
Australian Government
Australian Security Intelligence Organisation
NITRO
REPORT
PRYING
MINDS
Foreign spies are targeting Australia's defence industry
Help protect our national security—*secure what you know with NITRO*
ASIO
Be aware
Be discreet
Be responsible
nitro.asio.gov.au

Foreign spies are aggressively targeting Australia's defence industry—'the workforce behind the Defence Force'—to steal sensitive defence-related research, development and product designs.

Any compromise of defence industry by these 'prying minds' could result in Australian companies losing unique intellectual property and commercial advantage. It also puts Australia's national security at risk. A suspicious approach could be the beginning of an act of espionage or foreign interference. If you experience a suspicious approach, report it via ASIO's online contact reporting portal—NITRO.

Why the defence industry?

Foreign spies want to steal Australia's defence-related research, development and product designs to manufacture their own versions for profit, and to gain military advantage.

These 'prying minds' also want to steal Australia's defence-related research, development and product designs so they know how to counter these technologies in the event of a conflict—and they may even boost their own militaries with the same technologies.

Defence industry partners, from small operators to large defence primes, hold information that is valuable to foreign spies; these spies will steal from Australia to advance their nation's interests at the expense of ours.

What does foreign intelligence targeting look like?

Foreign spies are proactive, creative and well resourced. They are also opportunistic. They are looking for small lapses in security practices—such as lax visitor-escorting policies or poor security controls in offices—that allow them to gain access to restricted areas. They might take photographs, or look through papers that have been left out.

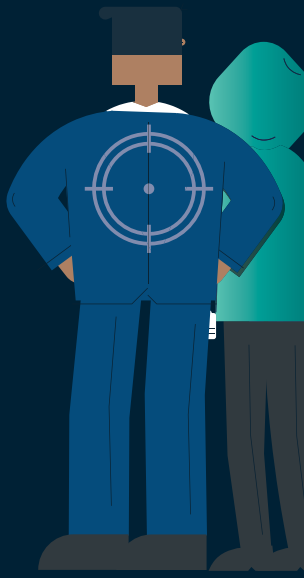
Foreign spies are persistent. They will often show an unusual level of interest in your work, and ask detailed questions about it—including what type of projects you are working on, and who else is working on them.

Foreign spies are looking to co-opt or coerce defence industry employees—or their contacts—to help them steal information. They are looking for individuals who work in sensitive areas—individuals who might be willing to work for them, or those who might be susceptible to being pressured to work for them.

Foreign spies might make one-off approaches or they might cultivate a person over time. So what do these approaches look like?

Sometimes it could be a colleague at a training course asking you about your work—at a level of detail that is suspicious. At other times, it could be a professional relationship or a friendship that has developed over time—that starts to take a suspicious turn when it includes unusual requests for access to people or information.

Foreign spies might also make approaches online—particularly through social media—or in person, or use a combination of these approaches.



WHAT

could make you susceptible to approaches by foreign spies?

- being stressed about personal or financial matters
- getting into situations where sensitive material could be easily compromised
- being concerned about the safety of family members

WHERE

could foreign spies target you?

- at social, religious or other gatherings
- through dating or other social media platforms
- through seemingly benign or coincidental interactions

HOW

can foreign spies coerce you into providing them with information?

- by creating a sense of personal connection or obligation
- by making you feel a sense of indebtedness
- by providing you with financial incentives, gifts, networking opportunities, or preferential access

To help you recognise the approaches you should report, remember the acronym 'SOUP' and these examples.

Suspicious You receive a social media request from a foreign national you've never met or heard of before, and they have an extensive list of foreign contacts, none of whom you know.

Ongoing You meet someone in an official capacity and they contact you afterwards to continue the association, either officially or unofficially.

Unusual You receive an unsolicited email from a professor in another country asking you to host a visiting scholar while they work with you for a period of time.

Persistent You attend a weekly social gathering where someone repeatedly asks detailed questions about your work duties.

What can you do to mitigate the foreign intelligence threat?

Advice for individuals

Be aware of the information you share online

- Limit and regularly audit what personal and professional information is available about you online.
- Review your social media and other online security settings to limit who can access your information.

Protect yourself—in Australia and overseas

- Where possible, do not take personal electronic devices overseas. Instead, consider taking a separate device with limited information on it that you format when you return.
- Do not discuss sensitive or classified information in non-secure areas.
- Do not leave electronic devices or sensitive documents unattended—including in hotel safes.

Report suspicious approaches

- Report to NITRO any suspicious approaches you experience or observe while overseas or on your return.

What can you do to mitigate the foreign intelligence threat?

Advice for security managers

Be aware of the information you share online

- Sensibly limit how much information the company provides on its website, especially in regard to which projects the company is undertaking and who is involved.

