CLAROTY

SOLUTION BRIEF

THE PATH TO SOCI COMPLIANCE

Inside Australia's Security of Critical Infrastructure Act 2018 (the SOCI Act) and how Claroty enables impacted organisations to achieve SOCI compliance

Introduction

The Security of Critical Infrastructure Act 2018 — otherwise known as the SOCI Act — was passed by the Australian government in July 2018 to create a mandatory cybersecurity framework for the regulation and protection of the nation's critical infrastructure sectors. The act has since undergone reforms focused on further securing and enhancing the resilience of these sectors amid increasingly frequent and disruptive cyber threats.

This solution brief provides a high-level overview of the SOCI Act, details the Claroty portfolio's support for SOCI compliance, and offers related guidance for security and risk practitioners in Australia and beyond.

SOCI Basics

Scope

The SOCI Act applies to all owners and operators of Australian critical infrastructure assets, which are known as **Responsible Entities**, as well as to all businesses with a direct interest in such assets, which are known as **Direct Interest Holders**.

Both categories span 22 asset classes for organisations in the following 11 critical infrastructure sectors:

- Communications
- Data storage & Processing
- Energy
- Financial Services
- Food & Grocery
- Health & Medical
- Higher Education & Research
- Transport
- Water & Sewerage.

SOCI Compliance Requirements

The requirements set forth by SOCI are called **Positive Security Obligations (PSOs)**, which aim to enhance risk management, resilience, and business as usual for Australia's most critical assets. These PSOs are:

1. Register of Critical Infrastructure Assets
2. Notification of Cybersecurity Incidents
3. Critical Infrastructure Risk Management Program (CIRMP)*

**Notably, the CIRMP PSO only applies to Responsible Entities in 13 of 22 asset classes.*

Enforcement Timelines & Deadlines

Two of SOCI's three PSOs — specifically, 1) Register of Critical Infrastructure Assets and 2) Notification of Cybersecurity Incidents — are currently already enforced for Responsible Entities and Direct Interest Holders.

Additionally, Responsible Entities have until the deadline of **18 August 2024** to demonstrate their compliance with the third PSO: Critical Infrastructure Risk Management Program (CIRMP). Such entities are also required to submit an annual report detailing their CIRMP by the deadline of **28 September 2024.**

How Claroty Supports SOCI Compliance

The Role of Cyber-physical Systems (CPS)

Claroty helps organisations comply with SOCI by extending cybersecurity controls to all cyber-physical systems (CPS), many of which are critical assets in the 22 classes regulated by SOCI. Key CPS include:

- **Operational technology (OT)** assets, such as the programmable logic controllers (PLCs) that drive power generation and manufacturing processes
- **Internet of Things (IoT)** and **Industrial IoT (IIoT)** devices, such as the security cameras and motion sensors that help keep hospitals safe and comfortable
- **Building management system (BMS)** equipment, such as the digitised HVAC controllers and elevators that enable us to breathe clean air and easily move throughout buildings
- **Internet of Medical Things (IoMT)** and other clinical devices, such as the infusion pumps and MRIs that monitor our vitals, diagnose our ailments, and help us keep us healthy

Although alignment between the Claroty Portfolio and SOCI spans all three of the act's PSOs, Claroty offers the most robust support for the third PSO: **Critical Infrastructure Risk Management Program (CIRMP),** which requires that CIRMPs address material risks that specific types of hazards pose to critical assets.

About the Claroty Portfolio

Claroty supports all use cases and objectives on the full CPS cybersecurity journey. Portfolio solutions include:

Claroty xDome

Claroty xDome is a flexible SaaS platform purpose-built for all use cases & types of CPS on the entire industrial cybersecurity journey.

Medigate by Claroty

Medigate by Claroty is a SaaS-based healthcare cybersecurity platform that safeguards the devices that underpin patient care.

Claroty SRA

Claroty Secure Remote Access (SRA) delivers frictionless, reliable, secure remote access for internal & third-party OT personnel.

