Strengthening Australia's National Resilience Through Intelligence-Led Regulation

Prepared by [redacted], on behalf of CI-ISAC Australia

EXECUTIVE STATEMENT

CI-ISAC Australia welcomes the Independent Review of the *Security of Critical Infrastructure Act 2018* (SOCI Act). As the only not-for-profit, member-owned, cross-sectoral Information Sharing and Analysis Centre (ISAC) in Australia, our submission is grounded in operational experience driving cyber resilience across all sectors of the critical infrastructure community.

Our central proposition is that the SOCI Act cannot fully achieve its national security objectives without embedded, mandatory, structured, and secure cross-sector Cyber Threat Intelligence (CTI) sharing.

While the SOCI Act has successfully established a compliance framework, it now needs to add the operational capability to function as an intelligence-driven national security system, particularly as threats escalate in terms of breadth, intensity, and speed. Furthermore, the significant proportion of Australian critical infrastructure under foreign ownership creates structural vulnerabilities — specifically regarding data visibility and potential foreign state influence — that the Act needs to address more directly.

This submission addresses the Review's four core questions on effectiveness, functionality, unintended consequences, and emerging threats, outlining the necessary transition from a compliance-centric regime to one grounded in real-time, sovereign intelligence.

Q1. IS THE SOCI ACT ACHIEVING ITS INTENDED OBJECTIVES?

Assessment: Partially. The Act has built the structural "skeleton" of national resilience but lacks the "nervous system" of real-time intelligence required to make it effective.

The Act has materially advanced the Commonwealth's ability to identify and manage risk by expanding coverage to 11 sectors and establishing the Register of Critical Infrastructure Assets. However, the objective of protecting Australia from espionage, sabotage, and coercion is not fully realised due to two critical gaps:

A. Lack of Sovereign Visibility

The effectiveness of SOCI is intrinsically linked to the quality and timeliness of intelligence. Currently, the government's visibility is uneven and reactive. Without mandatory CTI sharing, neither the government, nor operators can detect coordinated campaigns targeting shared dependencies (e.g., cloud providers, MSPs) until a major incident occurs. The objective of *prevention* is currently secondary to *reaction*.

B. The Foreign Ownership Blind Spot

A defining feature of Australia's critical infrastructure is the high level of foreign ownership. This creates a "sovereignty gap" where the Act's objectives are undermined by:

- **Data Opacity:** Foreign-owned entities often rely on offshore Security Operations Centres (SOCs), meaning threat data remains outside Australian jurisdiction.
- **Conflicting Obligations:** Foreign owners may be subject to intelligence collection laws in their home jurisdictions, or corporate policies that restrict reporting to Australian authorities.

Recommendation: To achieve its objectives, SOCI must mandate CTI sharing. This ensures the Commonwealth receives operationally relevant data in real-time, bypassing offshore legal or corporate bottlenecks and ensuring sovereign visibility over Australian assets.

Q2. IS THE SOCI ACT FUNCTIONING AS INTENDED?

Assessment: Structurally, yes – but operationally it is driving a "compliance checklist" culture rather than "threat-informed" defence. The legislative framework (Act, Rules, Guidance) is functioning, but the operational outcome is inconsistent.

A. Static vs. Dynamic Risk Management

The Critical Infrastructure Risk Management Programme (CIRMP) is intended to be a living defence strategy. However, without a continuous feed of actionable intelligence, many entities treat CIRMPs as static compliance documents.

- **The Gap:** Security controls are often generic rather than **threat-informed**. Entities are defending against hypothetical risks rather than the specific Tactics, Techniques, and Procedures (TTPs) currently being used by adversaries against their sector.
- **The Solution:** CIRMP obligations must be amended to explicitly require *intelligence-led* risk identification. Controls must be prioritised based on Australian-relevant threat intelligence, not just compliance frameworks.

B. The Public-Private Gap

The Cyber and Infrastructure Security Centre (CISC) functions well as a regulator, but government

cannot be the sole source of intelligence. Industry possesses the bulk of the telemetry but lacks a unified mechanism to share it.

- **The Role of CI-ISAC:** There is a missing layer between the regulator and the operator. CI-ISAC functions as this bridge, aggregating industry intelligence to support government situational awareness, while providing operators with the context needed to interpret government advice.

Q3. DOES THE SOCI ACT HAVE UNINTENDED CONSEQUENCES?

Assessment: Yes. The Act has created a high compliance burden that disproportionately affects smaller operators and reinforces siloed defences.

A. Disproportionate Compliance Burden

Stakeholder feedback indicates that the administrative burden of SOCI compliance is substantial. Smaller operators, who may lack cyber teams with access to threat intelligence, are overwhelmed by the requirement to identify "material risks" without the operational context to do so.

