CI-ISAC
AUSTRALIA

THE FUTURE OF CYBER RESILIENCE

Australia's Cyber Threat Intelligence Hub for Critical Infrastructure

PROSPECTUS | JUN 2025

www.ci-isac.org.au

A MESSAGE FROM THE CEO

A United Front Against Cyber Threats

The 2023-2030 Australian Cyber Security Strategy rightly calls for a new era of collaboration. At CI-ISAC Australia, we are answering that call with proven results. As Australia's only sovereign, not-for-profit, and industry-led Information Sharing and Analysis Centre (ISAC) dedicated to all critical infrastructure sectors. We were established to fill a vital gap – to build a united, proactive defence capability to protect the nation's most essential services.

Our track record of fostering collaboration across diverse critical infrastructure sectors has positioned us as the natural choice to lead sector-specific initiatives under the national strategy. This expertise was recognised on 29 January 2025 when CI-ISAC was announced as the recipient of an Australian Government grant to scale-up a health-specific Information Sharing and Analysis Centre (HS-ISAC) for Australia's healthcare industry.

This Healthcare sharing capability represents a direct implementation of the Australian Cyber Security Strategy 2023-2030's collaborative vision. The pilot program specifically targets Healthcare as a sector requiring support to achieve cyber maturity. CI-ISAC is leveraging our proven methodology of sharing and collaborating across sectors to deliver actionable insights to our new Health members.

This world-first approach demonstrates how our cross-sectoral experience translates into targeted solutions that strengthen Australia's overall cyber resilience while addressing the unique challenges of individual Critical Infrastructure sectors.

David Sandell
Co-founder | CEO, CI-ISAC Australia

THE UNSEEN BATTLEFIELD: AUSTRALIA'S CRITICAL INFRASTRUCTURE UNDER SIEGE

Cyber-attacks against Australian critical infrastructure are growing in number, speed, and sophistication. The stakes are significant, impacting not just the private and public sectors, but consumer confidence, societal trust, and in the case of a catastrophic cyber event, our very way of life.

As Lieutenant General Michelle McGuiness said at the 2025 AUSCERT Cyber Security Conference, the nation needs to prepare for a catastrophic cyber incident that cripples the nation and has long-lasting effects.

Financially motivated cyber-criminals, state-based actors, and issue-motivated groups are routinely targeting our networks and data. The disruptions and privacy implications to critical infrastructure operators and government systems is cause for grave concern. This isn't just an Australian problem; it's a global trend, with attackers indiscriminately targeting essential sectors like healthcare, energy, finance, and telecommunications.

In this rapidly evolving landscape, relying on fragmented information sharing, or informal groups will always mean we are a step behind.

With constrained cyber resources and time, a collective, intelligence-led approach is no longer a luxury; it’s a necessity to move away from reactively responding to cyber incidents as they occur.

12%	increase in reported cyber incidents targeting Australian companies in FY2023-24 financial year
› 36,700	calls to the ASD Cybersecurity hotline
11%	of incidents directly impacted Critical Infrastructure

Source: 2024 ASD Annual Cyber Threat Report

THE LIMITS OF ISOLATION: WHY TRADITIONAL DEFENCES FALL SHORT

Beyond Your Own Walls: The Power of Collective Insight

While individual organisational security is crucial, today's complex cyber threat landscape often outpaces isolated approaches to cyber defence. Many organisations find themselves:

- ⚠ **Drowning in data, starved for intelligence:** Sifting through raw threat information (IP addresses, CVEs) without context is overwhelming. Actionable intelligence – understanding the 'who, what, why, and how' – is what truly empowers effective defences.
- ⚠ **Trapped by Informal Sharing Pitfalls:** Unstructured sharing on casual platforms lacks the security, contextualisation, and analytical rigour needed for critical infrastructure. These sources can lead to information overload, inconsistent quality, and even compliance risk management.
- ⚠ **Missing cross-sectoral attack patterns:** Cyber threats don't respect sectoral boundaries. An attack on one CI entity can be a precursor for another. Siloed sharing within sectors misses these critical cross-sectoral patterns and opportunities to proactively get ahead of threats.

