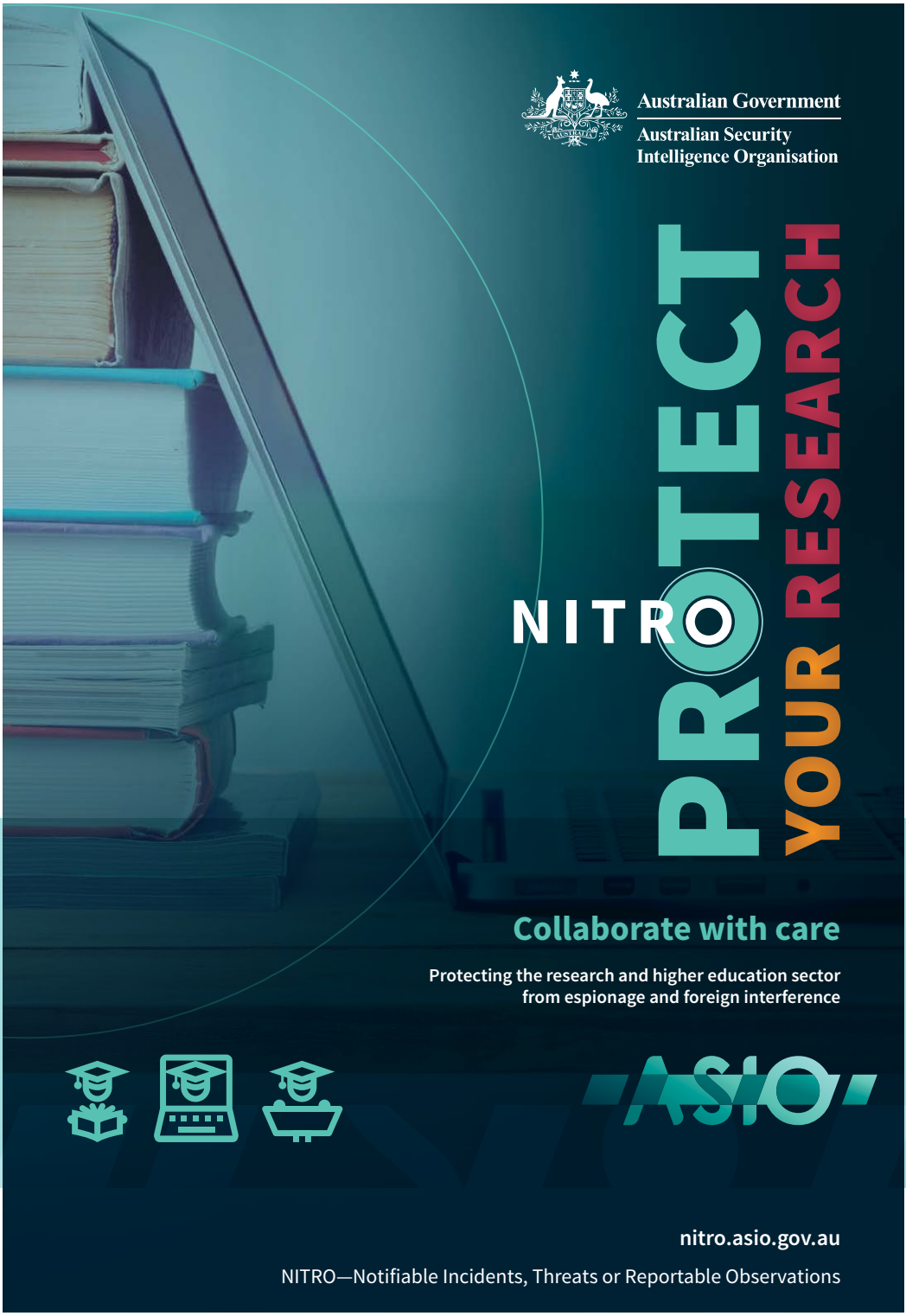


Australian Government
Australian Security Intelligence Organisation

NITRO PROTECT YOUR RESEARCH

Collaborate with care

Protecting the research and higher education sector from espionage and foreign interference

