Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Security Legislation Amendment (Critical Infrastructure) Act 2021

The Security Legislation Amendment (Critical Infrastructure) Act 2021 has amended the *Security of Critical Infrastructure Act 2018* (the Act) to build upon the existing framework which aims to strengthen the security and resilience of critical infrastructure.

What is the purpose of the reforms?

To provide a framework for managing risks to national security relating to critical infrastructure, including by:

- improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and
- facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks.

Amendments to the Act have strengthened the security and resilience of critical infrastructure, by:

- expanding the scope of the Act from applying to four sectors to eleven sectors;
- providing a regime for the Commonwealth to receive reports in relation to cyber security incidents; and
- providing a regime for the Commonwealth to respond to serious cyber security incidents

Why are the changes needed?

Australia is facing increasing cyber security threats to essential services, businesses and all levels of government. In recent years we have seen cyber-attacks on federal Parliamentary networks, logistics, the medical sector and universities – just to mention a few.

While owners and operators of critical infrastructure are best placed to deal with such threats, it takes a team effort to bring about positive change. That is why the ongoing security and resilience of critical infrastructure must be a shared responsibility – by all governments and the owners and operators of the infrastructure. The 2021 amendments to the Act is step one to bringing together the team.

What is a Critical Infrastructure Asset?

The coverage of the framework under the Act has been expanded from four sectors (water, electricity, gas and ports) to eleven sectors and 22 asset classes:

- Communications sector
  - telecommunications asset
  - broadcasting asset
  - domain name system
- Data storage and processing sector
  - data storage or processing asset
- Financial services and markets sector
  - banking asset
  - superannuation asset
  - insurance asset
  - financial market infrastructure asset
- Water and sewerage sector
  - water asset
- Energy sector
  - gas asset
  - electricity asset
  - energy market operator asset
  - liquid fuel asset
- Health care and medical sector
  - hospital
- Higher education and research sector
  - education asset
- Food and grocery sector
  - food and grocery asset
- Transport sector
  - freight infrastructure asset
  - freight services asset
  - port asset
  - public transport asset
  - aviation asset
- Space technology sector, and
- Defence industry sector
  - defence industry asset.

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.

CONTACT US | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au

The specific meaning of these assets can be found in section 5 and sections 10-12KA of the Act, and the Security of Critical Infrastructure (Definition) Rules 2021.

The meaning of an **asset** includes a system, network, facility, computer, computer device, computer program, data, premises and "any other thing".

The Minister may also **privately declare an asset** to be a critical infrastructure asset if certain thresholds are met. The Minister must consult with the responsible entity for that asset before an asset is declared and notify the responsible entity once the declaration is made.

What are the obligations?

Depending on the obligation, the responsibility for complying with the framework will sit with either the **Responsible Entity** or **Direct Interest Holders**.

- A **Responsible Entity** for a critical infrastructure asset is the body with ultimate operational responsibility for the asset.
- **Direct Interest Holders** are entities that hold a direct or joint interest of at least 10 per cent in a critical infrastructure asset, or who hold an interest and are in a position to directly or indirectly influence or control the asset.

Register of Critical Infrastructure Assets

The Register requires reporting entities, who are either direct interest holders or the responsible entity of critical infrastructure assets, to provide to Government ownership, operational, interest and control information.

For further information, please refer to the Register of Critical Infrastructure Assets Factsheet, found at www.CISC.gov.au

Mandatory Cyber Incident Reporting

Responsible entities for critical infrastructure assets will be required to report critical and other cyber security incidents to the Australian Cyber Security Centre's online cyber incident reporting portal, found at cyber.gov.au.

For further information, please refer to the Mandatory Cyber Incident Reporting Factsheet, found at www.CISC.gov.au

Government Assistance

Government Assistance measures will allow Government to provide assistance immediately prior to, during or following a significant cyber security incident to ensure the continued provision of essential services, including to:

- gather information to determine if another power in the Act should be exercised;
- direct an entity to do, or not do, a specified act; or
- request an authorised agency provide support.

For further information, please refer to the Cyber Incidence Response: Government Assistance Measures Factsheet, found at www.CISC.gov.au

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.