Promote a security culture

- Show that you value good security practices—help staff to identify security breaches, and encourage them to report any security concerns they may have.
- Regularly review your employees in terms of their suitability to hold a security clearance—identify any sudden changes in their personal circumstances and/or behaviour.
- Ensure that your security clearance holders adhere to their obligations—for example, by using the Contact Reporting Scheme.

Promote IT security

- Conduct regular security training and refreshers for staff—emphasise their IT security responsibilities.
- Regularly update software and apply patches to company IT devices.
- Immediately report any unusual activity occurring on company IT devices.

Encourage staff to report suspicious approaches

- Encourage your staff to report to NITRO any suspicious approaches they experience or observe—in Australia or while overseas.

What can I do if I experience a suspicious approach?

The Notifiable Incidents, Threats or Reportable Observations (NITRO) portal is a secure online tool to report concerns, directly to ASIO, about espionage, insider threats or foreign interference. NITRO is specifically designed for defence industry personnel—especially non-clearance holders.

Incidents to report could include suspicious approaches in person or online, or persistent and unusual questioning—either targeted at you or someone you know. Reportable incidents also include any contact with a foreign national that seems suspicious, unusual or persistent in any way, or that becomes ongoing. In addition, you should submit a NITRO report when a person or group, regardless of nationality, seeks to obtain information they do not need to know.

For more information on how these incidents may look or feel, what you can do to report them, and how this could help protect Australia's national security, visit nitro.asio.gov.au.

ASIO also recommends raising your concerns with your organisation or agency's security adviser, if you have one. They need your information to do their job.

The callers used multiple fake identities and asked for different people each time

Case study 1

In early 2020, over several weeks, a number of unknown callers contacted an Australian defence industry company, asking to speak with personnel involved in a sensitive capability development project. The callers requested some personnel by name. If the employee requested was not available, the callers asked for details of other employees they could contact about the project. The callers used multiple fake identities and asked for different people each time, attempting to map out which key individuals were involved in what critical aspects of the development project. Fortunately, staff followed their company's internal security policy and didn't provide personal information to unannounced callers, and the company was able to identify the attempted organisational mapping activity early. Staff reported the incidents to their company's security team, which then reported the incidents to ASIO. This mitigated the harm before it was allowed to occur.

This example shows how easily 'prying minds' can exploit information through open channels to draw deeper conclusions about personnel involved in developing Australian defence capabilities, including sensitive projects.

Case study 2

Foreign intelligence services are attracted to public events that showcase defence industry capabilities or offer networking opportunities, as they can use these events to target defence industry personnel.

During a public cyber security event in 2019, a 'prying mind' approached a defence industry employee. She showed undue interest in the employee, feigned unfamiliarity with the topics being discussed and asked numerous questions. She then persuaded the defence industry employee to plug a USB thumb drive into his personal laptop, which contained sensitive research notes and personal information. When the defence industry employee left the event, the 'prying mind' followed him to the car park and continued to ask suspicious questions about his work, workplace, education and personal life. She asked for a lift home from the event and attempted to establish ongoing contact with the defence industry employee. After the incident, the employee reported the behaviour as suspicious and unusual.

Later in 2019, at a separate public cyber security event, the same 'prying mind' approached another defence industry employee and asked probing questions about their full name, employment, background, projects they worked on with the Department of Defence and contact details. The 'prying mind' suggested to the employee that they socialise outside the event.

This example demonstrates how 'prying minds' can seek to form a relationship with someone by exploiting that person's willingness to help others and, in doing so, gain access to devices and sensitive information. It also shows the value of the reporting process. As both defence industry employees reported these incidents, ASIO was able to link them and gain a better understanding of foreign intelligence targeting and the overall intelligence picture.

She showed undue interest in the employee, feigned unfamiliarity with the topics being discussed and asked numerous questions