**Isolated efforts can only see part of the threat.
Collective intelligence reveals the full picture**

What is Cyber Threat Intelligence?

CTI transforms raw security data into actionable insights that enable proactive defence. Rather than simply knowing that a threat exists, CTI provides the critical context: who is behind the attack, what their methods and motivations are, how they operate, and what this means for your specific environment.

It's the difference between receiving a flood of IP addresses and understanding that a particular threat actor is systematically targeting your sector using specific techniques.

What makes Threat Sharing Effective?

1. trusted sources that provide reliable, timely information;
2. analytical rigour that contextualises threats within your operational environment;
3. collaborative sharing that reveals cross-sector attack patterns;
4. collective learning that prevents organisations from repeating costly mistakes already made by others.

When CTI works properly, one organisation's hard-learned security lesson becomes protective intelligence for the entire community, accelerating defensive maturity across sectors.

INTRODUCING CI-ISAC AUSTRALIA: YOUR PARTNER IN CYBER RESILIENCE

CI-ISAC Australia: Uniting for a Stronger Defence

CI-ISAC Australia is the nation's only sovereign, not-for-profit, industry-owned, and led cyber intelligence sharing community, exclusively focused on owners and operators of Australia's critical infrastructure and their material suppliers.

We provide a trusted, ecosystem for harnessing the collective insights of all CI sectors, coupled with a world-leading Threat Intelligence capability to enrich and contextualise member-shared information.

OUR VISION

to be Australia's trusted cyber intelligence platform for Critical Infrastructure, strengthening national resilience through collaborative defence

OUR MISSION

As Australia's only sovereign, industry-led Information Sharing and Analysis Centre for Critical Infrastructure, we connect owners, operators and suppliers to share actionable operational threat intelligence and build collective cyber resilience

KEY CHARACTERISTICS

World-Class Threat Sharing

Access real-time, actionable intelligence.

Protected Critical Infrastructure

Get ahead of cyber-attacks.

Sovereign Capability

Australian-focused, data sovereign, supporting our national interests.

THE CI-ISAC ADVANTAGE: HOW WE DELIVER UNIQUE VALUE

COLLECTIVE STRENGTH
TANGIBLE BENEFITS

COLLECTION

Trusted & Secure CTI Sharing:

We provide a trusted, independent environment to securely gather and disseminate contextualised Cyber Threat Intelligence (CTI) across all CI sectors. Our accessible Member Portal and Threat Sharing Platform for machine-to-machine sharing, ensures timely and relevant information reaches you effectively.

ANALYSIS BY NIO

Actionable Intelligence, Not Just Data:

Our National Intelligence Office (NIO) is the analytical heart of CI-ISAC. The NIO interprets raw data from members and diverse sources, contextualises threats, and provides clear, actionable advisories and strategic insights, reducing the cognitive burden on your team.

INTELLIGENCE

Collective Defence & Proactive Posture:

CI-ISAC harnesses collective insights to enable true collective cyber defence. We help your organisation move from a reactive, incident-driven approach to a proactive, threat-led posture, allowing you to get ahead of attackers.

ACTION

Commercially Safe & Collaborative Ecosystem:

CI-ISAC enables you to operate within a commercially safe environment with IP and liability protections. Our culture fosters participation and collaboration, ensuring no member is left behind. You benefit from our dedicated member services team, expert partners, and the strategic guidance of our Industry Advisory Group (IAG).

RESULTS

Sovereign Focus, National Impact:

As a sovereign capability, CI-ISAC prioritises Australia's national interests and data sovereignty. Our unique cross-sectoral model is ideal for Australia's landscape, recognising that cyber threats often transcend industry silos, and collective visibility is key.