Claroty CTD

Claroty Continuous Threat Detection (CTD) offers robust, on-premises cybersecurity controls for industrial environments.

Mapping Claroty Capabilities to the Critical Infrastructure Risk Management Program PSO

The following table outlines the extent that the capabilities provided by solutions within Claroty's portfolio address material risks posed by the specific types of hazards detailed in the SOCI Act's rule for CIRMPs:

HAZARD TYPE	HAZARD DETAILS	SUMMARY OF CLAROTY SUPPORT	SOLUTION(S)
1. Cyber and Information Security	Cyber and information security hazards pose cyber risks to digital systems, computers, datasets, and networks that underpin critical infrastructure. They typically entail improper access, misuse, or unauthorised control and can impair the availability, confidentiality, integrity, and/or safety of a critical asset.	Claroty enhances protection against cyber and information security hazards by defining and enabling enforcement of segmentation policies that harden critical infrastructure networks, securing and tightly controlling remote and onsite access to such networks, and revealing and guiding the mitigation of cyber risks posed by unpatched vulnerabilities and other weaknesses affecting critical assets in these networks.	**Claroty xDome, Medigate, SRA, & CTD**
2. Physical Security	Physical security hazards pose physical risks to systems or other components essential to the availability, integrity, or safety of a critical asset. Examples include unauthorised physical access to sensitive facilities and natural disasters.	Claroty helps mitigate physical security risks by providing a Secure Remote Access (SRA) solution that offers highly secure-yet-frictionless remote access to the physical facilities in which critical infrastructure assets and networks operate. Suitable for both internal employees and third-parties, Claroty SRA reduces the need for personnel to be onsite to execute a range of use cases while ensuring all remote maintenance and related tasks are tightly controlled and do not expose critical assets to additional risks.	**Claroty xDome, Medigate, SRA, & CTD**
3. Personnel	Personnel hazards refer to risks posed by internal or third-party personnel (such as contractors or vendors) who have the access and ability to disrupt the functioning of or to cause significant damage to a critical asset. This type of hazard is commonly referred to as the insider threat.	There are two core functionalities through which Claroty's solutions help protect against insider threats and other personnel hazards. First, Claroty continuously monitors a customer's critical infrastructure network(s) for the earliest indicators of all manner of potential threats to critical assets — and these include insider threats. Second, Claroty tightly controls, monitors, and secures both onsite and remote access to critical assets for internal and third-party personnel, thereby substantially reducing the risk of intentional and unintentional insider threats and related risks.	**Claroty xDome, Medigate, SRA, & CTD**
4. Supply Chain	Supply chain hazards cover the risk of disruption to supply chains to the extent that a critical asset is negatively impacted. The threat can be naturally occurring, malicious, or intended to compromise the respective critical asset. This type of hazard also encompasses risks posed by over-reliance on suppliers.	Claroty helps mitigate supply chain risks by automatically correlating all critical assets against the latest common vulnerabilities and exposures (CVEs) and other cybersecurity weaknesses, continually assessing risks in critical infrastructure networks, and delivering secure-yet-frictionless remote access to these networks for internal and third-party users. As a result, customers can more effectively and efficiently assess, manage, and mitigate risks across their supply chains.	**Claroty xDome, Medigate, SRA, & CTD**

Conclusion

Claroty's CPS cybersecurity portfolio is especially ideal for security and risk practitioners at Australian critical infrastructure organisations that are required to comply with the requirements set forth by the SOCI Act. The portfolio offers extensive support for the act's critical infrastructure risk management program (CIRMP) Positive Security Obligation (PSO), particularly for organisations that own or operate critical assets categorised within at least one of the 22 SOCI-regulated asset classes.

By harnessing and seamlessly integrating Claroty's solutions with their existing security tools and workflows, security and risk practitioners can more easily comply with all SOCI PSOs across all of their critical assets.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organisations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organisations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.