



[Home](#)

[About](#)

[FAQs](#)

[Publications](#)

[News](#)

[Contact](#)

Frequently-Asked Questions

Frequently-asked questions about the ACSC and cyber security are answered below.

What is the role of the ACSC?

The role of the ACSC is to:

- lead the Australian Government's operational response to cyber security incidents
- organise national cyber security operations and resources
- encourage and receive reporting of cyber security incidents
- raise awareness of the level of cyber threats to Australia
- study and investigate cyber threats.

When did the ACSC become operational?

The ACSC was opened on Thursday 27 November 2014.

How is the ACSC funded?

The ACSC is funded from existing agency resources. Each portfolio participating in the ACSC will contribute to the costs.

How many staff will the ACSC have?

How many staff will the ACSC have?

The ACSC will have approximately 300 officers by 2017.

Who has responsibility for the ACSC?

The ACSC is the joint responsibility of the [Attorney-General](#) and [Minister for Defence](#).

Major General Stephen Day, head of Cyber and Information Security at the [Australian Signals Directorate](#), is the centre's first coordinator.

How does the ACSC work with the private sector?

The ACSC builds on the already strong links between government and the private sector, particularly those already established by ACSC agencies. The ACSC is considering a number of models for partnering with industry which will allow close engagement on everything from information sharing to the development of effective response strategies.

How is the ACSC different from the former Cyber Security Operations Centre?

The ACSC is the next evolution of Australia's cyber security capability. The Cyber Security Operations Centre was a Defence-based capability that hosted liaison staff from other government agencies. The ACSC comprises staff from the former Cyber Security Operations Centre (CSOC) and the co-location of all contributing agencies cyber security capabilities in one location.

The ACSC has co-located:

- [ASD's cyber security mission](#) - the Commonwealth authority on information security provides advice and assistance to Australian government agencies
- Attorney-General's [CERT Australia](#) - the point of contact in government for cyber security issues affecting major Australian businesses
- representatives of the [Australian Federal Police](#), who investigate and respond to cyber crime of national significance
- the [Australian Crime Commission](#), which discovers, understands and prioritises cyber crime threat intelligence to enhance response options
- cyber investigations and telecommunication security specialists from the [Australian Security Intelligence Organisation](#)
- strategic intelligence analysts from the [Defence Intelligence Organisation](#).

What are the ACSC governance arrangements?

The Cyber Security Operations Board (CSOB) is responsible for strategic oversight of the government's operational cyber security capabilities and coordination of cyber security measures. The board members are at the level of secretary and agency head.

The responsibilities, mandates and authorities for each agency are unaltered.

Each agency is responsible for protecting the privacy and sensitivity of their information according to relevant policies and legislations.

The [Inspector General of Intelligence and Security \(IGIS\)](#) has oversight of all activities of the Australian Intelligence Community agencies in the ACSC.

REPORT A CYBER SECURITY INCIDENT

Reports help the ACSC to develop a better understanding of the threat environment and will assist other organisations who are also at risk.

Cyber security incident reports are also used in aggregate for developing new defensive policies, procedures, techniques and training measures to help prevent future incidents.

Information for Australian businesses

Information for individual Australian citizens

Information for Federal, State and Local government agencies

[Privacy](#) [Copyright](#) [Disclaimer](#) [Accessibility](#) [Site map](#)