From: Tony Prompong
To: Emma Miles-Buckler; Donna Williams-Stewart
Subject: FW: Clean devices - Robbie Muir to China
Date: Tuesday, 1 October 2019 12:37:38 p.m.
Attachments: image001.png
image002.png

Hi Emma,

Below email outlines what we can and cant offer regarding hardware and email access.
Also attached is travel advice.

I will be providing Robbie Muir with a new laptop, new connection and mobile early November so he will be comfortable with the devices.

Thanks for the Mobile form ill get that processed soon.

Regards

Tony Prompong
Operations Advisor – IT Support
IT Operations

E **xxxxxxxxx@xxxx.xxxx.xx**

Wellington Office, Level 7, Radio New Zealand House, 155 The Terrace
PO Box 5501, Wellington 6145, New Zealand | T 04 462 4477 | M 027 271 8301
W **www.linz.govt.nz** | **data.linz.govt.nz**
http://www.linz.govt.nz/sites/default/files/images/email-signature-v2.png

---

From: Berny Fischer
Sent: Wednesday, 25 September 2019 4:22 PM
To: Donna Williams-Stewart <@..>; Tony Prompong <@..>
Cc: Clive Eastwood <@..>; Francois Meyer <@.vt.nz>
Subject: RE: Clean devices - Robbie Muir to China

HI All,

PSR has developed some pretty good documentation for this.

Attached is generic document for any government official travelling on business, it's a few pages long – I would be happy to summarize and brief Robbie on the important points before he goes if that's easier than reading it.

I have also attached a 2 pager on recommendations for electronic media.

We suggest he takes a clean laptop with VPN access to work and check email on (i.e. doesn't not use web mail or email on phone) and a clean/new burner mobile phone – with no email access on it.

It might be useful if we sat down and came up with 'LINZ staff travelling' IT guide for future scenarios like this as they probably aren't that common and will help staff understand what they need to do in advance etc. I say the royal 'we' as you guys will probably end up wearing the 'clean' device and 'burner' phone situation so needs to be something realistic for everyone.

Any questions – you know where I live.

Cheers,

Berny

From: Donna Williams-Stewart
Sent: Wednesday, 25 September 2019 2:10 PM
To: Francois Meyer <@..>; Clive Eastwood <@..>
Cc: Tony Prompong <@..>; Berny Fischer <@..>
Subject: FW: Clean devices - Robbie Muir to China

Hi,

Please be advised that Robbie Muir, DCE, Strategy and Stewardship will be travelling to China in his role as Registrar General of Land to present at the World Bank conference.

Tony Prompong and I met with Emma Miles-Buckler yesterday to discuss what Robbie will need in terms of Security regarding the devices he will need while over in China.

Please advise what security guidance we will need to advise Robbie regarding access to LINZ information, whilst in China or any Security Clearance is required.
He will be leaving NZ 20th November 2019 and returning 24th November 2019.

Regards
Donna

From: Emma Miles-Buckler <@..>
Sent: Monday, 23 September 2019 2:22 PM
To: Donna Williams-Stewart <@..>
Subject: RE: Clean devices - Robbie Muir to China

Robbie has a LINZ mobile and physical device but he will need a clean one for China - new device and number please

Thanks

From: Donna Williams-Stewart
Sent: Monday, 23 September 2019 2:20 PM
To: Emma Miles-Buckler <@..>; Chris Monteith <@..>
Cc: Morwenna Grills <@..>
Subject: RE: Clean devices - Robbie Muir to China

Hi Emma,

We can definitely assist and have a laptop ready for Robbie before the time. Also, in terms of a mobile, we can arrange for Robbie to have a LINZ mobile number and number if he doesn't have one already.

Ill set up a meeting with Tony Prompong, our IT Support to discuss Robbies needs to access the LINZ Network and how, and what the lead times are to have laptop and mobile ready and tested for Robbie before the time.

