National security is a shared responsibility. Everyone has a role to play to counter the cost and impact of espionage on Australia and Australians.

ASIO estimates the threat from espionage will grow in intensity and sophistication in the next decade. While the public and private sectors are defending themselves against some espionage, more can be done to counter espionage. The threat is real and anyone with access to sensitive information can be a target. The consequences financially, reputationally and nationally can be severe.

Governments, businesses and organisations can establish robust security measures and maintain a strong security culture. A strong security culture creates a workplace that is safer, more secure and more resilient to threats. Good security is achievable and it works.

Organisations can build and foster a strong security culture by creating an environment that **ENABLES**, **ENCOURAGES** and **EDUCATES** security-savvy behaviours.

Government workers and security clearance holders have an obligation to report suspicious approaches:

contact your security manager and fill out a contact report

Other workers can report suspicious approaches by:

using ASIO's Notifiable Incidents, Threats or Reportable Observations (NITRO) portal at **nitro.asio.gov.au**

calling the National Security Hotline on **1800 123 400**

FOSTERING GOOD SECURITY CULTURE

Australian organisations are well-versed in protecting themselves against criminal activity, fraud and workplace accidents. Effective defence against potential espionage employs a similar ethos. Simple steps can make a difference in stopping espionage.

Understand the threat – acknowledge the threat is real. Anyone with access to sensitive information can be a target, and the consequences for your bottom line, reputation and the national interest can be severe.

Identify the risk – know what is valuable and what is vulnerable in your organisation, whether it is data, assets or individuals.

Manage the risk – implement a coherent, connected security strategy across your whole enterprise – your people, places, technology and information. Continuous and consistent education and engagement with staff builds a strong culture that is security aware and alert to anomalous behaviour.

RESOURCES

ASIO has developed a range of materials, digital and printable, to assist individuals and organisations to protect themselves against espionage. These are publicly available on ASIO's website asio.gov.au/protective-security-advice.

To read the Australian Institute of Criminology's report, *The cost of espionage*, visit asio.gov.au/coe.

ASIO
asio.gov.au/coe

Australian Government
Australian Security Intelligence Organisation

THE CO$T OF ESPIONAGE

CLEARANCE HOLDERS



ASIO
asio.gov.au/coe

Espionage is the state-sponsored theft of information or capabilities for passage to another country, which undermines Australia's national interest or advantages a foreign country. It is corrosive and weakens our sovereignty, businesses, military and economy.

It is estimated espionage cost the Australian economy

$12.5 billion

in 2023–24.

Conservative estimates show espionage could cost Australia

tens of billions

more if we do not take security seriously.

We also know these figures are a significant underestimate, because by definition espionage is difficult to detect and difficult to measure, which means many of the most serious, significant and cascading costs of espionage are not included in the $12.5 billion figure. Some costs of espionage are obvious and immediate, while others are hidden, subjective, dispersed or enduring in nature, taking months or years to be realised.

Source: *The cost of espionage* report available at asio.gov.au/coe

CLEARANCE HOLDERS

Spies from multiple countries routinely and relentlessly trawl professional networking sites, seeking to identify, target and cultivate Australians with access to privileged information. They pose as consultants, head-hunters, local government officials, academics and think-tank researchers, claiming to be from fictional companies.

Fake job ads are created and advertised on popular career sites. The jobs are often well-paid, part-time roles for people with expertise in geopolitics or defence. Be careful what you share about yourself online and on social media.

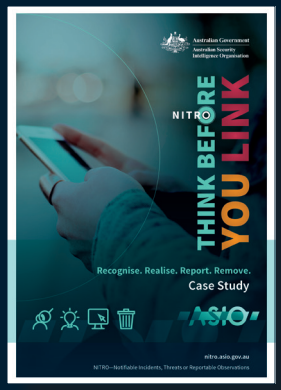
This form of espionage is low-cost, low-risk, low-effort – and conducted at scale.

All too often, we make it all too easy. On just one professional networking site, the profiles of more than 35,000 Australians indicate they have access to sensitive and potentially classified information.

Around 7,000 reference their work in Defence, including the specific project they are working on, the team they are working in and the critical technologies they are working with.

Close to 400 explicitly say they work on AUKUS, and the figure rises above 2,000 if you include broader references to 'submarines' and 'nuclear'.

Nearly 2,500 publicly boast about having a security clearance and 1,300 claim to work in the national security community.



If you have sensitive information, common sense is a good place to start.

Be alert to the threat. Don't make yourself a target on social media. Don't use PASSWORD as a password. Update your software. Follow the rules for handling sensitive or classified information.

If you are pressed for inside information, be discreet. If an approach seems suspicious, report it.

ASIO's protective security advice for clearance holders ***Report prying minds*** and ***Think before you link*** are available at **asio.gov.au/prying-minds** and **asio.gov.au/TBYL**.