CI-ISAC AUSTRALIA

CRITICAL INFRASTRUCTURE

Information Sharing and Analysis Centre

PROSPECTUS

JULY 2024

THE FUTURE OF CYBER STRENGTH

CI-ISAC Australia is a not-for-profit, cyber intelligence sharing community focused on owners and operators of Australia's critical infrastructure.

By providing timely and actionable intelligence, CI-ISAC enhances the cyber defences of all members, ensuring none are left behind.

This self-sustaining ecosystem effectively anticipates, mitigates, and responds to cyber threats to Critical Infrastructure.

THE FUTURE OF CYBER STRENGTH

#strongertogether

With the diversity, sophistication, and volume of cyber-attacks growing each day, it is imperative that Australia's Critical Infrastructure companies strengthen their cyber risk management posture.

The Australian Government has responded to increased cyber threats by introducing legislative and regulatory reforms to the nation's Critical Infrastructure (CI) sectors, recognising that Cyber Threat Intelligence (CTI) sharing and collective cyber defence are fundamental to improved risk management.

Membership of the Critical Infrastructure Information Sharing and Analysis Centre (CI-ISAC) is that fundamental cyber risk mitigation measure - addressing cyber security weakness that simply cannot be risk-accepted by Australian CI companies and their executives.

CI-ISAC has been established in Australia to harness the collective insights of all CI sectors to provide an information-sharing capability to enable collective cyber defence for its members. We are building a robust, highly-trusted intelligence-sharing community and cyber capabilities for critical infrastructure operators within and across all sectors.

CI-ISAC is a not-for-profit entity that represents an opportunity for industry to self-organise and uplift their own cyber defences in a trusted, sustainable manner. CI-ISAC is purpose driven with a vision that is in harmony with the Commonwealth objective to make Australia the most cyber secure nation by 2030.

The ISAC model has been proven effective over the last two decades as sector-specific US ISACs expanded globally. CI-ISAC has evolved the standard ISAC model to operationalise the world's first cross-sectoral ISAC, focussed on providing enabling capabilities and structures to support the collective defence of Australian CI.

The strength and utility of an ISAC is directly related to the number of members it has brought together and the diversity of insights and knowledge that these members bring to the ISAC's intelligence sharing platform.

CI-ISAC has achieved a first-tranche of members. Threat intelligence sharing is underway and we invite all of Australia's Critical Infrastructure owners and operators to join this growing community.

Stephen Beaumont AM

BOARD AND CEO

CEO | Co-Founder
Mr David Sandell

Director
Ms Helaine Leggat

Chair of the Board
Mr Stephen Beaumont AM

Advisor to the Board
Dr Gary Waters

Co-Founder
Dr Scott Flower

OUR MISSION

The Critical Infrastructure Information Sharing and Analysis Centre (CI-ISAC) Australia is the only data sovereign cyber intelligence sharing community focused on owners and operators of Australia's Critical Infrastructure and material suppliers.

The community's mission is to help ensure the cyber resilience and continuity of Australia's Critical Infrastructure by supporting entities to share information and provide central supporting capabilities to protect against malicious cyber acts.

As a not-for-profit, member-driven and supported organisation, CI-ISAC serves its members and in turn all Australians by building a trusted, self-sustaining cyber community. Innovative technology, resiliency resources and industry peer-to-peer networks are leveraged to anticipate, mitigate, and respond to cyber threats.

OUR VALUES

TRUST

We are a trusted custodian of members' sensitive information and advisor to support cyber resilience and contribute to collective cyber defences.

INTEGRITY

We take responsibility for safe and secure operations and strive for the highest ethical standards and integrity that underpins our decisions.

AGILITY

We are able to move, think and adapt quickly as we partner with members to innovate based on their needs and environmental changes to the threat landscape.

EXCELLENCE

We exceed best practices in ensuring excellence in the quality of our products, services and interactions.

WHAT MAKES CI-ISAC UNIQUE?