Regards
Donna

From: Emma Miles-Buckler <@..>
Sent: Monday, 23 September 2019 2:02 PM
To: Donna Williams-Stewart <@..>; Chris Monteith <@..>
Cc: Morwenna Grills <@..>
Subject: Clean devices - Robbie Muir to China

Hi – in the 3rd week in November Robbie will be going to China to present at a World Bank conference and he will need clean devices to take in … at this stage he will need a laptop and a cell phone.

Not sure what the rules are around this but can we please either meet so you can you let me know what your suggestion are – or an email is fine

Thank you

Emma

Emma Miles-Buckler
Executive Assistant to Robbie Muir
Registrar General of Land & Deputy Chief Executive, Strategy & Stewardship

E xxxxxxxxxxxxxx@xxxx.xxxx.xx **DDI 04 462 4452 | M 022 306 9787**
Wellington Office, Level 7, Radio New Zealand House, 155 The Terrace
PO Box 5501, Wellington 6145, New Zealand | T 04 460 0110
W www.linz.govt.nz | data.linz.govt.nz

PSR | Protective Security Requirements

TRAVELLING OVERSEAS WITH ELECTRONIC DEVICES

Introduction

The sophistication and versatility of modern mobile electronic devices means they are often used to extend office functionality outside the workspace and domestic spheres. In terms of convenience, connectivity and increased productivity, the benefits of mobile devices are undeniable. Their use does not however come without increasing risk and they should be used in strict compliance with agency policy and security requirements.

As such, while mobile and electronic device security can be inconvenient, it is essential agencies and personnel actively consider and mitigate the risks of operating mobile and electronic devices overseas.

All electronic devices, whether personal or work, are vulnerable to interception, manipulation and/or information extraction. These risks are heightened overseas. Even personal devices which have not been used to process official information hold a significant amount of information about you. While the compromise of a personal device may not result in the compromise of official information it could still be used maliciously by a hostile agency or individual.

- Agencies should consider whether it is absolutely necessary for a staff member to take their work electronic devices overseas.
- Agency personnel should consider whether it is absolutely necessary to take their personal electronic devices overseas.

If it decided that it is necessary then the guidelines below should be followed where possible.

Personnel should consider taking a “clean” electronic mobile device overseas, that is, a newly purchased device to be used for the length of the trip only and which has not stored any information associated with the user.

Personal Devices

Before traveling you should

- Update the device with the necessary security and application patches.
- Enable device security features such as access passwords and PINs.

During travel you should

- Never use your personal mobile or electronic device(s) for official business.
- Maintain physical control of electronic devices at all times; if a device is taken out of your sight or physical control, treat it as compromised. This includes storage in hotel safes and checked-in luggage.
- Practice security awareness; do not allow strangers to access or handle any electronic devices in your possession and be alert to any covert access to information stored on them, for example, onlookers attempting to read the screen.

Work Devices

In addition to the guidelines outlined for personal devices above, if taking and operating a work electronic device overseas, personnel should comply with the following measures.

Before travel you should

- Remove any official information stored on the device that is not required.

During travel you should

- Not use work devices to access or process sensitive or official material in public locations, for example, in hotel lobbies, airports or while using public transportation.
- If the device is not being used, especially during classified conversations, consider disabling wireless and Bluetooth functions and powering the device off and/or removing the battery.
- If your electronic device is taken out of your sight or physical control, treat the device as compromised and cease to use it.
- Use the device for work and/or official purposes only, not for personal purposes.

After travel you should

- Report any compromise of an electronic device – either suspected or actual – to the agency Chief Security Officer as soon as possible and have the device sanitised before it is used again.