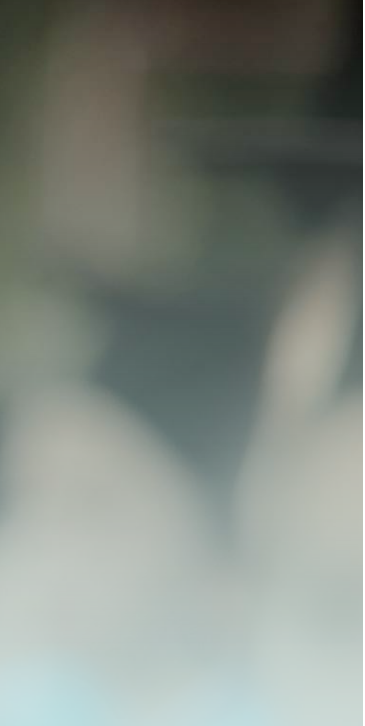
ASIO

nitro.asio.gov.au

NITRO—Notifiable Incidents, Threats or Reportable Observations

Academic environments worldwide depend on researchers being collaborative, with the productive exchange of information being key to intellectual and scientific progress. However, many foreign governments and their intelligence services attempt to exploit this collaborative environment to acquire information and technology to their benefit, and to your—and Australia's—detriment.

Australia is the target of sophisticated and persistent espionage and foreign interference activities from a range of nations. Academic and research institutions are a particular target of these activities because of your success: you are world leaders in developing cutting-edge technology and innovative research to address the global challenges Australia faces.



How espionage and foreign interference could affect your institution and your career

As the Director-General of Security, Mike Burgess, stated in his Annual Threat Assessment in 2023, Australia is facing an unprecedented challenge from espionage and foreign interference.

While the espionage threat is well known—it involves **foreign powers and their proxies** seeking to steal national security, economic or other information—foreign interference is a more nuanced activity. All foreign states seek to influence matters of importance to them. However, when this activity is carried out covertly by or on behalf of a foreign power, and is contrary to Australia's sovereignty, values and national interest, it becomes **foreign interference**.

Espionage and foreign interference can negatively impact your institution—and your career—in a number of ways. For example, if a foreign researcher accesses and publishes your unpublished research or data, it can deprive you of the opportunity to publish and commercialise your work, and could make it more difficult for you and your institution to attract funding in future.

However, even legitimate academic engagement with partners can cause damage to the national interest and present a national security threat. For instance, if it results in the inadvertent transfer of sensitive science and technology research, expertise and/or data to a foreign power. This is particularly the case if the research or data relates to dual-use technology or military capability.

What are foreign powers and their proxies?

Foreign powers are foreign governments, entities under their direction or control, or foreign political organisations working to undermine Australia's national security or advantage a foreign power. For example:

- Foreign governments are the central political and executive bodies that direct, authorise and oversee the policies and activities of foreign countries.
- Foreign intelligence services are the formal military or civilian arms of foreign governments that collect information and undertake acts of foreign interference, espionage or sabotage.
- State-owned enterprises are corporate enterprises, but largely under the control of a foreign government. Given the level of control the foreign government can exert over these companies, they can be used to undertake acts of foreign interference, espionage or sabotage on behalf of the foreign country.

Foreign proxies are individuals or entities that collaborate with or are used by a foreign power to undertake acts of foreign interference, espionage or sabotage. They may not be under the formal control of the foreign government.

Research areas being targeted

Foreign powers and their proxies are most likely to target areas in which Australia has particular **technology or research strengths**, including how these are applied by Australian industry. Australian research is particularly strong in areas such as medical and health sciences, biotechnology and engineering. The strengths of these areas are in both the quantity and quality of cutting-edge research (measured in numbers of researchers and publications, and their influence) and in the degree of commercialisation of this research (measured in number of patents and income generated). **These areas of excellence in Australian research are likely to be attractive to foreign states.**

For further guidance on the types of critical technology or dual-use research that are desirable to foreign powers and their proxies, refer to the Australian Government's ***List of Critical Technologies in the National Interest****.* ***www.industry.gov.au***

However, the threat to Australian research goes beyond critical technology: foreign powers and their proxies may attempt to interfere with any academic activity they see as threatening their interests. For example, they may try to shape academic inquiry, language or course content to reflect their preferred narratives and silence dissenting views—by exerting pressure on individual researchers, professional staff and students, both online and in person.