> “CI-ISAC ENABLES MORE OF A STORY AROUND THE CYBER-ATTACKS IMPACTING AUSTRALIA, ANALYSIS AND INDICATORS ARE TIED TO RELEVANT ATTACKS, WHICH HELPS US RESPOND."
>
> *- Healthcare member -*

> THESE ARE THE HIGHEST QUALITY ADVISORIES THAT WE RECEIVE. 15-20% OF ADVISORIES ARE BEING USED. THE ADVISORIES HAVE HIGHLIGHTED AND EXTENDED OUR EFFORTS TO UNDERSTAND THE GAPS IN VISIBILITY OF OUR OT ENVIRONMENTS.
>
> *- Healthcare member -*

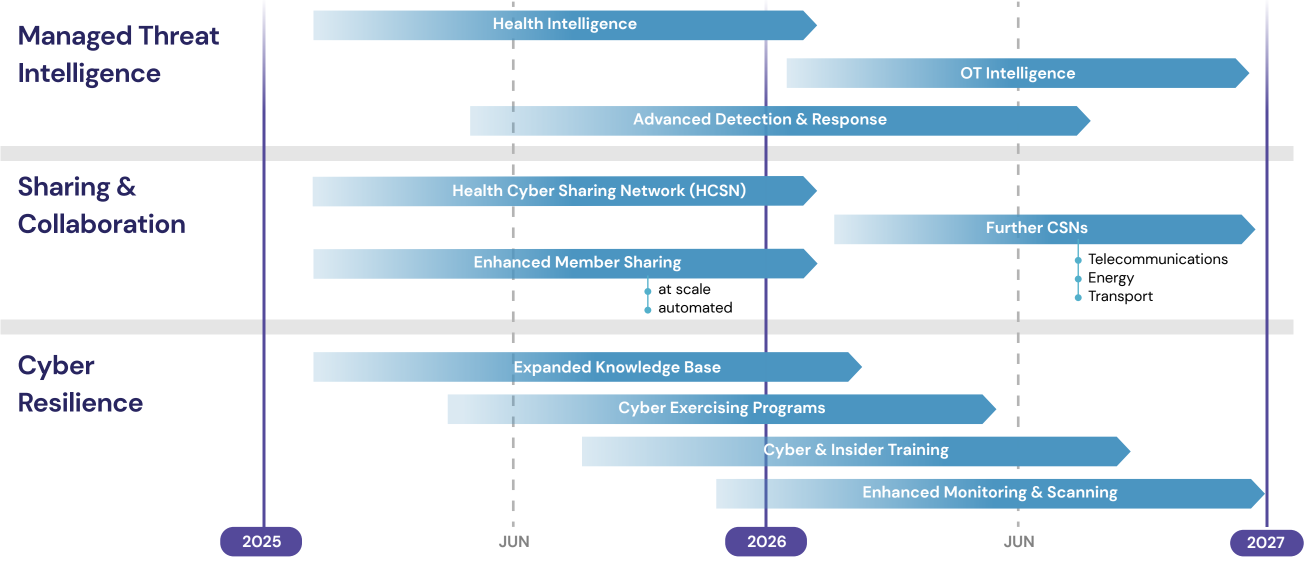
OUR EVOLVING VALUE
CORE SERVICES & CAPABILITIES

Empowering Your Defence

CI-ISAC delivers a robust suite of operational services designed for immediate impact, with a clear roadmap for continuous enhancement to meet evolving member needs.

SERVICES	CURRENT OFFERINGS
Managed Threat Intelligence *Cyber Threat Intelligence that enhances teams' ability to rapidly assess relevant threats and proactively defend their environments.*	• Threat & Vulnerability Advisories • Strategic Insights • Technical Reporting • Cyber & Intelligence Briefings • Threat Sharing Platform (TSP) • Automated Threat Feeds (IOCs) • Commercial & Closed Intel Sources • Analyst on Demand
Sharing & Collaboration *Trusted cyber sharing networks (CSNs), facilitated by CI-ISAC to encourage sharing and collaboration to benefit all AU CI entities.*	• National & Sector-Specific Threat Sharing Forums • Analyst Collaboration Sessions • Legal/Technical/Procedural Protections • Accessible Sharing
Cyber Resilience *Resources and capabilities built by CI-ISAC and informed and guided by members to build defences and resilience across CI.*	• Feature-Rich Member Portal • 700+ Advisories Developed

