



Australian Government


**Australian Security
Intelligence Organisation**

An aerial view of a commercial airplane flying towards the viewer, with its landing gear deployed. The background is a bright, cloudy sky.

MANAGING THE ESPIONAGE AND FOREIGN INTERFERENCE THREAT WHILE TRAVELLING OVERSEAS

The ASIO logo, consisting of the letters 'ASIO' in a stylized, bold font, with a blue and white color scheme. The logo is positioned in the bottom right corner of the cover, above a dark blue horizontal band.

ASIO



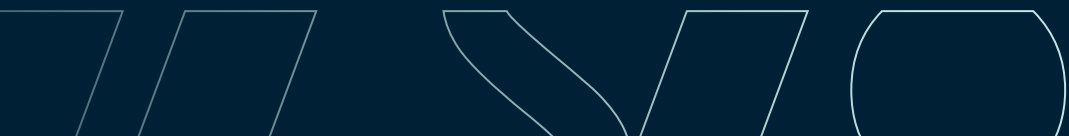
Espionage and foreign interference can occur anywhere.

What to know about the threat

Multiple countries are aggressively conducting espionage and foreign interference against Australia. Foreign powers are interested in what you know, what you can access, and what you can do for them. They want information about Australia's political system, defence capabilities and operations, national security arrangements, unique technologies, economic and trade advantages, diaspora communities, sensitive and commercially valuable Australian information, intellectual property, and databases of personal information.

Some foreign powers are also determined to interfere in Australia's democracy, undermine Australia's sovereignty and shape political and business decision-making. This is occurring in all states and territories, at all levels of government, on all sides of politics and in the private sector.

Espionage and foreign interference can occur anywhere. In fact, foreign intelligence services can target you more easily in their home countries. When you're travelling overseas for business, ensure you take these steps to enhance your personal safety and protect your knowledge and assets.



What to know before you go

Know your value

Before you travel, know the value of the sensitive or classified knowledge you hold. Could third parties find it valuable? What would happen if it ended up in the wrong hands? Also be aware that foreign intelligence services 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

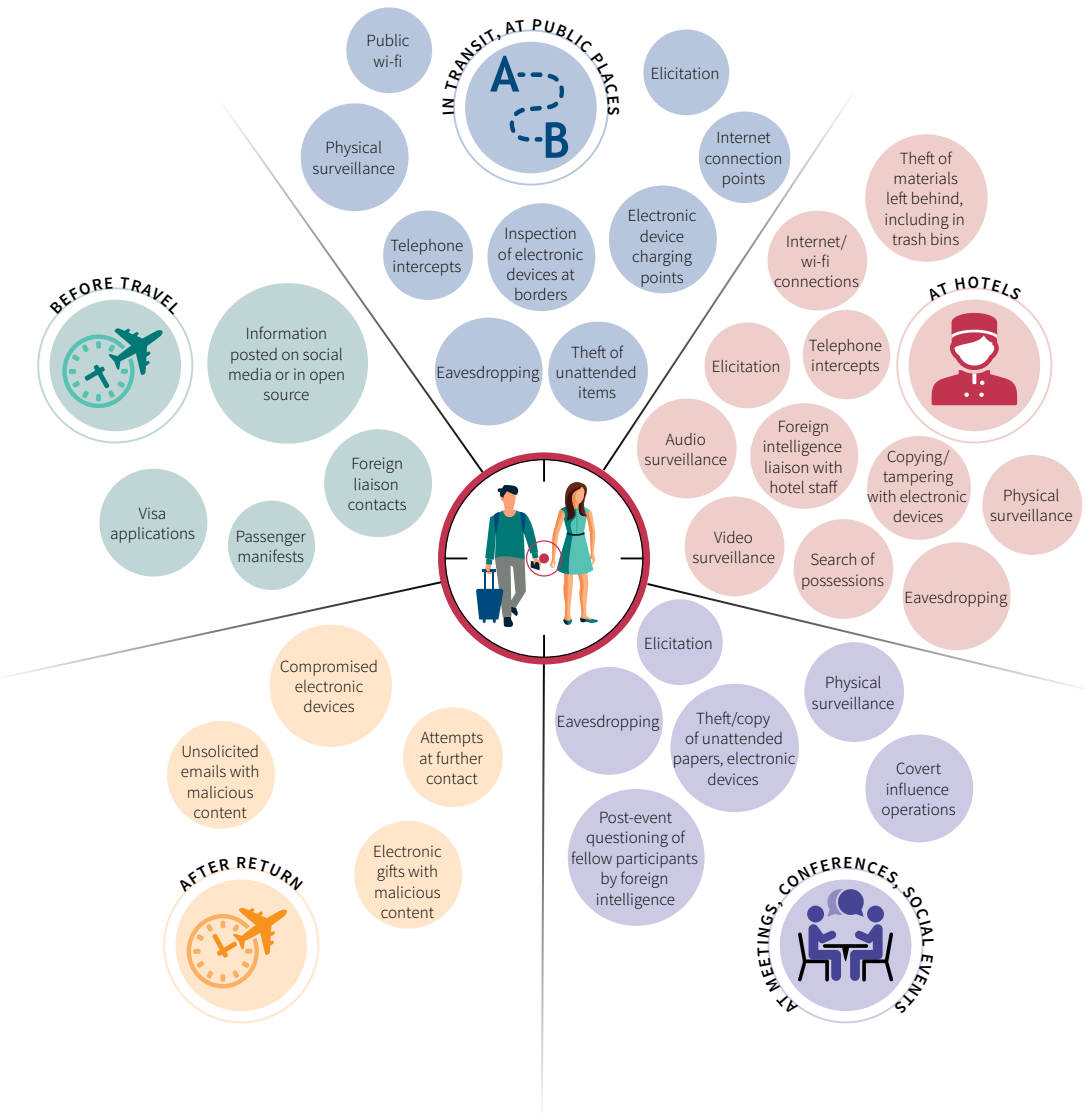
Before you book any overseas business travel, check with your workplace security team for advice about your destination/s—your team may have access to ASIO's assessments about the threat to Australian interests for each country, including the threat from foreign intelligence services. Also, visit Smartraveller (www.smartraveller.gov.au) for current travel advice about your destination/s. We recommend you subscribe to Smartraveller (a free service) to receive travel updates while you're travelling.