How foreign powers or their proxies may approach you

Foreign powers and their proxies can ***try to mask their activities*** *in a variety of ways, including by pretending to be* ***journalists, academics, industry figures or members of think tanks****.*

Or they may be legitimately employed as journalists or academics, and conduct other intelligence activities at the same time.

So, at first glance, an approach from foreign powers and their proxies **may be indistinguishable from normal business relationships, networking opportunities or requests for academic collaboration**.

Suspicious approaches could include:

- receiving **requests to collaborate** on research with foreign institutions or researchers in areas that are **associated with critical technology or are politically sensitive**;
- receiving **unsolicited requests**—including from foreign diplomats—for your **expert opinion**;
- receiving **financial donations** from foreign or foreign-linked entities—they can be trying to gain access to or influence sensitive research or research personnel;
- **unusual, unsolicited, or persistent attempts** to access research papers or material, including unpublished data;
- **invitations—both solicited and unsolicited**—to participate in **international conferences**, which may include excessive offers of hospitality or gifts, such as all-expenses-paid trips; and
- **foreign delegations** wanting to enter sensitive research facilities, such as laboratories, for tours or meetings.

While these types of approaches can often represent genuine academic engagement, they can also be attempts by foreign agents or their proxies to gain access to Australia's sensitive or classified information, to facilitate technology transfer and/or to steal Australia's and your institution's intellectual property.

How you can protect yourself—advice for individuals

The threat is sophisticated but there are things you can do about it

- **Be alert to the threat** and recognise the **value of the information and access you hold**.
- **Be aware, be discreet and be responsible** about what you post online or discuss in public—and with whom. Without knowing it, you may reveal sensitive information about yourself, your research or your institution, which malicious agents can use to target you and your institution. Consider whether your research has sensitive aspects that should not be discussed online.
- **Conduct thorough due diligence** before collaborating with international partners and adhere to your institution's policies. Refer to the **ASIO Due Diligence Integrity Tool** for guidance, which is available to subscribers of the ASIO Outreach portal. Apply for access at **asio.gov.au/outreach**.
- **Maintain optimal IT security practices at all times**, with strong passwords and secure devices.
- **Take precautions when studying and researching overseas** to protect yourself and your institution (refer to the ***Students and researchers travelling overseas are being targeted*** section of this booklet on p.10 for more information).
- **Report any security concerns you have**. Something that seems minor could turn out to be major. Reporting can help your institution and the Australian Government discover and counteract hostile activity before harm occurs (refer to the ***How to report security concerns*** section of this booklet on p.22 for more information).

How you can protect your institution—advice for administrators and security managers

Promote a security culture within your institution

- **Deliver induction training** that raises staff awareness about the threat of espionage and foreign interference to research and the sensitive information your organisation holds; particularly for staff who work in critical or dual-use technology, or on politically sensitive topics.
- Show that you **value good security practices**—help staff identify potential security concerns in their research or on campus, and encourage them to report these.

Collaborate with care

- Develop a policy that clearly **defines which research areas and international partners are regarded as higher risk**, and use enhanced due diligence processes to protect these collaborations as a priority.
- Ensure that any collaborative research adheres to **Australian Government requirements**, such as Defence Export Controls or the Australian Foreign Relations Act.
- Require your staff—particularly those who work on critical or dual-use technology or on politically sensitive topics—to regularly **declare any foreign affiliations or financial interests** that could compromise their work.

Consider how much sensitive information your institution shares online

- Publicly promoting your institution's research is an important part of academic life. However, foreign powers and their proxies can use this information to identify researchers working on critical or dual-use technology and target them to acquire it. Where possible, create policies that sensibly **limit how much of this information is shared online**.

Ensure robust IT and physical security

- Schedule regular **security training and refreshers** for staff—emphasise their IT and other security responsibilities.
- Train staff to identify **common social engineering techniques** and **spearphishing emails**, which can be used to facillitate a cyber attack.
- Implement IT and physical security access controls that **limit who can access sensitive information and areas**, so that if a security incident occurs, you can easily identify who has accessed information and when.
- Regularly **update** software and **patch** company IT devices.
- Immediately **report** any unusual activity occurring on your IT networks or devices.