ROADMAP HIGHLIGHTS



PROOF IN ACTION: THE HEALTH CYBER SHARING NETWORK (HCSN)

Capability in Action

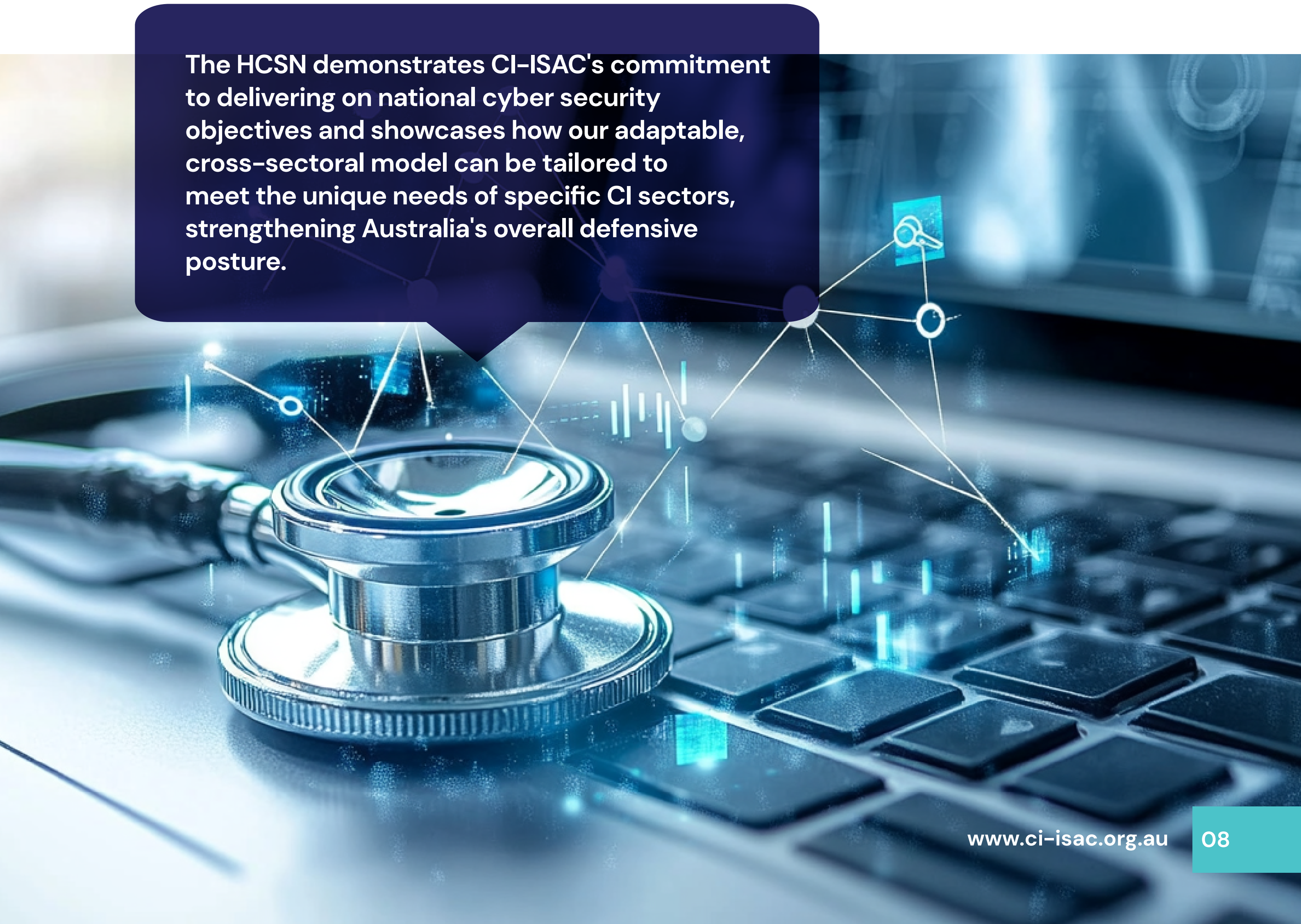
CI-ISAC's capability and trusted model are recognised at the highest levels. As part of the 2023-30 Australian Cyber Security Strategy, CI-ISAC was awarded a significant grant to establish and operate the Health Cyber Sharing Network (HCSN).

