txOne networks | Keep the Operation Running

Navigating Australia's SOCI Act 2018:

Updates and OT Security Solutions

What's SOCI?

The **Security of Critical Infrastructure (SOCI) Act 2018** is an Australian law designed to safeguard the nation's essential services – from energy and water to communications and healthcare – against cyber and physical threats. Within it, there are three requirements of note, called **positive security obligations**. Quoting verbatim from the Act, most critical infrastructure assets must:

1. "Provide operational and ownership information to the Register of Critical Infrastructure Assets"
2. "Report cyber incidents which impact the delivery of essential services"
3. "Adopt, maintain and comply with a written risk management program"

The Act currently covers **22 asset classes across 11 industries**, encompassing a broad range of critical infrastructure assets in both public and private sectors. In essence, SOCI provides a regulatory backbone to ensure that vital systems are resilient, with provisions for mandatory cyber incident reporting and even government assistance powers in the event of extreme attacks. This comprehensive approach reflects Australia's recognition that disruptions – whether from hostile cyberattacks, supply chain failures, or natural disasters – pose a national security risk and must be managed proactively.

What's New in SOCI for Critical Infrastructure Owners?

Recent amendments and rules (especially since 2022-2024) have significantly strengthened SOCI, introducing new obligations. Notably, the government "switched on" the requirement for a **Critical Infrastructure Risk Management Program (CIRMP)** – a formal, written risk management program that responsible entities (any entity that owns or operates an asset) must implement. This risk management program must take an "all-hazards" approach, addressing a spectrum of risks including personnel security, supply chain integrity, physical site security, natural hazards, and cyber/information security. Specifically, the **CIRMP Rules 2023** mandate that organizations comply with at least one recognized cybersecurity framework (or equivalent) at a minimum baseline. Options include the Australian Essential Eight strategies at Maturity Level 1, ISO/IEC 27001, the U.S. NIST Cybersecurity Framework, the U.S. DOE C2M2

(Level 1), or the AESCSF framework for the energy sector. This essentially forces critical infrastructure providers to uplift their cybersecurity to a common standard.

Timeline of new obligations: These requirements came with grace periods. Affected entities had to put in place a written risk management program by 17 August 2023, begin mandatory annual reporting on their risk program by 30 June 2024, and achieve compliance with the chosen cybersecurity framework by 17 August 2024. The annual reports – approved by the board – must detail how the entity is meeting its security obligations and managing risks, and the first report (for the 2023-2024 financial year) was due by 28 September 2024. Meanwhile, since 2022, it has been mandatory for critical infrastructure operators to report serious cyber incidents to the Australian Cyber Security Centre within tight time frames (in some cases, within 12 hours of awareness). All these measures represent a major step-up in oversight; now, failure to comply can lead to regulatory action or penalties.

Expanded scope and powers: Recent legislative updates have broadened who and what is covered under SOCI. In late 2024, amendments to the Act expanded the definition of "critical infrastructure asset" to include **secondary assets holding business-critical data** that are essential to the primary asset's functioning. This means not just physical infrastructure, but IT systems (like databases or cloud services) supporting critical operations may now fall under SOCI's remit. The amendments also bolstered government powers: introducing a "last resort" direction power for the Home Affairs Minister to intervene in multi-asset cyber incidents and enabling regulators to issue directives if an entity's risk management program is found to be *seriously deficient*. Additionally, the security obligations have been extended to cover critical telecommunications assets, folding telecom sector security requirements into the SOCI framework.

These changes come alongside broader initiatives like the new **Australian Cyber Security Act 2024**, which introduces economy-wide cyber measures (e.g., mandatory ransomware incident reporting and IoT device standards) as part of Australia's 2023–2030 Cyber Security Strategy. In summary, owners and operators of critical infrastructure need to know that regulatory expectations have grown: more asset types are covered, baseline cyber hygiene is compulsory, and regulators now have sharper teeth, giving new bite to their bark when enforcing compliance.