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).

Ask your workplace security team about your workplace's security expectations, and who to contact and what to do if you have security concerns during your travel. 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.

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 practice good security—foreign intelligence services 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

- Don't take classified material with you. If you absolutely need to take classified material, ensure you handle it correctly by only storing it in approved containers and managing the access to these containers.
- 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

The Australian Cyber Security Centre (ACSC) advises that Australian electronic devices are routinely targeted during overseas travel—it is a real and persistent threat. Ask your security team about this—or look at the ACSC’s recommendations about securing electronic devices before, during and after you travel overseas. These include:


- 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.
- Never pack electronic devices (including multi-factor authentication tokens) in checked-in luggage.
- Don’t leave electronic devices unattended in hotel rooms or hotel safes—keep them with you or within sight at all times.
- Don’t connect to open or untrusted wi-fi networks—use secure networks or Virtual Private Network (VPN) connections.
- Disable capabilities such as mobile data, wi-fi and Bluetooth when not in use—be aware devices in flight mode are still vulnerable to compromise.
- Be careful when charging. Only use your own chargers and cables that are specific to your device—don’t use charging stations or USB outlets.
- Power down and isolate from electronic devices when you’re having sensitive conversations.
- Be discreet when using your devices. Ensure that no one can observe your passwords and activities—including between plane seats or through windows.
- 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.
- Encrypted apps and devices are not secure—technical collection and eavesdropping can still occur.



Know when to say ‘no’

When you travel overseas for official government or business purposes, your hosts may offer you hospitality and gifts. In some cases, this can be normal and does not pose a threat. In other cases, where your hosts make persistent or excessive offers, it may be an attempt to gain your favour, create a sense of obligation, or test your willingness to help a foreign intelligence service. Some gifts can be modified to contain listening devices and electronic gifts can be designed to execute malicious code if connected to other devices or workplace network/s.

Follow your workplace’s policy for managing hospitality and gifts. If you’re uncertain, use your judgement to decide whether an offer seems more generous than it should for a typical, professional relationship—and speak with your security team for further advice. ASIO recommends you do not accept electronic gifts. However, if you have to accept electronic gifts, make sure they are isolated from areas where sensitive conversations are held, and then destroyed—discuss secure disposal options with your workplace security team.



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



*Trust your instincts.
If something seems
slightly off, report it.
Your observations or
experiences could
help identify a
wider pattern.*

What to do after you go

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 foreign intelligence services, including how these services target government personnel, information, and facilities.

Security clearance holders must report through the CRS any behaviour, activities or approaches that seemed suspicious, unusual or persistent, and the details of any foreign nationals who seek to establish social contact outside official meetings and/or who become ongoing professional or personal contacts. You don't need to report ongoing professional contact as part of official engagements if a formal corporate record of the conversation/engagement is produced. You should also report people who tried to access or obtain information—or access places—that they shouldn't have.

Government personnel (including staff and contractors) and **security clearance holders** can report to their workplace security team, who can submit a contact report on your behalf. Alternatively, you can email a contact report directly to ASIO at cr@asio.gov.au.

Non-government personnel and **non-security clearance holders** are strongly encouraged to report as well. Reports can be made to a workplace security team, or directly to ASIO via the Notifiable Incidents, Threats or Reportable Observations (NITRO) portal at nitro.asio.gov.au.

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