Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Security Legislation Amendment (Critical Infrastructure Protection) Act 2022

The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act) amends the *Security of Critical Infrastructure Act 2018* (the SOCI Act) to build upon the existing framework and uplift the security and resilience of Australia's critical infrastructure.

What is the purpose of the reforms?

To strengthen the existing framework for managing risks to critical infrastructure, including by:

- introducing a requirement for owners and operators of critical infrastructure assets to establish, maintain, and comply with a **risk management program** to manage the material risk of a hazard occurring, which could impact the availability, integrity, reliability or confidentiality of the critical infrastructure asset;
- establishing a mechanism for **the declaration of Systems of National Significance** (SoNs)– those being the assets most interconnected, interdependent, and essential to Australia's social or economic stability, defence or national security;
- establishing a framework of **Enhanced Cyber Security Obligations**, which may apply to systems of national significance; and
- enhancing the framework for the use and disclosure of protected information.

Why is the SLACIP Act needed?

Australia is facing increasing cyber security threats to essential services and businesses. 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 will, in most cases, be 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 Commonwealth and State/Territory governments and the owners and operators of the infrastructure. The SLACIP Act is another step to jointly addressing the threat of cyber security.

What is a Critical Infrastructure Asset?

The specific meaning of these assets can be found in section 5, section 9 and sections 10-12KA of the SOCI Act, and the *Security of Critical Infrastructure (Definitions) Rules 2021*.

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

The Minister may prescribe an asset as a critical infrastructure asset under section 9 if certain thresholds are met, including that the asset relates to a critical infrastructure sector. The Minister may also **privately declare an asset** under section 51 of the SOCI Act to be a critical infrastructure asset if certain thresholds are met. Under a section 51 declaration the Minister must consult with the responsible entity for that asset before an asset is declared and notify the responsible entity within 30 days after making the declaration.

What are the new obligations?

Responsible entities for certain critical infrastructure assets will have to comply with risk management program obligations. Our most critical assets, a small subset, may also be declared as SoNS, which imposes additional cyber security obligations.

Who is responsible for complying?

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% in a critical infrastructure asset, or who hold an interest and are in a position to directly or indirectly influence or control the asset.

Risk Management Program

The risk management program requires responsible entities of critical infrastructure assets to **establish, maintain, and comply with** a risk management program.

This will require entities to take a holistic and proactive approach in **identifying and mitigating hazards that pose material risks** to the availability, integrity, reliability or confidentiality of the asset.

- Entities must identify, (and as far as is reasonably **practicable**) prevent and mitigate 'material risks' that could have a 'relevant impact' on the asset.
- A material risk refers to those risks and hazards that, if realised, may affect the availability, integrity, reliability and confidentiality of critical infrastructure assets.

Entities are also required to **review** the risk management program on a regular basis and ensure the program is **up to date**.

Entities will be required to provide an **annual report** to the Government, approved by its board, council or other governing body, regarding the risk management program.

For further information, please refer to the Risk Management Program Factsheet, found at www.CISC.gov.au.

Enhanced Cyber Security Obligations

Enhanced Cyber Security Obligations will only apply to SoNS. SoNS are critical infrastructure assets that are crucial to the nation due to the cascading consequences of disruption to other critical infrastructure assets and sectors if they are unavailable.

Only a small subset of critical infrastructure assets will be SoNS. The Minister may only declare a critical infrastructure asset a SoNS if satisfied that the **asset is of national significance**.

Under the Enhanced Cyber Security Obligations, the Secretary of Home Affairs may require the responsible entity for a system of national significance to undertake one or more prescribed cyber security activities:

- develop **cyber security incident response plans** to prepare for a cyber incident.
- undertake **cyber security exercises** to build cyber preparedness.
- **undertake vulnerability assessments** to identify vulnerabilities for remediation.
- **provide system information** to build Australia's situational awareness.

The Enhanced Cyber Security Obligations will support the sharing of near-real time threat information to provide industry with a more mature understanding of emerging cyber security threats, and the capability to reduce the risks of a significant cyber attack against Australia's most critical assets. For further information, please refer to Enhanced Cyber Security Obligations Factsheet, found at www.CISC.gov.au