- **The Unintended Consequence:** Resources are diverted from operational security to compliance activities.
- **The Solution:** CTI sharing *reduces* this burden. By providing pre-assessed, contextualised threat data and shared playbooks, CI-ISAC reduces the analytical workload on individual entities. It allows smaller players to benefit from the "herd immunity" provided by larger, more mature operators who are collaborating to inform the national threat picture.

B. Sector Fragmentation

By regulating sector-by-sector, the Act unintentionally reinforces silos.

- **The Unintended Consequence:** A threat actor targeting the energy sector using a specific supply-chain vulnerability is often not visible to the water or transport sectors until it is too late. The Act currently treats these as separate risk environments, whereas adversaries treat them as a single attack surface.

Q4. IS THE ACT EFFECTIVE AT MANAGING NEW AND EMERGING THREATS?

Assessment: No. The current principles-based approach is too slow to counter cyber-enabled espionage, cross-sector supply chain attacks, and threats from foreign interference.

A. Horizontal Threats vs. Vertical Regulation

Modern adversaries operate horizontally, exploiting shared service providers and software supply chains to compromise hundreds of entities simultaneously. SOCI's vertical (sector-specific) structure is not designed to detect these systemic campaigns.

- **Emergent Threat:** Coordinated pre-positioning of malware in Operational Technology (OT) networks across multiple sectors, accelerated by Artificial Intelligence (AI).
- **Required Capability:** Only cross-sector CTI correlation can reveal these patterns. CI-ISAC provides the "horizontal" view that the vertical approach by the regulator misses and provides an opportunity to better address the systemic impact of emerging threats impacting multiple critical infrastructure sectors.

B. Foreign Interference and Coercion

The risk of foreign interference has evolved beyond simple espionage to active coercion.

- **Emergent Threat:** External nation-states pressuring foreign-owned operators to delay incident reporting, withhold forensic data, or manipulate infrastructure availability during geopolitical tensions.
- **The Gap:** The Act currently relies on the *goodwill* of the operator to report. If the operator is compromised by its own parent company or state influence, the SOCI Act is rendered unenforceable, effectively stripping it of its powers.
- **Required Capability:** A "Foreign Influence Exposed" category for assets is required, mandating stricter CTI sharing and domestic data retention to ensure Australia retains control, especially during a crisis.

RECOMMENDATIONS

To address these gaps and ensure the SOCI Act remains fit for purpose, CI-ISAC Australia recommends the following reforms:

1. Mandate Cyber Threat Intelligence (CTI) Sharing

Insert a new Part into the Act creating a statutory obligation for Responsible Entities to participate in approved CTI-sharing mechanisms. This transforms SOCI from a static compliance regime into a dynamic, intelligence-led system.

2. Formally Recognise CI-ISAC as an Official CTI Partner

The Act should define CI-ISAC as an "Approved Intelligence Sharing Organisation." This would:

- Bridge the gap between public and private sectors.
- Provide liability protections for entities sharing intelligence in good faith.

- Allow the government to leverage CI-ISAC's cross-sector visibility to inform national security decision-making.

3. Mandate Threat-Informed Security Controls

Amend CIRMP Rules to require that risk identification and control selection be explicitly informed by current threat intelligence. This ensures defences evolve at the same speed as the adversary.

4. Establish a "Foreign Influence Exposed" Category

Create a specific category for assets with material offshore control or exposure to foreign intelligence laws. These assets should face enhanced obligations, including:

- Mandatory domestic retention of security logs (Data Localisation).
- Strict requirements for local autonomy during crisis scenarios.
- Segmented access to national intelligence to prevent leakage to foreign states.

CONCLUSION

The *Security of Critical Infrastructure Act 2018* was a necessary and welcomed evolution in Australia's national security posture, but the threat landscape of 2025 has outpaced the regulatory model. SOCI is a robust framework for compliance, yet it lacks the operational machinery for genuine resilience. The Review should support the SOCI Act evolving into a dynamic, intelligence-led system that builds resilience.

This submission has demonstrated that the "missing capability" within SOCI is not more regulation, but better intelligence. Without a statutory mandate for cross-sector Cyber Threat Intelligence (CTI) sharing, our national defence remains reactive, siloed, and dependent on the goodwill of private operators, many of whom are foreign-owned or influenced. Australia requires sovereign visibility over its own assets, independent of foreign corporate structures and foreign national allegiances.

CI-ISAC Australia is ready to help the Government operationalise this shift by enabling a trusted sharing community backed by world-class Cyber Threat Intelligence to bridge the gap between the public and private sectors. By mandating CTI sharing and formally integrating CI-ISAC into the SOCI framework, the Commonwealth can ensure that Australia's critical infrastructure is not merely compliant on paper but actively defended in practice.