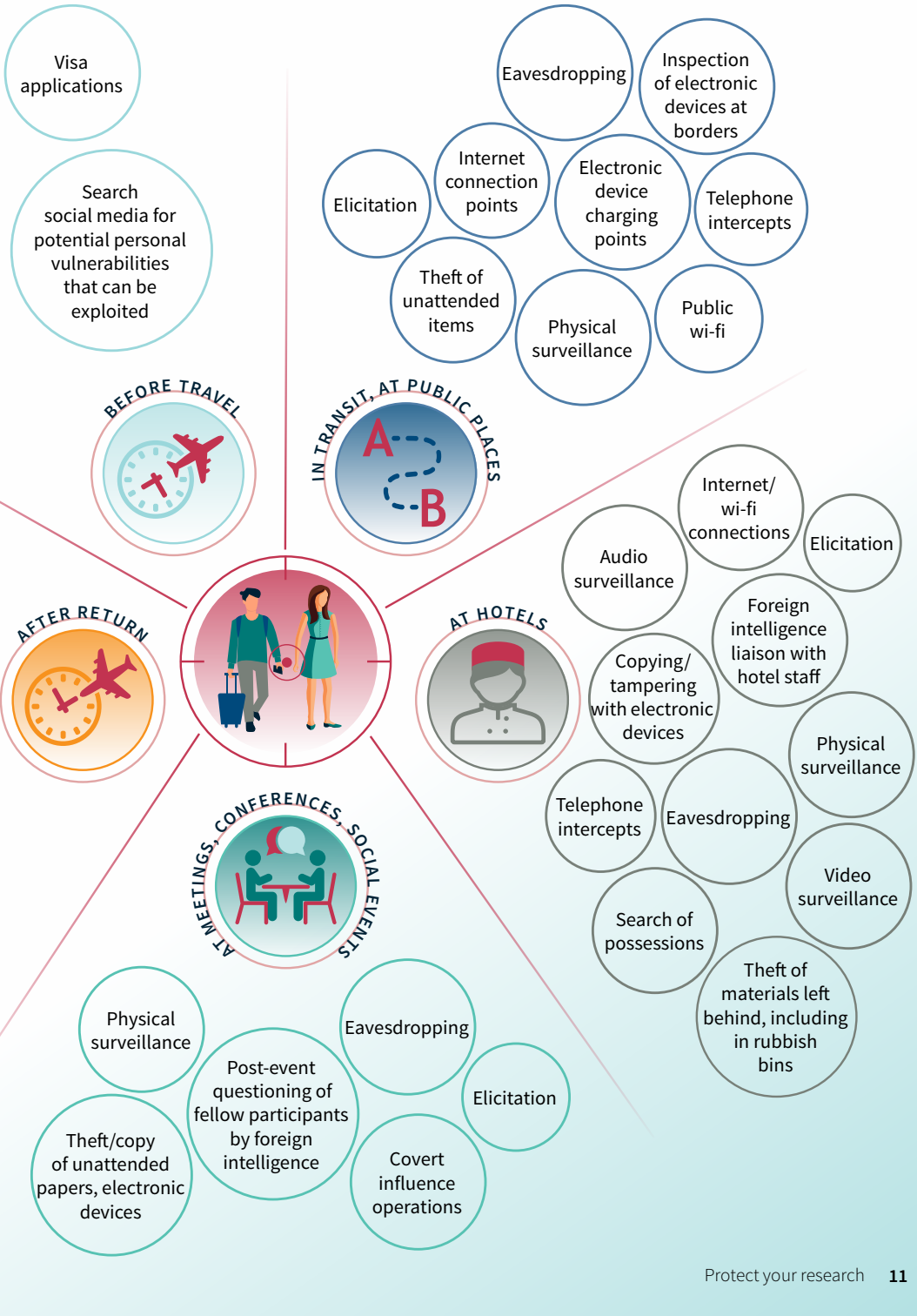
Students and researchers travelling overseas are being targeted

Foreign powers and their proxies have a long history of targeting students and academics to meet their intelligence requirements. The open and collaborative nature of higher education institutions can allow them to:

- identify students or researchers who can help them gain access to information or people they are interested in—either now or in the future;
- initiate relationships with students or researchers for seemingly straightforward reasons—such as job or internship opportunities, paid paper-writing engagements, language exchanges and cultural immersion programs; and
- ask students or researchers—once relationships have developed—to perform tasks and provide information (not necessarily sensitive or classified) in exchange for payment or other rewards, with demands slowly increasing over time.

