



Australian Government



Critical
Infrastructure
Centre

Proactive Risk Assessments

The Critical Infrastructure Centre brings together expertise and capability from across the Australian Government to manage the complex and evolving national security risks from foreign involvement in Australia's critical infrastructure.

The Centre is focused on assessing the risks of sabotage, espionage and coercion in the five priority sectors of telecommunications, electricity, gas, water and ports.

What is a proactive risk assessment?

Proactive risk assessments identify and outline ways to manage national security risks from foreign involvement in Australia's critical infrastructure, to ensure its security and continuity.

Proactive risk assessments are prioritised towards the most critical assets across our four priority sectors, irrespective of whether they are foreign or domestically owned.

Assessments provide a better understanding for government and industry of where national security risks exist in an asset or across a sector as a result of foreign involvement.

A proactive risk assessment is not a security audit; the Centre will not seek to determine your compliance with any internal or external security obligations.

We want all critical infrastructure owners and operators to be better equipped to manage national security risks.

Why should I participate?

Ensuring the resilience of Australia's critical infrastructure is a responsibility shared by states and territories, the Commonwealth Government and owners and operators of critical infrastructure. It is crucial that we work together to provide essential services to the Australian economy and to the community.

Participation in a proactive assessment is an opportunity to work closely with the Centre and benefit from our expertise. We will work with you to identify and outline ways to manage national security risks related to your asset. Information you provide to the Centre will be treated in confidence.

Participants receive valuable information, including:

- an assessment summary outlining the key outcomes of the risk assessment, and
- practical guidance to mitigate national security risks identified through the assessment.

The Centre will work with the asset owner and operators to implement suggested mitigations. Successful implementation of suggested mitigations should boost business continuity, protect against reputational loss, and improve the security of your asset.

How is a proactive risk assessment undertaken?

1 Data collection

We work with Commonwealth agencies, state and territory governments, regulators and private owners and operators to understand and assess risks. As such, we will work with you to collect information on:

- People – including key positions, ownership and control structure and boards, background checking & security clearances
- Information & data holdings – including sensitive information holdings, storage & accessibility
- Physical facilities – including access control & critical areas
- Information technology – including Industrial Control Systems (including SCADA), business systems & IT system security
- Interdependencies – including supply chains, outsourcing, offshoring & criticality to and reliance on other sectors
- Governance – including security management, security culture and training, security processes and procedures & quality assurance, and
- Resilience – including service continuity, recovery & ability to respond.

2 Face-to-face workshop

For some assets, we may conduct a workshop with relevant stakeholders to outline the threat environment and test and refine the assessment of vulnerabilities, consequences and potential mitigations specific to the asset as well as outcomes that may be applicable to the broader sector.

3 Produce documents

We will provide owners and operators with an assessment summary outlining the key outcomes of the risk assessment and best practice guidance on mitigating risks and increasing resilience. The Centre will work with the asset to implement suggested mitigations.