Palo Alto Networks Submission to the Department of Home Affairs Review of the Security of Critical Infrastructure (SOCI) Act 2018

Lodged - 22/12/2025

Executive Summary

Palo Alto Networks welcomes the opportunity to provide feedback on the effectiveness of the *Security of Critical Infrastructure (SOCI) Act*. As a global leader in cybersecurity, our perspective is informed by real-time threat intelligence from Unit 42 and our experience securing Australia's most vital entities. While the Act has successfully upli

fted the national "cyber floor," the rapid evolution of AI-enabled threats and adversarial speed necessitates a shift from periodic compliance to real-time, automated resilience.

---

1. Achieving Intended Objectives

Palo Alto Networks observes that the SOCI Act has been instrumental in maturing the cybersecurity posture of Australian industry.

- Elevation of Cyber Governance: The Act has successfully transitioned cybersecurity from a technical "IT issue" to a mandatory board-level risk through the Critical Infrastructure Risk Management Program (CIRMP).
- Defining the Baseline: By mandating the Register of Critical Infrastructure Assets, the Act has established a foundational level of visibility that was previously absent across several of the 11 designated sectors.
- Shift Toward Resilience: The "all-hazards" approach has effectively broadened the scope of protection beyond simple data breaches to include the continuity of essential services.

2. Functioning as Intended

While the legislative framework is robust, its operational application faces some friction in an increasingly complex regulatory environment.

- Regulatory Harmonisation: A key area for improvement is the overlap between SOCI, the Privacy Act, and sector-specific regulations (such as APRA's CPS 234). Entities are currently facing a "reporting tax" that diverts resources from active defense to administrative compliance. We advocate for a "Report Once" framework.
- Information Sharing: The Act functions best when it facilitates a two-way flow of intelligence. Palo Alto Networks encourages further integration between the Australian

Signals Directorate (ASD) and the private sector to ensure threat data is actionable and timely.
- Telecommunications Integration: We strongly support the recent legislative efforts to harmonise telecommunications security within the SOCI framework, ensuring a consistent national approach to network integrity.

3. Unintended Consequences

Palo Alto Networks identifies several areas where the Act may inadvertently create new risks:

- Compliance-First Mindset: There is a risk that the CIRMP creates a "checkbox" culture. If entities prioritise meeting legislative minimums over implementing Zero Trust architectures and AI-driven automation, they remain vulnerable to sophisticated actors who bypass static controls. Adopting or advocating for frameworks that seek to provide real-time continuous risk management (such as the US DoD continuous authority to operate framework) will provide a foundational capability to move with greater speed and agility against cyber threats and vulnerabilities.
- Adversarial Roadmaps: Overly prescriptive transparency requirements regarding specific network configurations or AI model logic can unintentionally provide a blueprint for attackers. Disclosure mandates must be risk-based to protect sensitive intellectual property and defensive strategies.
- Absence of Merits Review: The breadth of Government Assistance powers (Part 3A) remains a point of concern. Recommend a clear post-incident review/oversight mechanism in the rarest of instances, to ensure that the powers are used proportionately, without impeding urgent incident response and mitigation efforts.

4. Emergent Threats and Capability Gaps

The current form of the SOCI Act faces challenges from "machine-speed" threats that did not exist when the legislation was first drafted.

- The AI-Speed Breach: Unit 42 research indicates that 20% of breaches now involve data exfiltration within the first hour of compromise. The Act's 12-hour and 72-hour reporting windows, while useful for forensics, are insufficient for real-time national defense against AI-automated attacks.
- Agentic AI and Identity Risks: The rise of AI Agents creates a new class of "insider." If an agent with privileged access is compromised via prompt injection, it can execute high-velocity attacks within critical systems. The Act must evolve to include "AI Supply Chain" and "AI Agent Identity" within its risk management definitions. For example, the Act should look to mandate the adoption of AI governance frameworks that align with international industry-leading standards, specifically ISO/IEC 42001 and the NIST AI Risk Management Framework (RMF). By embedding these benchmarks into risk management definitions, the legislation ensures critical infrastructure entities adopt a structured, interoperable approach to mitigating "machine-speed" vulnerabilities and

agentic identity risks, bridging the gap between legacy compliance and modern, AI-driven operational resilience.

- Platformization vs. Tool Sprawl: Modern threats exploit the gaps between siloed security tools. The SOCI Act should incentivise integrated visibility —integrated security architectures that provide end-to-end visibility—rather than the adoption of disparate "point solutions" that increase the attack surface. This will assist having consolidated security architectures that reduce visibility gaps while enabling organisations to adopt technology with lower technical risk and in shorter timeframes. Ultimately lifting the cybersecurity posture of Australia in a short period of time.

Recommendations

1. Adopt "Secure by Design" AI: Update the CIRMP guidelines to include specific risk management protocols for the deployment of Generative AI and autonomous agents within critical infrastructure.
2. Streamline Incident Reporting: Implement a unified reporting portal to reduce the administrative burden on CISOs during active crisis management.
3. Incentivise Modernisation: Move beyond static compliance by incentivising the adoption of AI-driven SOCs and Attack Surface Management (ASM) to match the speed of modern adversaries by minimising the mean time to detect and mean time to respond.

Palo Alto Networks stands ready to further discuss these insights to ensure Australia remains a global leader in critical infrastructure resilience.

About Palo Alto Networks

As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organisations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, and security operations, enhanced by the expertise and threat intelligence of Unit 42. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at **www.paloaltonetworks.com**.

Further information: [redacted] at [redacted].