However, foreign powers and their proxies have far greater powers in their own country. Students and researchers travelling, working and studying overseas are therefore particularly attractive to foreign powers and their proxies.

How security can be compromised—and how you can protect yourself—before, during and after travel


Visa applications
Search social media for potential personal vulnerabilities that can be exploited
BEFORE TRAVEL
Eavesdropping
Inspection of electronic devices at borders
Internet connection points
Elicitation
Electronic device charging points
Telephone intercepts
Theft of unattended items
Physical surveillance
Public wi-fi
IN TRANSIT, AT PUBLIC PLACES
A
B
Internet/ wi-fi connections
Elicitation
Audio surveillance
Foreign intelligence liaison with hotel staff
AT HOTELS
Copying/ tampering with electronic devices
Physical surveillance
Telephone intercepts
Eavesdropping
Video surveillance
Search of possessions
Theft of materials left behind, including in rubbish bins
AFTER RETURN
AT MEETINGS, CONFERENCES, SOCIAL EVENTS
Physical surveillance
Eavesdropping
Post-event questioning of fellow participants by foreign intelligence
Elicitation
Theft/copy of unattended papers, electronic devices
Covert influence operations

How to protect yourself and your research when you are travelling overseas

Be aware of the threat from foreign powers and their proxies, and adhere to basic personal security practices, as outlined below.

Before you travel:

- Ask your security manager about the security environment in your destination.
- Subscribe to DFAT's Smartraveller service for email and SMS updates on your destination.
- Ask your head of department if any research areas are off-limits for discussion while overseas.
- Think about the personal information and research data you're carrying with you—perhaps on a USB, or your phone or laptop. If you're carrying research that is sensitive, or off-limits for discussion while overseas, consider leaving it behind in Australia.

While you are overseas:

- Be sceptical about opportunities that seem too good to be true.
- Before accepting offers from foreign governments—such as all-expenses-paid study tours or immersion programs, conference opportunities or paid report writing—consider whether they might come with strings attached in terms of future obligations.
- Be wary of foreign contacts who show undue interest in your personal or family background and your career plans—particularly if you're interested in working in sensitive government or defence-related positions in the future.
- Be careful about accepting USBs and other electronic devices, including when they are offered as gifts, and do not plug them in to personal or sensitive computer systems; these could contain malicious software that allows others to remotely access your devices.
- Be wary of requests for odd or overly specific personal or professional information during social contact and/or attempts to contact you outside official academic channels. These may indicate someone is collecting information for intelligence activity.
- Maintain detailed records of any financial compensation you receive from foreign organisations, and any groups or associations you join while you're overseas.

When you return home:

- Reset passwords or PINs for all accounts you accessed when you were overseas.
- Report any suspicious activity or ongoing contact to your program coordinator and security manager.
- Report any attempts by foreign nationals to contact you that seem suspicious or overly persistent.

How to manage visitors and delegations from overseas

Australian research and higher education institutions frequently host visitors and delegations from overseas. These visits allow researchers to present their work to an international audience, and can lead to productive and profitable exchanges that contribute to the intellectual life of their institutions and Australia's national interest.

However, when hosting guests, be aware that foreign powers and their proxies—including those that have an otherwise positive relationship with Australia—can use this opportunity to illegitimately acquire sensitive Australian research and intellectual property, and influence your institution's business decisions in their interests. Foreign intelligence services are known to use delegations as cover, and to task delegates to collect intelligence on their behalf.

A strong security culture is the most effective way to defend your research and institution against the threat of espionage and foreign interference. A strong security culture is one in which your people understand the value of the information they hold and the assets and places they have access to—and how to protect them.

