CI-ISAC's Statement on the Independent Review into the *Security of Critical Infrastructure Act* 2018

600+	Majority	Rec. 6A
TISN roundtable participants	favour mandatory cyber threat intelligence sharing across all sectors	mandates bidirectional govt–industry exchange

Australia's window to build genuine sovereign cyber capability is open. Dr Jill Slay AM's Independent Review of the *SOCI Act* 2018 has delivered a clear mandate: mandatory cyber threat intelligence sharing, bidirectional government–industry exchange, and a wholesale shift from compliance culture to proactive security culture. **The Government has accepted all six recommendations in principle**. CI-ISAC is positioned to provide the institutional architecture to make these recommendations an operational reality.

> *"The SOCI Act is too reactive and too slow compared to evolving risks — despite multiple previous modifications."*
> — Dr Jill Slay AM, Independent Review

WHAT THE REVIEW FOUND

The verdict is unambiguous. 70% of stakeholder sentiment about the SOCI Act was negative; not about the Act's intent, but its inability to keep pace. Nation-state actors, AI-enabled attacks, and supply chain compromises have fundamentally changed the threat landscape since 2018. The Act has not kept up.

Beneath the structural lag of the legislation sits a cultural failure: compliance has displaced security. Boards don't engage. Practitioners attest without conviction. Penalties are unenforced. The review's fix is structural: real enforcement, and a bidirectional intelligence model that makes the adversary *visible* to critical infrastructure operators, not just to government.

The key recommendations:

- Rec. 5 mandates CTI sharing across all sectors.
- Rec. 6A requires two-way cyber threat information exchange between government and operators
- Rec. 2 introduces a penalty-based compliance regime where demonstrated participation in sector intelligence sharing carries direct regulatory credit.

CI-ISAC: BUILT FOR EXACTLY THIS MOMENT

CI-ISAC is Australia's only cross-sector, not-for-profit cyber intelligence sharing organisation. We are an active, operating network delivering threat advisories, vulnerability feeds, MITRE ATT&CK-mapped intelligence, and real-time situational awareness to critical infrastructure operators daily. Beyond our intelligence advisories, we provide a direct capability uplift through knowledge items, structured technological integrations and support to stretched cyber teams — *returning hours to teams that can't afford to lose them*.

The Health Cyber Security Network (HCSN) proves the model at scale. Commissioned by the Department of Home Affairs to test whether the health sector warranted a dedicated intelligence capability, CI-ISAC delivered. Health is now our largest sector: 60+ member organisations, 600+ facilities, spanning hospitals, pathology, digital health infrastructure, and the medical supply chain, operationalised in under a year. When the Review describes health as simultaneously the most targeted, most under-resourced, and most consequentially exposed sector in Australia, it is describing exactly the gap the HCSN was built to close.

The HCSN model is the template for how Rec. 5 and 6A get implemented across every regulated sector: government and industry contribute threat information into the network; CI-ISAC operationalises, contextualises, and distributes actionable intelligence at the speed the threat environment demands. Bi-directionality is not a new concept for us; it is fundamentally how we operate.

THE OPPORTUNITY AND THE RISK

The reform process will determine whether this moment produces genuine national capability or another layer of compliance overhead. The institutional architecture question *must* be resolved in favour of what already works.

The US experience is a warning: CISA's enabling statute has operated on short-term congressional extensions since September 2025. A sovereign capability contingent on short-term government funding cycles is not sustainable. Australia can build it's own enduring capability differently.

Three things CI-ISAC is calling for in the reform process:

- **Mandate participation in CI-ISAC's cross-sector intelligence network** as the delivery mechanism for Rec. 5 and 6A; not a new government-built structure that replicates what exists.
- **Formalise bidirectional exchange** through CI-ISAC's platform: government and cross-sector sightings in, actionable intelligence out across critical infrastructure sectors
- **Credit participation in enforcement decisions,** as proposed by Rec 6A. Operators engaged with the network should carry demonstrable regulatory advantage under the incoming penalty regime.

The Review has set the course, and the Government has signaled its intent. The question for critical infrastructure operators is no longer **if** these changes are coming, but **how** they will be operationalised. CI-ISAC offers the only proven, industry-led architecture ready to turn these recommendations into an immediate defensive advantage.

To discuss how your organisation can leverage our cross-sector network, and secure the regulatory credit proposed in the reforms, reach out to our team today. With Tranche 1 consultations closing on 1 May 2026, and Tranche 2 opening soon after, the window to shape Australia's sovereign cyber future is now.

https://ci-isac.org.au/contact-us/