CI-ISAC Australia is the only cyber intelligence sharing community focused on owners and operators of Australia's Critical Infrastructure and material suppliers.

Innovative technology, resiliency resources and industry peer-to-peer networks are leveraged to anticipate, mitigate, and respond to cyber threats.

- Developed as a whole-of-nation, sovereign capability run by industry for industry.
- CI-ISAC strives to leave no member behind, pledging to support all members equally.
- Low barrier to entry, both to share information and gain value from advisories.
- CI-ISAC is the only cross-sectoral ISAC globally.
- Quality over quantity, strict focus on actionable intelligence and removing noise.
- Australia-first threat-focus, augmented by Global perspectives.
- A trusted data-sovereign environment, keeping member intelligence in Australia.
- Primarily focused on operational outcomes that uplift defences for our membership.
- Context and accessibility of intelligence form the core of our advisories and reporting.
- Provides a constant, independent and trusted partner to support the industry to uplift collective defences.

STRENGTH IN NUMBERS

Critical Infrastructure owners and operators will join CI-ISAC for a range of reasons:

- Strengthen their **cyber and business risk management posture**
- Access **cross-sectoral contextualised intelligence**
- Building **trusted peer-to-peer industry cybersecurity relationships** in their own unique CI sector, as well as increasing the opportunity to engage with other private and public sector experts.
- Be better prepared for crises by **receiving early warnings and strategies** to address potential incidents.
- Evolve from a reactive, incident-driven, approach to becoming **threat-led to stay ahead of attackers** proactively.

CORE SERVICES

- Threat & information sharing
- Actionable threat advisories
- Member briefings
- Threat & strategic reports
- Cyber capability resources
- Community events

KEY BENEFITS

Business risk mitigation measure – rapid sharing of contextualised CTI and provision of 'turn-key' capabilities and solutions that address legislative and regulatory requirements.

Satisfy legislative & regulatory reform – As the Australian government calls on the nation's Critical Infrastructure companies to have access to relevant, timely and contextual Cyber Threat Intelligence and information sharing.

Trusted CTI sharing – The ability to form a trusted environment to securely and independently gather and disseminate CTI across all CI sectors.

Value for money – Many single-sector ISACs do not offer value as these would introduce more overheads and result in less CTI sharing. CI-ISAC offers a lean, well-governed ecosystem to service all CI operators and optimise CTI sharing.

Alignment with existing federal initiatives – TISN and CTIS span industry sectors, and CI-ISAC complements these to extend their reach by acting as a cross-sectoral, trusted intermediary.

Geographic focus - Australia does not have the scale to warrant single-sector ISACs, which work well in the US, where individual sectors dwarf the entire Australian CI ecosystem.

Extended Reach – Cyber threats are not sector-specific; a cyber-attack in one sector will likely impact other CI sectors. Mature players are already analysing threats across sectors, and CI-ISAC extends this visibility to all CI companies, regardless of size.

Unparalleled insights – Operating a truly cross-sectoral information-sharing ecosystem in the form of CI-ISAC enables analysis of threats as they emerge, enabling effective risk management to proactively uplift security controls and inform incident response when attacks occur.

Central enabling capabilities – CI-ISAC provides the framework, capabilities, and coordination to support mature players to lead intelligence sharing for their sector and leverage the network effects of all members to inform capability build.

MEMBERSHIP TIERS

CI-ISAC leverages membership fees to promote the collective uplift of all critical infrastructure defences, and as such members of all tiers gain access to the same core services. Membership is broken down into tiers representing the varying sizes of member organisations. Your CI-ISAC contact will be able to confirm fees based on your organisation size.

PRIVATE SECTOR

Membership tiers are based on the higher value of member's employees, or revenue/budget.

	Employees	Revenue / Budget	Seats
Tier 1	10,000+	> A$500m	15
Tier 2	3,500-10,000	< A$500m	10
Tier 3	1,000-3,499	< A$250m	7
Tier 4	200-999	< A$50m	3

PUBLIC SECTOR

Membership tiers are based on the higher value of a member's serviced population or annual budget.