What Technical Implementations Are Needed?

Security officers should adopt a proven cybersecurity framework, such as the Australian Essential Eight or ISO 27001 standards, and implement its controls accordingly. In practical terms, this means establishing measures like strict application allow-listing, timely patch

management or equivalent mitigations, multi-factor authentication for critical access, daily data backups, and monitoring for intrusions (all staples of the Essential Eight). Entities are now expected to conduct **regular vulnerability assessments and risk reviews** of their critical assets. Identified weaknesses must be addressed to prevent known threats from easily exploiting unpatched systems.

Crucially, network architecture and device security in OT (Operational Technology) environments need upgrading. Historically, many ICS (industrial control systems) were "air-gapped", meaning machines were kept physically separate from each other as a form of security. In modern times, those air gaps have vanished – increased connectivity means OT systems are now just as exposed to cyber threats as IT systems. Therefore, organizations should implement **network segmentation**, creating "micro-segments" with granular controls to isolate critical OT networks and limit the blast radius of any incident. Deploying inline security tools (such as industrial firewalls or intrusion prevention systems) allows you to filter malicious traffic and virtually patch vulnerabilities on legacy devices. Using these tools will shield unpatched systems from known exploits without needing to take them offline, giving you "no patch, no problem" peace of mind.

In addition, companies must **secure their endpoints** in the ICS/OT environment. Traditional antivirus solutions often fall short in industrial settings (due to heavy resource usage and need for internet updates), so the better approach is to use application whitelisting, or lightweight, behavior-based endpoint protection designed for mission-critical systems. These solutions operate on the principle of "least privilege", blocking any application or process that isn't explicitly allowed. Implementing such endpoint protection ensures that even if your Windows-based ICS machines can't be frequently patched or connected to the internet, they are not left defenseless.

Beyond cyber-specific controls, technical teams should also address **supply chain and maintenance security**, as required by SOCI's all-hazards risk management program. This includes vetting vendors and ensuring that any new equipment or software updates are malware-free and authentic. By inspecting and cleaning portable media and offline systems, companies can defend even air-gapped environments from infection and meet the Act's intent to manage supply chain risks. Robust monitoring and incident response processes are also vital; visibility into both IT and OT networks – through centralized logging, anomaly detection, or ICS network monitoring tools –supports early threat detection and compliance with mandatory incident reporting obligations.

In summary, the technical implementations span multiple domains: strengthening baseline cyber defenses, segmenting and protecting critical networks and endpoints, securing the supply chain/maintenance processes, and continuously monitoring and improving – all as part of a

formal risk management program that is documented, approved, and annually reviewed, per SOCI demands.

How TXOne Products Can Help Meet SOCI Obligations

To address the stringent requirements of the SOCI Act, organizations can leverage **TXOne Networks' suite of OT-focused security solutions**. Purpose-built for industrial and critical infrastructure environments, this portfolio aligns well with the Act's emphasis on robust, all-round protection. Here's how each category of TXOne products can assist critical infrastructure owners in complying with SOCI and enhancing security:

Portable Inspector & Supply Chain Security – Device Inspection Tools

- **Purpose:** Prevent malware entry via portable media and new equipment.
- **Key Features:** The **Portable Inspector** provides installation-free scanning for USB drives, laptops, and air-gapped systems. It comes equipped with LED indicators that provide a quick pass/fail status, no internet required. **ElementOne** aggregates results from all Portable Inspectors, revealing "shadow OT" devices and centralizing asset/vulnerability data, tracking risk across the OT environment.
- **SOCI Relevance:** Addresses supply chain and insider threat controls under the all-hazards risk management program.