Before you host visitors and delegations from overseas:

- Develop a plan—in consultation with your institution's security team—that anticipates and manages any security threats that may arise during the visit.
- Ensure you have a complete list of visitors before the event, and be aware of attempts to add or substitute visitors—such as translators—at the last minute. When delegations try to bring an unannounced visitor, late-notice substitute or extra member, this person may be an intelligence officer.
- Discuss with your security team which information, systems and premises visitors can access. Decide which sensitive research should not be discussed with visitors, and what measures your institution can take to restrict visitor access to sensitive systems and premises.
- Ensure you have enough security escorts for the number of visitors you expect, and make it easy to identify visitors by having them wear a special lanyard or visible access pass.
- Ensure that delegates are escorted at all times: to and from meeting rooms, bathrooms, dining facilities and smoking areas.

Before you host visitors and delegations from overseas: (continued)

- Make sure that hosts and security escorts know what your institution considers inappropriate visitor or delegate behaviour. Similarly, ensure you brief visitors on what you expect of them during functions or engagements.

- Empower hosts and security escorts to challenge visitors who are behaving inappropriately. Make hosts aware that members of delegations may attempt to breach security protocols on the assumption that they'll be safe from being challenged by hosts who don't want to offend them.
- Don't plan meetings or engagements in active work areas, particularly if sensitive research is conducted in these areas.
- If it is unavoidable to bring visitors through a work area, ensure that staff are pre-warned about delegation visits to their work areas, so that no sensitive material is left on desks or screens, and that discussions are circumspect.
- Ensure visitors do not bring electronic equipment, such as mobile phones, cameras, other recording devices or other USB devices (chargers, scanners, Wi-Fi and Bluetooth adaptors, DSL modems etc.) into sensitive areas of your institution.
- Consider deactivating network ports and wi-fi if meetings or engagements are to be held in active work areas. Foreign delegates have been known to attempt to insert USBs into computer systems to extract information and introduce malware.

- Have an institutional policy for dealing with gifts from foreign delegations. Ensure that any gifts you receive are not kept in sensitive work areas. Gifts from foreign delegations have been used to conceal recording devices to collect and exfiltrate information. Destroy any electronic gifts, including cables and power adapters—do not connect them to any organisational or personal devices or networks.
- Meet with your security team and security escorts for a post-visit 'wash-up' to discuss the visit and any security lapses the team identified—your goal is constant improvement in managing visitors and foreign delegations to mitigate against espionage and foreign interference.


Tetra Pak

Case study 1: stolen research = lost intellectual property + lost revenue

The Department of Electrical and Computer Engineering at Duke University in Durham, North Carolina, is a world-leader in the research of metamaterials—artificial materials with properties not found in nature, which are used in high-end medical devices, smart solar power management and battlefield communication.

In January 2007, a foreign PhD student in the department arranged for a research team from his home country to visit Duke. Foreign researchers toured a laboratory in the engineering department, and photographed key pieces of equipment, including research prototypes. According to the FBI, the entire lab was then reproduced in the foreign country.

In 2010, the foreign PhD graduate returned to his home country and started his own lab using research pioneered at Duke. The foreign researcher later commercialised this research, and founded a company that as of 2017 was valued at US$1.7 billion.

The theft of this research and its replication overseas meant that the Duke researchers were not able to commercialise what they had created, and Duke University missed out on associated revenue.

This case study demonstrates the importance of physical security practices in preventing technology transfer.

- *Who has access to your institution's research labs?*
- *Who can invite and escort guests within restricted facilities at your institution?*
- *How is this access controlled—and can it be audited if your research or systems are compromised?*

Case study 2: no such thing as a free lunch

In 2021, representatives of an Australia-based foundation—backed by a wealthy foreign-based business figure—approached an Australian university and offered to pay all expenses for a dinner to commemorate the diplomatic relationship between the Australian Government and the business figure's home country.

When staff conducted basic due diligence on the foundation by searching online, they discovered the business figure had been linked to multiple accusations of bribery and corruption internationally.

When staff discovered these accusations, they recommended the university not proceed with the collaboration, as it could potentially be an avenue for foreign interference, and cause reputational damage to the university.

Donations can be a vector for foreign inference: foreign-linked entities can use donations to gain access to senior staff and key decision-makers, and influence the institution's business decisions and the direction of research in a way that benefits a foreign country.