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

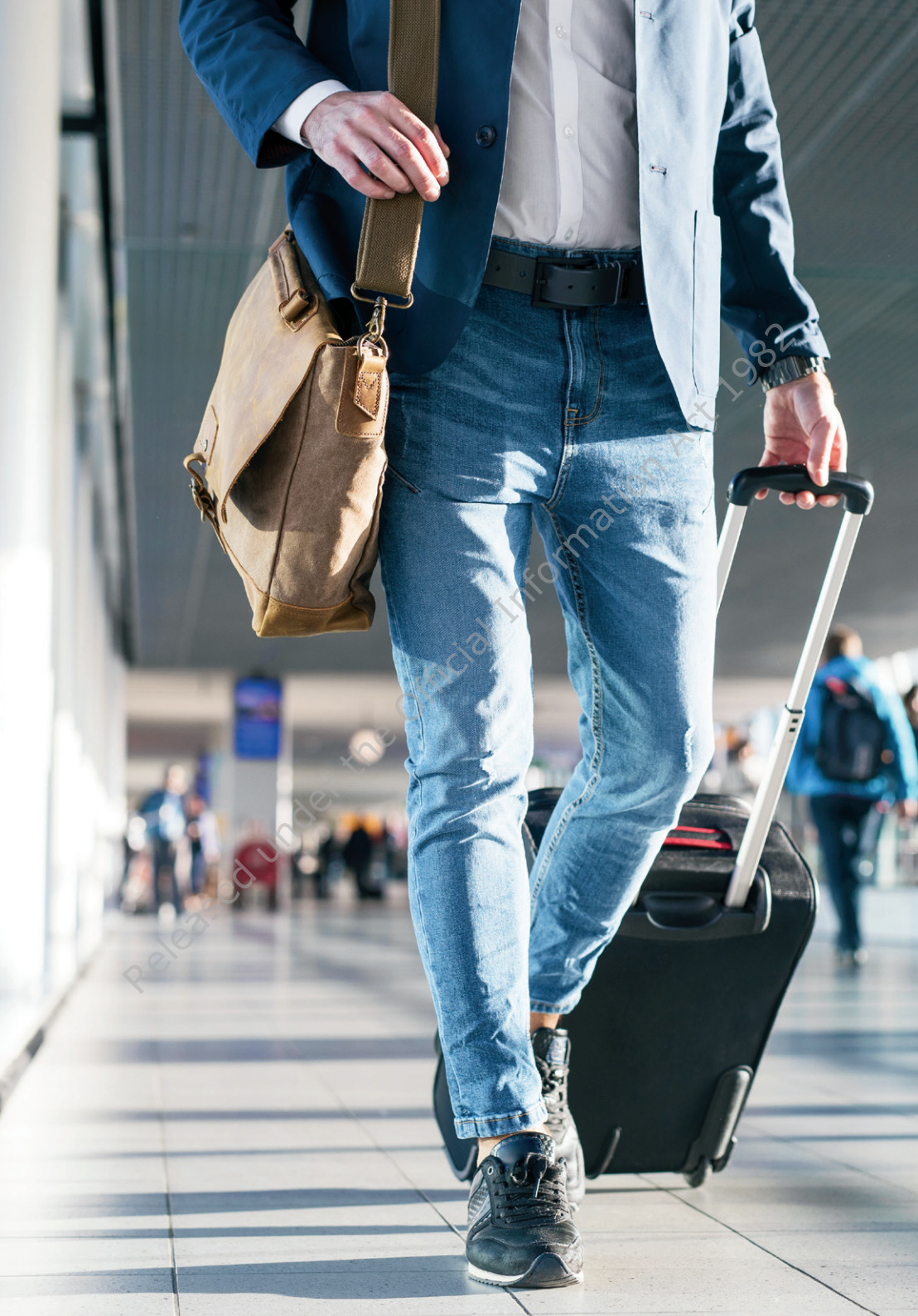
- ✓ Always consult your organisation's security team to see if you need a security briefing.
- ✓ Share a detailed itinerary of your travel plans with your managers and/or colleagues.
- ✓ Know your security responsibilities and meet Protective Security Requirements while you're travelling.
- ✓ Consider 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