This initiative leverages CI-ISAC's existing sovereign infrastructure and deep expertise to rapidly enhance the cyber resilience of Australia's vital healthcare sector.

HCSN Attributes:

- A health-specific focus to drive targeted sharing across the diverse health ecosystem.
- Uplifting capabilities through tailored intelligence, knowledge resources, training, and cyber exercises.
- Fostering industry-to-industry sharing in a secure, collaborative environment.

The HCSN demonstrates CI-ISAC's commitment to delivering on national cyber security objectives and showcases how our adaptable, cross-sectoral model can be tailored to meet the unique needs of specific CI sectors, strengthening Australia's overall defensive posture.



WHO WE SERVE & MEMBERSHIP BENEFITS

Join a Community Protecting Australia's Future

CI-ISAC supports owners and operators across all 11 of Australia's Critical Infrastructure sectors, government entities (federal, state, and local), and their material suppliers. Our ecosystem is designed for organisations of all sizes and cyber maturity levels.

KEY MEMBERSHIP BENEFITS:

Reduce Risk

Prioritise resources by focusing on mitigating the risks that matter most.

Save Money & Resources

Free up internal teams by leveraging expert, contextualised intelligence.

Proactive Defence

Shift from reacting to incidents to proactively anticipating and preventing them.

Enhanced Situational Awareness

Gain unparalleled cross-sectoral insights into the threat landscape.

National Contribution

Play a direct role in strengthening Australia's collective cyber defences.

Membership Tiers:

Membership is structured to be accessible and provide value for money. Tiers are based on your organisation's size and type (Private Sector, Public Sector, Small to Medium Business). For detailed membership tiers and benefits, visit the following URL:

ci-isac.org.au/membership

Health Sector Focus:

Organisations in the Healthcare Sector can join the Health Cyber Sharing Network (HCSN) for free until February 2026, view more information:

ci-isac.org.au/hcsn

OUR COMMITMENT & GOVERNANCE

Your Trusted Partner in Cyber Defence

Our NFP Commitment & Governance:

As a public, not-for-profit, member-driven organisation, CI-ISAC reinvests all revenue into enhancing services and CTI sharing capabilities for our members. Our strategic direction is guided by a dedicated Management Board and informed by our Industry Advisory Group, ensuring we remain aligned with member needs. We have built a loyal membership base across Australia's critical infrastructure sectors over the last three years.

The Time to Act is Now

The cyber threat to Australia's critical infrastructure is real and growing. Collective action is our strongest defence. Join a rapidly growing community of over 150+ organisations committed to a stronger, more resilient Australia

Take the Next Step:

Request a Briefing

Submit an Expression of Interest (EOI) for a confidential discussion about your organisation's needs and receive a personalised briefing

SUBMIT EOI

Explore Membership

Visit our website to learn more about how CI-ISAC can empower your cyber defences.

MORE INFORMATION

Connect With Us

Direct any queries to the team, and we'll be in touch.

EMAIL US

CI-ISAC AUSTRALIA

Contact Information:

p. 1300 556 210
e. info@ci-isac.org.au

Office:

CI-ISAC Australia HQ
Suite 8, 84 Wises Road,
Maroochydore QLD 4558

CI-ISAC Sydney:
81-83 Campbell Street,
Surry Hills NSW 2010

www.ci-isac.org.au

#StrongerTogether