Australian Government
Major Projects Facilitation Agency

Fact sheet

Security of Critical Infrastructure Act 2018

If your project involves assets considered to be Australian critical infrastructure, you must fulfil obligations designed to manage security risks to the asset in accordance with this Act.

1. What obligations do I have?

Owners, operators and direct interest holders of Australia's critical infrastructure assets must meet applicable security reporting and risk management obligations under the *Security of Critical Infrastructure Act 2018* (the SOCI Act). Obligations are different for each asset class and depend on whether you own or operate the asset, or hold a direct interest in the asset.

The SOCI Act applies to the following sectors, each of which include critical infrastructure assets:

- communications
- financial services and markets
- data storage or processing
- defence industry
- higher education and research
- energy
- food and grocery
- health care and medical
- space technology
- transport
- water and sewerage.

The Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 (the Rules) prescribe the asset classes within each of these sectors that are considered to be critical infrastructure assets.

Please refer to guidance on critical infrastructure asset class definitions[PDF] from the Cyber and Infrastructure Security Centre (CISC) to help determine if you are an owner, operator or direct interest holder of a critical infrastructure asset.

Depending on the asset class and your involvement, you may need to do the following:

- provide operational and ownership information to the Register of Critical Infrastructure Assets
- develop and maintain a Critical Infrastructure Risk Management Program
- notify your asset's third-party data storage or processing provider
- report cyber security incidents.

Guidance and fact sheets on each of these obligations are available from the CISC website.

If you are the responsible entity for critical infrastructure that has been declared a System of National Significance (SoNS), the following enhanced cyber security obligations may apply:

- develop and maintain a cyber security incident response plan
- undertake cyber security exercises
- undertake a vulnerability assessment
- provide system information to develop and maintain a near real-time threat picture.

2. Who oversees the obligations?

CISC, within the Department of Home Affairs, is the primary regulator under the SOCI Act and manages the Register of Critical Infrastructure Assets. CISC monitors compliance with requirements for the Critical Infrastructure Risk Management Program and regulates annual reporting for all assets except for payment systems. The Reserve Bank of Australia (RBA) regulates payment systems.

This fact sheet provides general information and does not constitute legal advice. You should seek independent legal advice tailored to your individual circumstances. The Major Projects Facilitation Agency (MPFA) assists major project proponents to navigate Australian Government approval processes. The MPFA does not grant approvals, nor administer the legislation listed in this fact sheet.

CISC prepares risk assessments in relation to national security risks to critical infrastructure. This includes providing advice to the Treasury regarding potential risks posed by foreign investment in critical infrastructure.

Unless an exemption applies, if a cyber security incident impacts on the availability of a critical infrastructure asset, the responsible entity must report the incident to the Australian Cyber Security Centre of the Australian Signals Directorate (ASD).

The Minister for Home Affairs may prescribe an asset as a critical infrastructure asset in the Rules, or, may privately declare an asset to be critical infrastructure if public knowledge that the asset is critical infrastructure would be a risk to national security. The Minister may also privately declare a critical infrastructure asset to be a SoNS. In both cases, each reporting entity for a declared asset will be notified.

The Secretary of the Department of Home Affairs decides which Enhanced Cyber Security Obligations apply to SoNS.

3. How do I meet the obligations?

The online forms portal on the CISC website is used to submit information relating to the Register of Critical Infrastructure Assets; Risk Management Programs; and Enhanced Cyber Security Obligations. Risk Management Program requirements for payment systems are submitted to the RBA.

Cyber security incident reports are made to the ASD's Australian Cyber Security Centre through the cyber incident reporting portal.

Responsible entities must take 'reasonable steps' to meet the obligation to notify their third-party data storage or processing provider that they are storing or processing data for a critical infrastructure asset. This may include writing to or emailing the provider and must be done as soon as practicable.

4. More information

Cyber and Infrastructure and Security Centre

Further information on security obligations for Australian critical infrastructure is available on the CISC website.

CISC can be contacted by email at enquiries@CISC.gov.au.

Major Projects Facilitation Agency

If you would like assistance to identify potential Australian Government regulatory approvals required for your project, please refer to the Major projects help tool self-assessment.

The MPFA team can be contacted by email at MPFA@industry.gov.au.

This fact sheet provides general information and does not constitute legal advice. You should seek independent legal advice tailored to your individual circumstances. The Major Projects Facilitation Agency (MPFA) assists major project proponents to navigate Australian Government approval processes. The MPFA does not grant approvals, nor administer the legislation listed in this fact sheet.