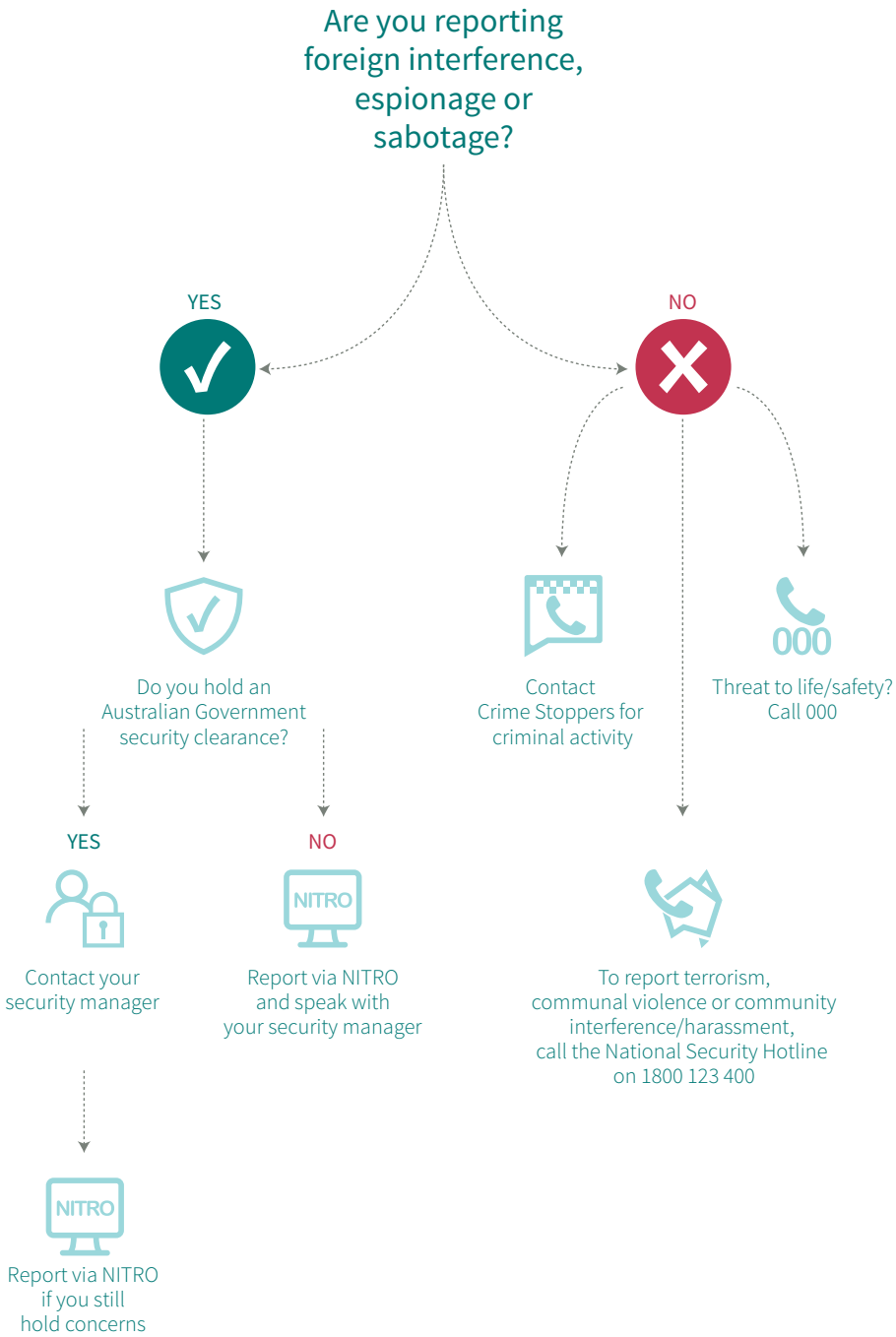
When should I use NITRO?

If you're unsure whether a particular security incident meets the criteria, report it anyway.

ASIO relies on reports from NITRO and the Contact Reporting Scheme to build a picture of how foreign spies are working in Australia. Your piece of information may be the piece of the puzzle we need to uncover a foreign spy network, or operation.

Australian Government clearance holders are required to report any contact with foreign nationals that is suspicious, unusual, persistent, or ongoing—regardless of whether the contact is social or official, in Australia or overseas. If you're a clearance holder and you identify a contact or security incident of concern, continue using the Contact Reporting Scheme. This means submitting a contact report to your agency security adviser (or equivalent).

Concerns that do not relate to espionage or foreign interference should be reported through existing reporting channels—report threats to life to local police, other criminal matters to Crime Stoppers, and information about a possible terrorist threat to the National Security Hotline.


Are you reporting foreign interference, espionage or sabotage?
YES
NO
Do you hold an Australian Government security clearance?
Contact Crime Stoppers for criminal activity
000
Threat to life/safety? Call 000
YES
NO
Contact your security manager
NITRO
Report via NITRO and speak with your security manager
To report terrorism, communal violence or community interference/harassment, call the National Security Hotline on 1800 123 400
NITRO
Report via NITRO if you still hold concerns

Be aware
foreign spies are targeting Australia's defence industry

Be discreet
don't divulge too much information—either in person or online—
about what you're working on or who you're working with

Be responsible
if you see something suspicious, it could be the beginning of an act
of espionage or foreign interference—so report it via NITRO

Secure what you know with NITRO

ASIO

nitro.asio.gov.au