

Australian Government

Australian Security Intelligence Organisation

MANAGING THE ESPIONAGE AND FOREIGN INTERFERENCE THREAT WHILE TRAVELLING OVERSEAS

ASIO

Espionage and foreign interference can occur anywhere.

What to know about the threat

Multiple foreign powers are aggressively conducting espionage and foreign interference against Australia. They want to know about Australia's politics, defence, national security, technology, economy and sensitive data. Some foreign powers are determined to undermine Australia's sovereignty, interfere in our democracy and influence decision-making.

These foreign powers want to know what you know, what you can access and how you can be used to act in their national interests. When you travel overseas, foreign intelligence services (FIS) can target you more easily in their home countries. To protect yourself and your assets while travelling, it's essential to take steps to enhance your personal safety and security.

What to know before you go

Know your value

Before you travel, **know the value of the sensitive or classified knowledge you hold**. Could FIS and their proxies find this information valuable? What would happen if it ended up in the wrong hands? Also be aware that FIS are very interested in the privileged places, systems and people you can access, and the processes and decision-making you know about, not only in your workplace but across the Australian Government.

BE AWARE

Know your destination

Before you book any overseas business travel, **check with your workplace security team for advice about your destination/s**. Ask about your workplace's security expectations and what to do if you have security concerns during your travel.

Be aware of the laws of your destination and how these apply to travellers, how citizens and visitors are typically treated by law enforcement, the relationship between the destination country and Australia, and if you could be lawfully compelled to hand over sensitive information/devices or download apps (for example, for visa or health purposes).

In terms of your destination, make sure you know how to contact local emergency services, and where to find – and how to contact – the nearest Australian diplomatic mission if you need assistance. If your destination doesn't have an Australian diplomatic mission, find out in advance which country can help Australian citizens. Keep this information with you at all times.



Visit Smartraveller
www.smartraveller.gov.au
for current travel advice

Subscribe to the ASIO Outreach portal
www.asio.gov.au/outreach

Know how it could happen

This graphic shows how you, your information and your devices could be targeted while you're travelling.





What to do on the go

Protect yourself

- **Stay aware of your surroundings** and contact emergency or security personnel if you need assistance.
- Provide your business contact details only – including for official documents, travel bookings and event registrations.
- Don't advertise your business and travel plans online.
- Travel light – only take the information and devices you really need.
- **Be discreet and practise good security** – FIS and criminals are more likely to target people who seem indiscreet or who display poor security practices.
- If travelling for an event, **know the visa, accommodation, travel and digital requirements** (for example, you may need to download apps or connect to unsecure networks). And if you are asked to provide a resume, consider if a detailed resume is necessary or if a simplified resume will be sufficient.
- **Don't do anything overseas that you wouldn't like people at home to know about**, as it could potentially be used as leverage against you.
- **Regularly check Smartraveller for travel advice updates** – and check with your workplace security team as soon as possible if there is a change to the security environment in your location.



Protect what you know

- **Do not travel with classified information above OFFICIAL: Sensitive**. The Department of Foreign Affairs and Trade's in-country posts can recommend options for you to safely access classified information.
- Keep sensitive or classified material with you at all times – never pack it in your check-in luggage or leave it unattended. **Hotel rooms and hotel safes are not secure.**
- Only discuss classified matters in approved secure facilities or via secure communications in Australian embassies or high commissions.
- **Be selective about where you discuss sensitive matters.** Conversations in planes, cars, hotel rooms, lifts, conference rooms, restaurants and outdoor areas (including hotel balconies) may be overheard or recorded.
- Be alert to questioning – some people can skilfully steer conversations to obtain information from you.
- Be aware that **physical, audio or video surveillance could occur** – let your workplace security team know as soon as possible if you notice anything concerning.



Protect your electronic devices

Australian electronic devices are routinely targeted during overseas travel – it is a real and persistent threat. You should talk to your security team about how to secure your electronic devices before, during and after you travel overseas.

Here are some recommendations:

Before you travel

Take dedicated devices to use while travelling – only use for essential work-related activity and never connect these to corporate networks – they should be factory reset upon your return. **Leave your personal devices at home** so your personal information and access isn't compromised, stolen or lost. If you can't leave your personal devices at home, **remove or delete unnecessary contents** and do a backup before travelling.

Set up **multi-factor authentication (MFA)** whenever possible for all your accounts. When possible, use a token, authentication app, or email address for MFA and avoid using text message as it's less secure.

Ensure all software and security updates on each device are current before departure.

