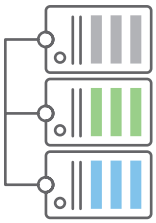
SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018 (SOCI ACT) – A brief overview



No one will argue that the cyber threat landscape is changing rapidly for the worse. We have seen an increasing number of attacks on critical infrastructure lately. Motivations for these attacks vary from financial gain to nation state attacks with the aim of causing damage and destruction to another nation.

The Australian government has responded to this new threat by proposing the Security Legislation Amendment (Critical Infrastructure) Bill 2020 to bolster the Security of Critical Infrastructure Act 2018 (SOCI Act).

The Bill has subsequently been split into two now. Bill One is designed to deal with immediate threats which has now been passed into law. Bill Two is basically now designed to deal with what are deemed the less urgent elements and is yet to be passed.

The key aspects of the split Bills are summarised below.

The Bills as a Framework

The Bills introduce the following key concepts:

BILL ONE

- Requiring notification of cyber security incidents
- Requiring certain entities relating to a critical infrastructure asset to provide information in relation to the asset, and to notify if certain events occur in relation to the asset
- Setting up a regime for the Commonwealth to **respond** to serious cyber security incidents

BILL TWO

- The keeping of a register of information in relation to critical infrastructure assets
- Requiring the responsible entity for one or more **critical infrastructure assets** to have, and comply with a critical infrastructure risk management program
- Imposing enhanced cyber security obligations that relate to **systems of national significance**
- Allowing the minister to require certain entities relating to a critical infrastructure asset to do, or refrain from doing, an act or thing if the minister is satisfied that there is a risk of an act or omission that would be prejudicial to security
- Allowing the Secretary to require certain entities relating to a critical infrastructure asset to provide certain information or documents
- Allowing the secretary to undertake an assessment of a critical infrastructure asset to determine if there is a risk to national security relating to the asset

Having discussed what the Bills include, the rest of this paper elaborates on the key elements contained within the Bills.

Definitions of Critical Infrastructure and Critical Infrastructure Assets

The Bill defines critical infrastructure as "Those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct **national defence** and **ensure national security**."

Critical infrastructure assets across each sector have been identified through an assessment of whether, if destroyed, degraded, or rendered unavailable, there would be a significant detrimental impact on:

- **Maintaining basic living standards for the Australian population** – this includes those essential services and other services without which the safety, health or welfare of the Australian community or a large section of the community would be endangered or seriously prejudiced
- Industries, commercial entities and financial institutions that underpin Australia's **wealth and prosperity**
- The security of **large or sensitive data holdings** which, if undermined, could lead to the theft of personal or commercially sensitive information, intellectual property or trade secrets
- **National security and defence** capabilities

These definitions are important as they define the applicability of the Act and sets scope.

Key Aspects of the Bill

The Bills give effect to this framework by introducing:

- **A Positive Security Obligation (Bill Two)** for critical infrastructure, including an all-hazards critical infrastructure risk management program and report information to the Register. Applies to specific critical infrastructure assets
- **Government assistance (Bill One)** to relevant entities for critical infrastructure sector assets in response to significant cyber attacks that impact on Australia's critical infrastructure assets and include mandatory cyber incident reporting

RSM

- The Minister for Home Affairs will have the power to declare a critical infrastructure asset as a **'system of national significance' (Bill Two)**, having regard to the nature and extent of interdependencies with other critical infrastructure assets. Systems of national significance will be subject to the **enhanced cyber security obligations**. The Enhanced Cyber Security Obligations are incident response plans, scenario based exercises, vulnerability assessments and access to system information

The applicability of the above is best summarised in the table below:

	Entities within Critical Infrastructure Sectors	Critical Infrastructure Assets	Systems of National Significance
Government Assistance	Yes	Yes	Yes
Positive Security Obligations	No	Yes	Yes
Enhanced Cyber Security Obligations	No	No	Yes

Who does the Bill Apply to?

Per Bill One, this applies to the following sectors. Please note that the Bill outlines the definition of each sector as well as its Critical infrastructure assets:

- Communications sector
- Data storage or processing sector
- Financial services and markets sector
- Water and sewerage sector
- Energy sector
- Health care and medical sector
- Higher education and research sector
- Food and grocery sector
- Transport sector
- Space technology sector
- Defence industry sector

RISK MANAGEMENT PER BILL TWO

Risk management related to critical assets forms the backbone of this Bill. The SOCI Act and the proposed changes will ultimately require responsible entities of critical infrastructure assets to manage security risks by meeting the following **principles-based outcomes**:

- **Identify material risks** – Entities will have a responsibility to take an all-hazards approach when identifying risks that may affect the availability, integrity, reliability and confidentiality of their asset
- **Mitigate risks to prevent incidents** – Entities will be required to understand the identified risks and have appropriate risk mitigations in place to manage those risks
- **Minimise the impact of realised incidents** – Entities will be required to have robust procedures in place to mitigate the impacts in the event a threat has been realised and recover as quickly as possible
- **Effective governance** – Through rules, entities will be required to have appropriate risk management oversight arrangements in place, including evaluation and testing

The types of risks that Bill Two aims to manage are:

- **Physical security risks** – This includes risk of harm to people and damage to physical assets
- **Cyber security risks** – Malicious cyber activity is one of the most significant threats facing Australian critical infrastructure assets and can range from denial of service attacks, to ransomware and targeted cyber intrusions
- **Personnel security risks** – This refers to the 'insider threat' or the risk of employees exploiting their legitimate access to an organisations' assets for unauthorised purposes including corporate espionage and sabotage
- **Supply chain risks** – The reliance on supply chains inherently involves dependencies on other assets, or providing other entities with some level of access to, or control of, your asset or business' deliverables. As is the case for personnel risk, supply chain risks relate to entities exploiting their legitimate access to, or control of, an organisations' assets for unauthorised purposes or otherwise creating a cascading impact to dependent assets.

To address the growing threats to Australia's critical infrastructure, the Federal government has introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020, subsequently split into two Bills, to bolster the Security of Critical Infrastructure Act 2018 (SOCI Act). The Bills have expanded the sectors that are classified as critical infrastructure and has introduced additional regulatory requirements per sector and per asset. I have discussed the key aspects of the Bills in this paper to ensure affected sectors are aware of the Bills and can start to prepare for the time when the Bills becomes law.

References: *Explanatory Document – Draft Exposure 3 Security Legislation Amendment (Critical Infrastructure) Bill 2020; Security Legislation Amendment (Critical Infrastructure) Bill 2020 (homeaffairs.gov.au)*