- *What is your institution's policy for accepting donations from foreign-linked entities and individuals?*
- *What due diligence does your institution conduct before accepting donations?*
- *What restrictions does your institution place on foreign entities and individuals that have donated funds when it comes to influencing business decisions and your research?*

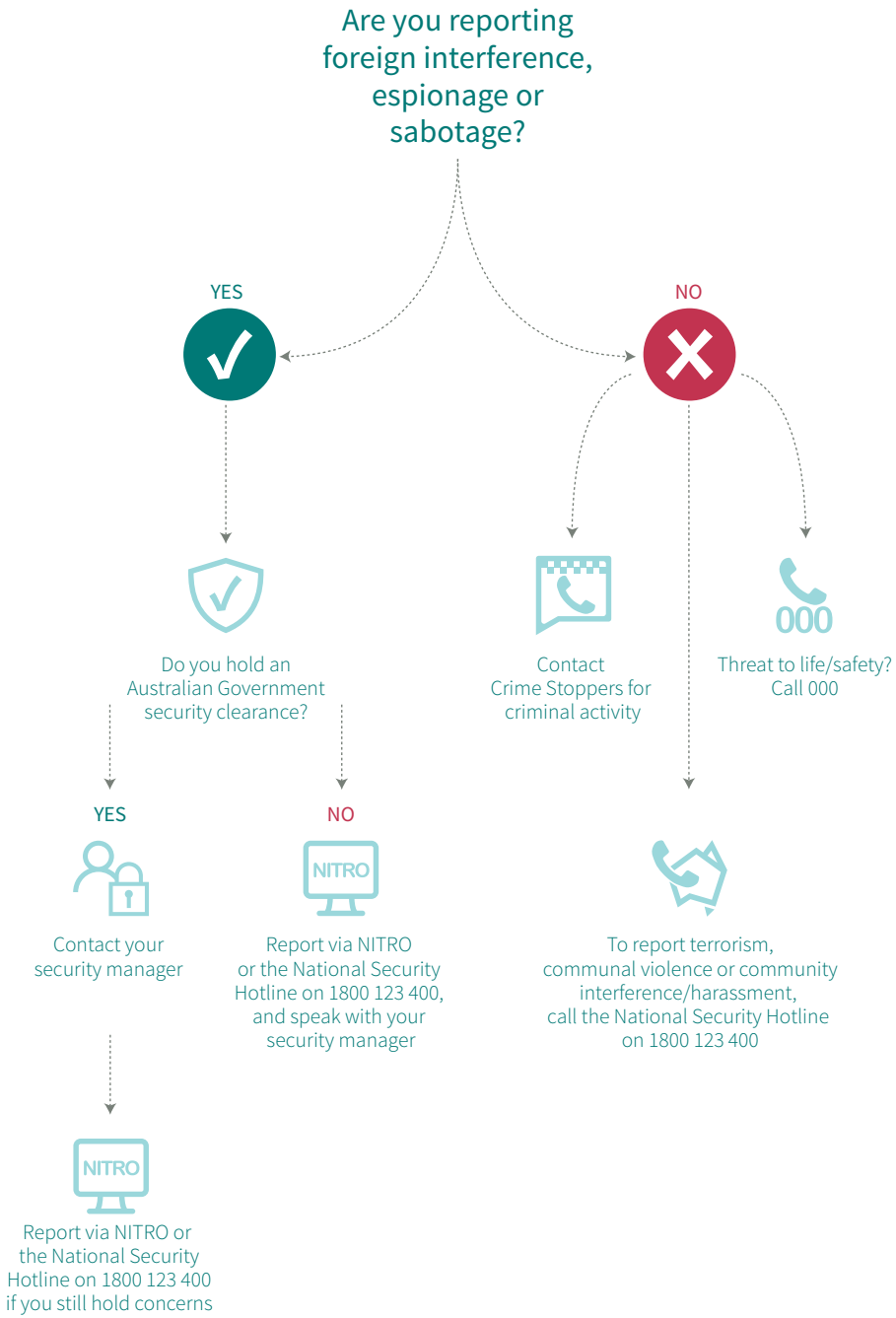
How to report security concerns

Reporting security concerns assists your institution and the Australian Government to discover and defend against hostile activity before major harm occurs.