TIP

Create a travel email address and use that to set up clean dedicated devices specifically for use during your travel/time overseas. Then set up email forwarding as needed to this new travel email address. Make sure you don't use it to log into any personal accounts you have used before or plan to use again after your trip. You can cancel the email forwarding on your return.

Do not preload files onto your device. Instead **use file sharing systems (iCloud, Google Drive, OneDrive etc) and share them with read-only permission to your travel email**. Then you can access/download those files on arrival.

Use new passwords for all accounts you will access while travelling and change them again after your trip.

Turn off camera and microphone access for all apps or change settings to 'only while using app'. Turn off background application refresh, turn off notifications for all applications not in use and turn off AirDrop and other wireless file sharing programs.

- Use a passphrase (ie a long password) when travelling overseas.
- PIN codes (ie 4-6 digits) are less secure and easier to observe.
- Avoid using biometrics (ie FaceID or fingerprint) while overseas, some countries may force you to unlock your device.





While you travel

- Never pack electronic devices (including multi-factor authentication tokens) in checked-in luggage.
- Tokens should always be with you or in a secure place (such as a container at Post) at all times.
- **Don't leave electronic devices unattended in hotel rooms** and hotel safes as they can be convenient areas to tamper with your devices. Keep them with you or within your sight at all times.
- Do not download applications while travelling.
- **Avoid scanning QR codes**. Instead, type in the website.
- Turn all devices off and on again overnight.
- All wi-fi networks should be considered unsafe. If you must connect to wi-fi for any reason, **use a virtual private network (VPN) connection**. This includes airports and hotels – don't assume these networks are safe even if your booking has been made through your organisation.
- Disable capabilities such as mobile data, wi-fi and Bluetooth when not in use. This is to limit the potential compromise of your data. Be aware that **devices in flight mode are still vulnerable to compromise**.
- Be careful when charging your devices. **Only use power outlets, and your own chargers and cables** that are specific to your device. If you must charge your device using a USB outlet, disable the USB option – allow charging only.
- Ensure conversations are held in appropriately classified rooms or video conferencing systems. If this isn't possible, **consider not having the conversation while overseas**.
- **Be discreet when using your devices**. Ensure that no one can observe your passwords and activities – including between plane seats or through windows. Also note that CCTV cameras can be used to identify your password combinations and activities.



TIP

Encrypted apps and devices are not secure – technical collection and eavesdropping can still occur.

Consider the use of lockdown mode on Apple devices to reduce the attack surface.



If a device starts behaving strangely, stop using it immediately and report it to your security team

After you travel

- **Change the PINs and passwords** for your devices and accounts accessed.
- **Report** any lost, stolen or possibly compromised devices to your workplace security team as soon as possible. If a device starts behaving strangely, stop using it immediately and report it to your security team.
- Cancel any email forwarding to your travel email address.
- Return corporate devices to your security team for inspection.

For more comprehensive advice, visit the Australian Cyber Security Centre at **www.cyber.gov.au** and search for **'Security tips for travelling'**.



Know when to say ‘no’

When travelling overseas for official purposes, be cautious of excessive hospitality and gifts from your hosts. These may be attempts to gain your favour or test your willingness to help.

Some gifts can contain hidden listening devices or malicious code. Use your judgement and if unsure, consult your security team.

ASIO recommends you decline electronic gifts, but if accepted, isolate them from sensitive areas and arrange for secure disposal with your security team.



‘Use your judgement to decide whether an offer seems more generous than it should’



What to do after you leave

Report anything suspicious, ongoing, unusual or persistent

The Australian Government Contact Reporting Scheme (CRS) is a vital tool that helps ASIO identify the activities of FIS, including how these services target government personnel, information and facilities.

*If you are unsure about reporting an incident – **you probably should**. Your reporting could help identify a wider pattern.*

Contact reporting is a requirement for individuals who hold a security clearance.

Under the CRS, you must report any behaviours, activities or approaches that seem:

- **S**uspicious
- **O**ngoing – contact with a foreign national
- **U**nusual
- **P**ersistent

You should also report:

- any changes in the subjects your contact wishes to talk about.
- people who tried to access information or places they shouldn't have.