Stellar Series (Endpoint Protection) – OT Endpoint Defense:

- **Purpose:** Protect legacy and mission-critical endpoints without internet-dependent antivirus.
- **Key Features:** The TXOne **Stellar** family (including StellarProtect) provides industrial-grade endpoint protection tailored for legacy and mission-critical systems. It does not require an internet connection for updates, instead relying on locally deployed machine learning and a robust allowlist of trusted applications to enforce least privilege and block both known and unknown malware as well as fileless attacks. Even if your HMI or SCADA server is running on an outdated Windows version, Stellar can lock it down so that ransomware or malicious code cannot execute, all while having **minimal performance impact** on the operational process.
- **SOCI Relevance:** Deploying such endpoint protection across critical assets directly supports mandatory cybersecurity framework controls of application whitelisting and malware prevention. **StellarOne**, the central management for Stellar endpoints, integrates threat intelligence (including the MITRE ATT&CK for ICS knowledge base) to

compose and generate compliance-ready reports which can help with fulfilling SOCI's annual reporting obligations.

EdgeIPS & EdgeFire (Network Defense) – OT Network Segmentation and Threat Prevention:

- **Purpose:** Enforce segmentation and protect unpatchable devices.
- **Key Features: EdgeFire** serves as an OT-native firewall, allowing granular network segmentation of your critical infrastructure environments – it can enforce zone-based policies to ensure that only authorized communications occur between industrial control system components, enabling threat containment. **EdgeIPS**, an Intrusion Prevention System, sits inline on the network to detect and block malicious traffic or exploit attempts in real time, all without disrupting operational processes. Notably, EdgeIPS enables **virtual patching**: if a PLC or legacy Windows server in your plant has a known vulnerability but cannot be taken down for a software patch, EdgeIPS can shield that device by intercepting exploits at the network level.
- **SOCI Relevance:** Meets risk-management requirements for segmentation, rapid mitigation of vulnerabilities, and incident containment. This "protect the unpatchable" approach means compliance with the Act's requirements (to address cybersecurity risks promptly) is achievable even for legacy systems – you don't have to wait for a maintenance window or vendor patch to mitigate a critical vulnerability. By deploying EdgeIPS/EdgeFire, organizations also gain deep visibility into network traffic patterns and potential attacks in the OT environment, aiding in incident detection and response.

Centralized Management & Monitoring (TXOne OneSeries Platforms) – Unified Security Oversight:

- **Purpose:** Unify monitoring and control across OT security layers.
- **Key Features: EdgeOne** can be used for centralized management of network devices, **StellarOne** for management of endpoint protection, and **SageOne** for cross-platform consolidated monitoring. Through these consoles, a security team can continuously monitor endpoint and network security status across all facilities, deploy policy updates, and collect logs/alerts for analysis. Central management can correlate an endpoint malware alert with a network intrusion event, providing a fuller picture of an incident. It can also map observed threats to known attack techniques (via the built-in MITRE ICS threat matrix) to understand the context of an attack.

- **SOCI Relevance:** When it's time to file the SOCI annual report or respond to regulators' queries, the organization can easily pull system-wide security metrics, incident records, and proof of control implementation from the TXOne management dashboard. In essence, the "single source of truth" for OT security is upheld, providing the continuous oversight, documentation, and incident tracking required for SOCI compliance.

By leveraging the above TXOne solutions, critical infrastructure operators can address multiple facets of the SOCI Act. They can harden their systems against cyber threats (meeting the cybersecurity framework baseline), control access and segment networks (reducing the impact of any breach), secure the supply chain and maintenance activities (covering "all hazards," not just cyber), and maintain the oversight needed for compliance. The combination of these tools – device inspection, endpoint protection, network defense, and unified management – embodies a defense-in-depth strategy aligned with Australia's regulatory expectations. In a time of heightened threat levels and regulatory scrutiny, using OT-specialized security technologies like TXOne's can significantly ease the burden of compliance while materially improving the security posture of critical infrastructure assets.

