploited?
- Have you noticed any suspicious computer activity or emails? They may be a sign that an upcoming event or visit is a cyber target.

Checklist

Before you go

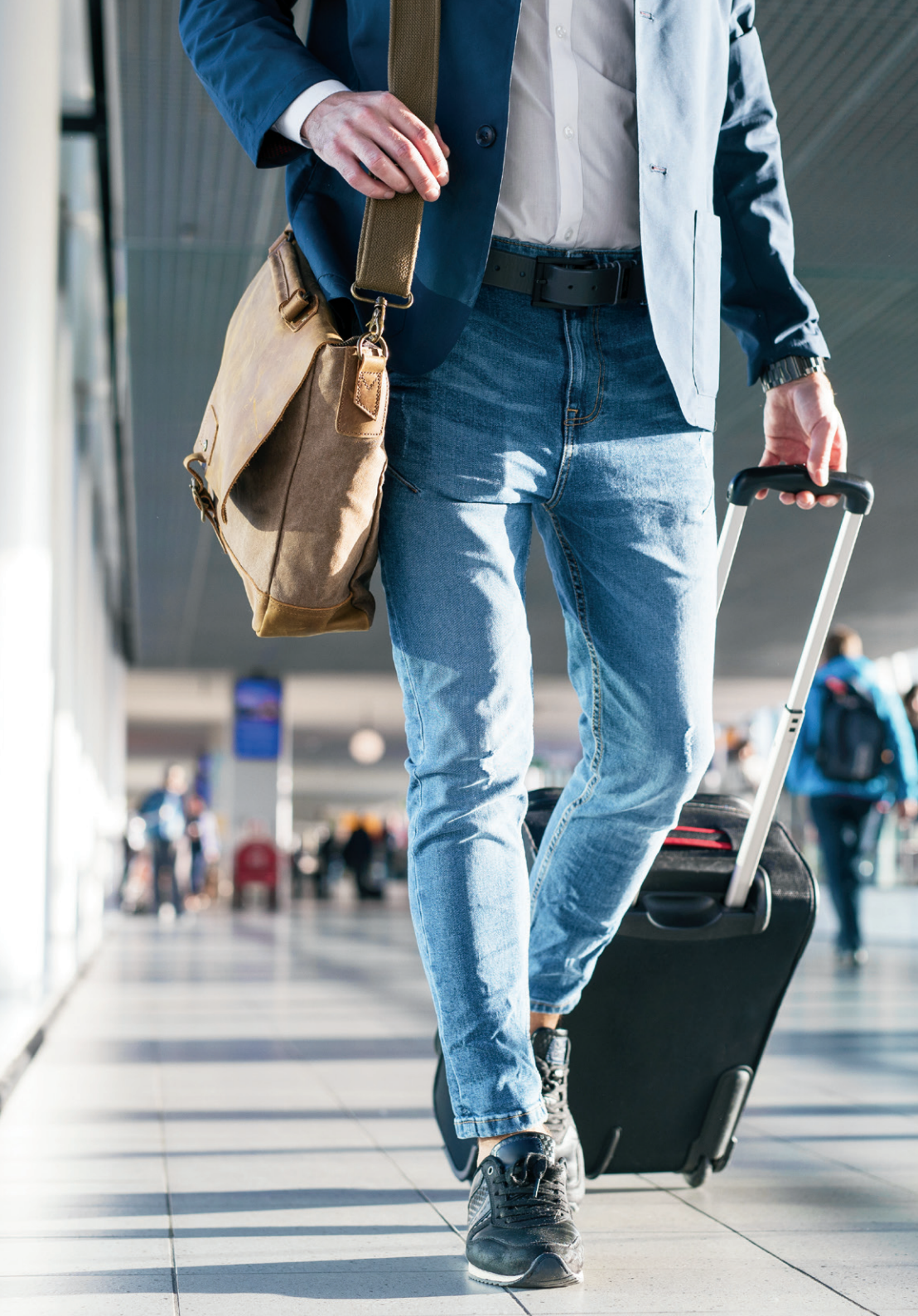
- ✓ Always consult your organisation's security team to see if you need a security briefing.
- ✓ Share a detailed itinerary of your travel plans with your managers and/or colleagues.
- ✓ Know your security responsibilities and meet Protective Security Requirements while you're travelling.
- ✓ Consider taking clean electronic devices with you – devices that have not been used and will not be used when you return. Your organisation may have clean devices you can use.
- ✓ Remove all non-essential data from your devices including any apps, accounts, contacts, emails, and files.
- ✓ Clear your web browsing history before you travel and use private browsing mode during your trip.
- ✓ Know what to share, trade, and protect. That means knowing your organisation's official stance on relevant topics and issues, what information you can share, and what information is sensitive and protected.
- ✓ Prepare responses for any tricky questions or sensitive issues that may come up.
- ✓ Register on MFAT's safe travel website: ***www.safetravel.govt.nz***

While you're away

- ✓ Make sure you only talk about sensitive or classified matters when you are in secure facilities within New Zealand posts.
- ✓ Don't give your personal email, social media accounts, or phone numbers to people you meet overseas. Only give out official contact details to your foreign business contacts.
- ✓ Be mindful that foreign intelligence services may use surveillance and eavesdropping techniques to listen to conversations you have in hotels, public or private vehicles, elevators, conference rooms, restaurants, and outdoor areas.
- ✓ Maintain physical control of official documents and electronic devices at all times. Consider using tamper evident bags or envelopes.
- ✓ Don't open unsolicited emails, attachments, or messages from unknown sources.
- ✓ Be wary of drinking alcohol and lowering your inhibitions at social events. These events give foreign intelligence services opportunities to learn more about you.
- ✓ Never carry electronic devices in your checked luggage. Don't leave your devices unattended in hotel rooms, including in safes.
- ✓ Ensure you enable encryption on your electronic devices or ask your security team to do it for you. Set complex passwords for each device.
- ✓ If you're connecting to the internet, use a trusted data network rather than an open Wi-Fi network.
- ✓ 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.
- ✓ Turn off GPS and location settings on all electronic devices.

When your return

- ✓ Report to your Chief Security Officer or your organisation's security team any:
  - official or social contact that seems suspicious, ongoing, unusual, or persistent in any way
  - unusual incidents you experience
  - electronic devices you suspect may have been compromised
  - protectively-marked material that is or may have been compromised.
- ✓ Hand any gifted devices to your Chief Security Officer on your return. Don't introduce gifted devices, including USB drives, memory storage devices, and compact discs to any New Zealand Government computer system or device.



For more information, go to:

www.protectivesecurity.govt.nz

psr@protectivesecurity.govt.nz

VERSION 2 / JUNE 2019

New Zealand Government