APPENDIX A: OPERATIONAL SUCCESS OF THE HEALTH SECTOR ISAC (HS-ISAC) PILOT

Supported by the Health Sector Information Sharing and Analysis Centre Acceleration Grants Program, CI-ISAC Australia has successfully operationalised the Health Cyber Security Network (HCSN). Within 11 months, this initiative has transitioned from a pilot concept to a national capability, delivering a world-leading cyber resilience model for the Australian health sector.

As a key initiative under Horizon 1 of the *2023-2030 Australian Cyber Security Strategy*, the project has achieved critical mass. It now provides threat intelligence coverage to an estimated 475 hospitals and health facilities, securing representation from five of the eight state and territory jurisdictions and four of the nation's seven largest private hospital groups so far.

1. Market Coverage and Stakeholder Engagement

The pilot has achieved systemic integration across the healthcare ecosystem, moving beyond early adopters to secure major infrastructure providers.

- **Critical Mass:** Secured 50 memberships, representing 50% of the revenue required for sustainability, validating the commercial viability of the model beyond the three-year grant period.
- **Public Sector Reach:** Established memberships with central health departments and digital health agencies in **Victoria, NSW, WA, Tasmania,** and the **ACT**. This provides a channel of influence into approximately 397 public hospitals (~57% of the national public network).
- **Private Sector Leadership:** Secured memberships with **Healthscope, St Vincent's Health Australia, Mater Group, and Epworth HealthCare**. These four partners alone represent over 10,000 hospital beds and ~30% of Australia's total private sector bed capacity.
- **Primary Care & Regional Reach:** Partnered with major Primary Health Networks (PHNs) and Local Health Districts (LHDs) across the East Coast and the **Royal Flying Doctor Service** (QLD and VIC), ensuring intelligence reaches regional and remote clinics.
- **Supply Chain & Industry:** Onboarded critical infrastructure providers including **Sonic Healthcare, Telstra Health and Best Practice Software, and EBOS Group.**

2. Operational Capabilities Delivered

The pilot has successfully bridged the gap between strategic policy and operational reality, delivering a "sovereign capability" that addresses specific health sector needs.

- **Speed and Pre-emption:** The pilot has reduced the "time-to-mitigation" by up to 12 hours. Major hospital networks report receiving CI-ISAC advisories for critical vulnerabilities significantly ahead of other state and commercial notifications.
- **Intelligence Volume:** CI-ISAC has disseminated over **71,000 technical indicators** via automated feeds, with over 34,000 sourced primarily by our National Intelligence Office.
- **Bi-Directional Government Integration:** The pilot has bridged the "consumption gap" for technical sources. CI-ISAC ingests data from multiple sources, curated for health-sector relevance, and delivers via feeds and contextual advisories based on member maturity.
- **OT and IoT Visibility:** Unlike standard IT feeds, CI-ISAC provides niche visibility into medical OT. Advisories have covered medical imaging software and life-support infrastructure, identifying vulnerabilities in "crown jewel" assets often overlooked by traditional security vendors.

3. Strategic Outcomes and National Impact

The pilot has delivered measurable outcomes against the objectives of the Cyber Security Strategy:

- **Addressing Security Inequity:** The pilot acts as an "outsourced threat intelligence capability" for resource-constrained entities. Feedback confirms that 15–20% of advisories trigger technical action in smaller organisations that lack internal cyber teams.
- **Breaking Silos (Collective Defence):** The project has replaced competitive isolation with collaboration. Major medical insurers and hospital groups are now sharing incident details and indicators into CI-ISAC, which lowers collective risk.
- **Supply Chain Transparency:** By onboarding medical software vendors and sharing intelligence with Managed Service Providers (MSPs), the pilot captures threat data "upstream." When a vendor hardens their environment based on CI-ISAC intelligence, it effectively protects the hundreds of clinics they service.
- **Commercial Sustainability:** The sector views CI-ISAC as an essential service, not a subsidised trial. With a 70% conversion rate from proposals to signed memberships and a strong forward-looking revenue forecast, the capability is on track to be self-sustaining by the conclusion of the grant.

Conclusion

The HS-ISAC pilot has proven that a sector-specific, not-for-profit, member-owned intelligence network is the most effective mechanism for uplifting national resilience. By aggregating intelligence from opaque areas — specifically regional health, supply chains, and medical OT — CI-ISAC provides visibility that central government agencies cannot achieve alone. The success of this pilot provides a blueprint for accelerating this model across additional critical infrastructure sectors in 2026.