Mapping TXOne Networks Solutions to the SOCI Acts

Section	Sub-section	Description	TXOne Mapping
30BC	1: a-d	**30BC: Notification of critical cyber security incidents**	**StellarOne** provides a holistic view of OT endpoints, agent logs, and audit logs. This centralized approach simplifies incident management by quickly identifying which assets are affected and how it affects other endpoints. It can also be integrated with SIEM to enhance threat detection and incident response capabilities. **Element One** logs all events generated from PI and PI Pro. This comprehensive logging functionality ensures complete visibility of security incidents throughout your network. **EdgeOne** performs a similar function by logging all event incidents generated within your network. **SageOne** is TXOne's CPS platform which allows you to integrate StellarOne, ElementOne, and EdgeOne
30BD	1: a-d	**30BD: Notification of other critical cyber security incidents** (1) If: (a) an entity is the responsible entity for a critical infrastructure asset; and (b) the entity becomes aware that: (i) a cyber security incident has occurred or is occurring; and (ii) the incident has had, or is having, a significant impact (whether direct or indirect) on the	

		availability of the asset; the entity must: (c) give the relevant Commonwealth body (see section 30BF) a report that: (i) is about the incident; and (ii) includes such information (if any) as is prescribed by the rules; and (d) do so as soon as practicable, and in any event within 12 hours, after the entity becomes so aware	for asset-centric risk and vulnerability management. It correlates all logs collected from these management consoles and generates events accordingly. Moreover, all these solutions possess the capability to forward logs to SIEM solutions, further enhancing their integration and overall security effectiveness.
30CD	a-f	**Responsible entity must have an incident response plan** If: (a) an entity is the responsible entity for a system of national significance; and (b) the statutory incident response planning obligations apply to the entity in relation to: (i) the system; and (ii) cyber security incidents;	With TXOne **Element**, **Stellar**, and **Edge** products put together, you can create a robust incident response strategy for your OT environment. **Element** • **ElementOne** (explained above). • **Portable Inspector** is an agentless malware scanning tool that inspects OT assets without needing software installation or system reboots.

		the entity must: (c) adopt; and (d) maintain; an incident response plan that applies to the entity in relation to: (e) the system; and (f) cyber security incidents.	• **Safe Port** is a media sanitization kiosk that rapidly scans and cleans external media of malware before they are introduced into sensitive OT environments. **Stellar**: • **StellarOne** (explained above). • **Stellar** agents provide real-time monitoring and detection, continuously monitoring OT systems for malware. CPSDR monitors for anomalies and unauthorized changes. **Edge**: • **EdgeOne** (explained above). • **EdgeIPS** provides robust intrusion prevention by monitoring network traffic for malicious and abnormal activities and blocking threats in real-time with its regular signature updates. **EdgeIPS** also segments the network to contain incidents

			and prevent spread of threats. Additionally, **EdgeIPS** supports hardware bypass, ensuring continuous network traffic even during system failures. • **EdgeFire** is a firewall designed for OT environments capable of catering to routing and NATing requirements inside the OT infrastructure. It can also segment the network. **SageOne** gives a high-level overview of your security posture for your assets' entire lifecycle across every stage: 1. Onboarding (Inspected by Element) 2. Staging (Secured by Stellar) 3. Production (Protected by Edge) 4. Maintenance (Inspected by Element).
30CU	1:a-b 2:a-b	**Requirement to undertake vulnerability assessment** (1) The Secretary may, by written notice given to an	Vulnerability assessment is crucial for enhancing cybersecurity as it helps organizations identify, quantify, and prioritize weaknesses in their systems.