You can report espionage or foreign interference concerns directly to ASIO through the **Notifiable Incidents, Threats or Reportable Observations (NITRO)** secure online portal. The types of incidents you might report include suspicious approaches in person or online, or being questioned in a persistent and unusual way about specific aspects of your work, workplace or colleagues.

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**.

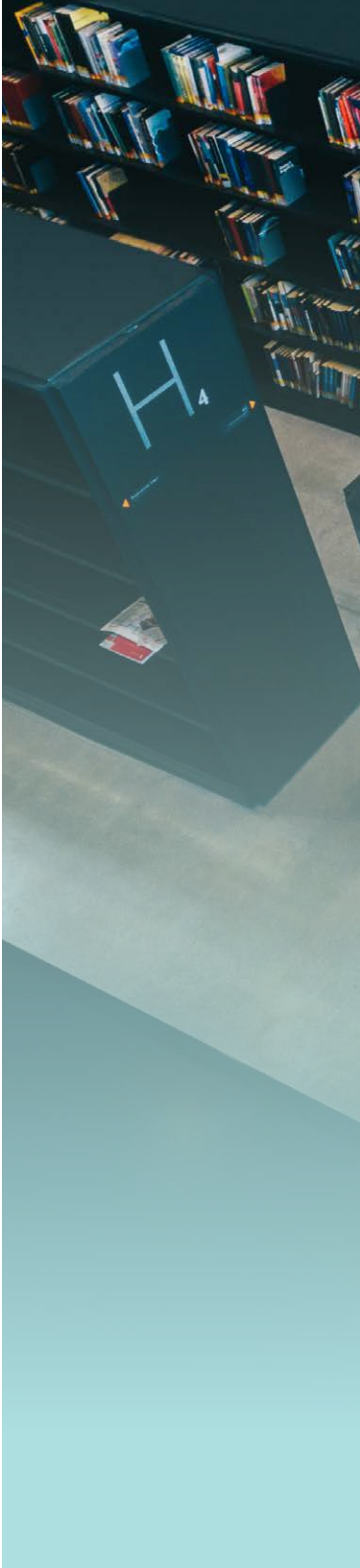
ASIO also recommends that you raise your concerns with your security manager, if you have one. They need your information to do their job.


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 or the National Security Hotline on 1800 123 400, 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 or the National Security Hotline on 1800 123 400 if you still hold concerns

Where to find more information

Being security aware and setting up good personnel, information and physical security practices are essential to countering the threat from foreign powers and their proxies. If you need more information about promoting a strong security culture in your institution, we recommend these resources:

- **Think Before You Link** is an ASIO campaign that raises awareness of the threat from malicious social media profiles. It provides guidance on how to avoid being targeted through professional networks and other online platforms. For Think Before You Link materials, visit **asio.gov.au/TBYL**
- **ASIO Outreach** provides advice to research and higher education institutions on current and emerging security threats, and on how to design and apply security policy. The Outreach portal contains intelligence reporting to help eligible subscribers make informed decisions about mitigating security threats and managing risk. To request access, visit **asio.gov.au/outreach**
- The **Australian Cyber Security Centre** provides cyber security advice, including prioritised mitigation strategies, guidance on the 'Essential Eight', and cyber supply chain risk management—this information is available at **cyber.gov.au**
- Through the **University Foreign Interference Taskforce**, the Australian Government is working together with the research and higher education sector to enhance protections, while preserving the openness and collaboration that is crucial to the success of Australia's world-class university system. For more information, visit **www.education.gov.au** or the Counter Foreign Interference Coordination Centre in the Department of Home Affairs—**www.homeaffairs.gov.au**
- The Australian Government's list of ***Critical Technologies in the National Interest*** captures current and emerging technologies that are important to Australia's national security, social cohesion and economic prosperity. It is available at **www.industry.gov.au**



Disclaimer

The information provided in this document is intended to be used as general guidance only and is not provided for any other purpose. In particular, it is not intended to provide comprehensive advice on its subject matter or in relation to any particular product, and should not be relied upon as providing such advice. Organisations or individuals using or relying upon this information are deemed to do so in conjunction with their own judgement and assessment of the information in light of their particular needs and circumstances.

Secure what you know with NITRO

ASIO

nitro.asio.gov.au