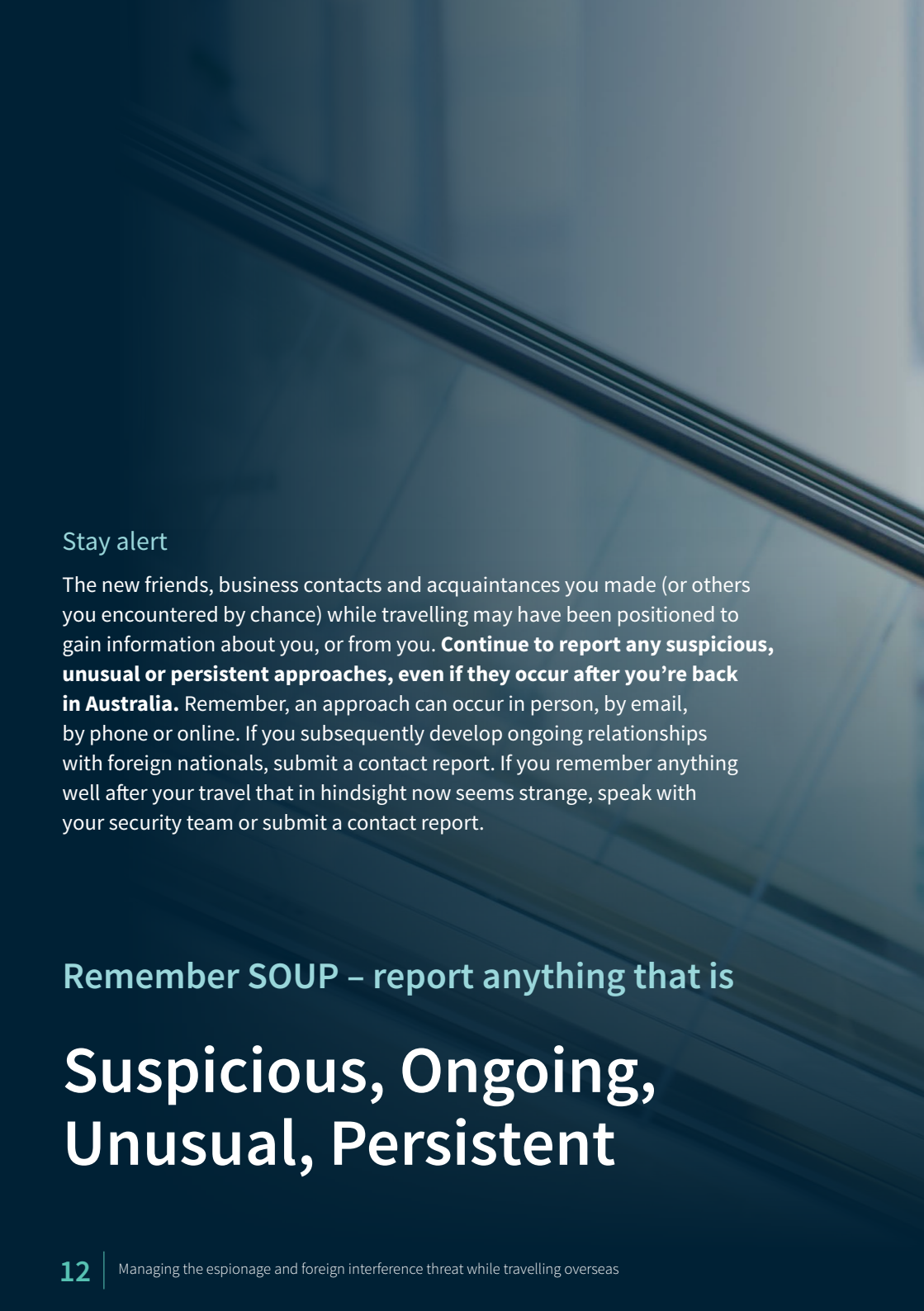
How to report

Government workers and security clearance holders:

- contact your Agency Security Adviser and fill out a contact report

Other workers:

- use ASIO's Notifiable incidents, Threats or Reportable Observations (NITRO) portal at nitro.asio.gov.au
- call the National Security Hotline on 1800 123 400



Stay alert

The new friends, business contacts and acquaintances you made (or others you encountered by chance) while travelling may have been positioned to gain information about you, or from you. **Continue to report any suspicious, unusual or persistent approaches, even if they occur after you're back in Australia.** Remember, an approach can occur in person, by email, by phone or online. If you subsequently develop ongoing relationships with foreign nationals, submit a contact report. If you remember anything well after your travel that in hindsight now seems strange, speak with your security team or submit a contact report.

Remember SOUP – report anything that is

Suspicious, Ongoing, Unusual, Persistent


REPORT
SUSPICIOUS
ACTIVITY



asio.gov.au

25-0726