		entity that is the responsible entity for a system of national significance, require the entity to: (a) undertake, or cause to be undertaken, a vulnerability assessment in relation to: (i) the system; and (ii) all types of cyber security incidents; and (b) do so within the period specified in the notice. (2) The Secretary may, by written notice given to an entity that is the responsible entity for a system of national significance, require the entity to: (a) undertake, or cause to be undertaken, a vulnerability assessment in relation to: (i) the system; and (ii) one or more specified types of cyber security incidents; and (b) do so within the period specified in the notice.	**Portable Inspector Pro** not only scans and removes malware from endpoints but also collects asset data like device details, a list of installed applications, and Windows Update information with associated vulnerability data (such as CVE references, severity, CVSS ratings, and patch availability for identified vulnerabilities). **ElementOne** (explained above). **SageOne** (explained above). **EdgeOne** aggregates information from EdgeIPS and EdgeFire to create a comprehensive vulnerability dashboard. This dashboard integrates seamlessly with TXOne VDS, providing asset vulnerability detection and featuring 14 actionable widgets, including Top Vulnerable Assets, Vulnerability Risk Matrix, Risk Level by Network Layer, and Total Detected Vulnerabilities.

30DB	2: a-c	**Secretary may require periodic reporting of system information** (2) The Secretary may, by written notice given to the entity, require the entity to: (a) prepare periodic reports that: (i) consist of any such information; and (ii) relate to such regular intervals as are specified in the notice; and (b) prepare those periodic reports: (i) in the manner and form specified in the notice; and (ii) in accordance with the information technology requirements specified in the notice; and (c) give each of those periodic reports to ASD within the period ascertained in accordance with the notice in relation to the periodic report concerned.	**ElementOne** creates an asset list of all endpoints that Portable inspector has scanned, including not only Asset Details but also Application Information, Update Information, and Vulnerabilities for each asset. When needed, this information can be exported to produce periodic system reports. **StellarOne** consolidates information from all managed agents and categorizes it by group within the StellarOne console, simplifying oversight. When periodic system information reports are needed, they can be generated by group or across all agents, containing key details like Hostname, MAC Address, IP Address, OS, Group Name, License Status, Last Connection, and Agent Version, etc.

30DC		**Secretary may require event-based reporting of system information** The Secretary may, by written notice given to the entity, require the entity to do the following things each time an event of that kind occurs: (a) prepare a report that consists of any such information; (b) prepare that report: (i) in the manner and form specified in the notice; and (ii) in accordance with the information technology requirements specified in the notice; (c) give that report to ASD as soon as practicable after the event occurs.	All of TXOne's product suites, **Element** (Supply Chain Control), **Edge** (Network Defense), and **Stellar** (Endpoint Protection)—can generate events when a detection is triggered by known malware, unapproved applications, unapproved network behavior, or any deviation from the baseline. The events are forwarded to their respective management servers (ElementOne, StellarOne, and EdgeOne). These events can be exported into reports to comply with event-based reporting requirements.

Sources

1. Amy Cooper-Boast. "Security of Critical Infrastructure Update – Risk Management Programs Rules Switched On." *Association of Corporate Counsel*, Mar. 2023.
2. Leah Sadoian. "SOCI Act Explained: Compliance Rules & Requirements." *UpGuard Blog*, 2024.
3. Kieran Doyle et al. "Breaking down the Cyber Security Act 2024 and amendments to the SOCI Act." *Wotton + Kearney*, Nov. 26, 2024.
4. "Security of Critical Infrastructure Act 2018 (SOCI)." *Cyber and Infrastructure Security Centre, Australian Govt*.
5. Anna Ribeiro. "Trend Micro debuts TXOne StellarProtect industrial-grade endpoint protection for ICS devices." *Industrial Cyber*, May 4, 2021.
6. Anna Ribeiro. "TXOne's Portable Security Pro works towards improving security in ICS environments." *Industrial Cyber*, Jan. 28, 2022.
7. TXOne Networks. "Virtual Patching in OT with TXOne Edge" (Video description), Apr. 2025.
8. TXOne Networks – Product Page Snippets (2023-2025): Edge Series for Network Defense; Stellar Endpoint Protection; ElementOne Datasheet.

txOne networks