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.

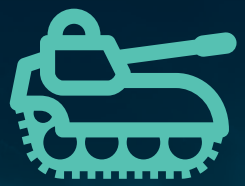
To read the Australian Institute of Criminology's report, *The cost of espionage*, visit asio.gov.au/coe.

ASIO
asio.gov.au/coe

Australian Government
Australian Security Intelligence Organisation

THE CO$T OF ESPIONAGE

DEFENCE





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

DEFENCE

Australia's military capabilities are a top target for foreign intelligence services. They want to blunt our operational edge; gain insights into our operational readiness, tactics and techniques; and better understand our allies' capabilities.

This includes maritime and aviation-related military capabilities, as well as innovations with both commercial and military applications, from fields such as quantum science and communications.

Important Defence projects are put at risk when Australians working on those projects advertise their work, security clearance or other information via social media platforms and job websites. This enables spies from multiple countries to identify, target and cultivate Australians with access to privileged information.

Several years ago, an Australian Defence contractor invented, manufactured and marketed a world-leading innovation.

Sales boomed for a while but suddenly collapsed, for no apparent reason. Customers began flooding the company's repair centre with faulty products. While the returns looked genuine, closer examination revealed they were cheap, nasty knock-offs. An investigation uncovered what happened.

One year earlier, company representatives had attended a defence industry event overseas and were approached by an enthusiastic local. She insisted on sharing some content with them via a USB, which they inserted into a company laptop. The USB infected the system with malware that allowed hackers to steal the blueprints for the product.

Almost certainly, the 'enthusiastic local' was working for a foreign intelligence service, which gave the blueprints to a state-owned enterprise that mass-produced the knock-offs at Australia's expense – the tangible cost of espionage.



ASIO's protective security advice for the defence sector ***Report prying minds*** is available at **asio.gov.au/prying-minds**.