	Population	Budget	Seats
Tier 1	> 500k	> A$500m	15
Tier 2	250k-500k	< A$500m	10
Tier 3	100k-250k	<A$250m	7
Tier 4	20-99k	< A$100m	3

SMB / NOT-FOR-PROFIT / CHARITIES

Membership tiers are based on the higher value of member's employees, or revenue/budget.

Charities are capped at Tier 1 unless their revenue exceeds A$100m annually

	Employees	Revenue / Budget	Seats
Tier 1	< 200	< A$25m	1
Tier 2	< 100	< A$10m	1
Tier 3	< 50	< A$5m	1
Tier 4	< 20	< A$2m	1

MSP / MSSP / MATERIAL SUPPLIERS

Membership tiers are based on the higher value of member's employees, or revenue.

	Employees	Revenue / Budget	Seats
Tier 1	> 3,500	> A$500m	15
Tier 2	< 3,500	< A$500m	10
Tier 3	< 1,000	< A$50m	5

CI-ISAC partners are priced based on organisation size (employees/revenue), with additional sponsorship opportunities becoming available as CI-ISAC matures.

https://www.ci-isac.org.au/

FAQS

What does CI-ISAC do?

We provide a mechanism for national collective defence for the Critical Infrastructure community. A cyber threat intelligence (CTI) sharing community solely focused on industry owners and operators of Australia's Critical Infrastructure to deliver collective cyber defence. (**collective cyber defence**).

The ability to facilitate an industry-led trusted environment to securely and independently gather and disseminate CTI across all CI sectors (**trusted CTI sharing**).

A commercially safe environment where Intellectual Property (IP) and liability protections exist (**commercially safe**).

Operational processes and technical capabilities enable sharing of contextualised CTI and the 'turn-key' capabilities that address member needs (**rapid and relevant operational outcomes**).

A transparent and open culture that encourages behaviours of participation, collaboration, and cooperation between members (**collaborative behaviour**).

Why is it different to services the Government / others provide in this space?

Draws on the collective insights of all CI sectors and creates an information-sharing capability to enable collective cyber defence for members. CI-ISAC augments existing public/private engagements such as TISN and CTIS by focusing on driving operational cyber defence through collective intelligence capabilities.

Central functions drive intelligence sharing and quality, reduce information overload and enable informed risk-based decision making. CI-ISAC takes a 'partner first' approach with complementary communities / services and works to establish a memorandum of understanding (MOU) to incorporate these into our ecosystem and benefit all members.

Who can be members?

CI-ISAC seeks to assist the 11 sectors and 22 asset classes that now constitute Australia's critical infrastructure sector as defined by the SOCI Act, some 11,000 affected entities. It also caters for the Australian government (local, state, federal) in which all critical infrastructure resides.

Phase two will see material suppliers to critical infrastructure (MSPs, MSSPs) incorporated into the CI-ISAC ecosystem to force-multiply the intelligence shared across Australia.

Who are the current members?

Lead members span Critical Infrastructure sectors and are represented at our cross-sectoral Threat Intelligence Forums.

We are in the process of securing leads for the final three sectors (Defence, Finance, Space) and have multiple sectors with 3+ members. There are further members in the pipeline, who we expect to commence on-boarding over the coming weeks.

Additionally, we have signed two intelligence sharing MOU's with AHECS (shared intelligence from all 38 Australian universities) and AusCERT.

How many staff does CI-ISAC need?

We have over 20 volunteers from across Australia helping drive the build out of CI-ISAC and deliver operational services to the membership.

CI-ISAC has on-boarded its first local hire on the Sunshine Coast who is helping build out its member services function.

We have commenced our intern program, with the first QLD-based intern supporting the intelligence office and additional interns currently being considered.

The CI-ISAC will ramp up staff numbers as the membership increases and will work with the Sunshine Coast University and Sunshine TAFE to source additional support.

CI-ISAC is also working with the AWSN and Veterans Employment Program to identify and fill positions across its functional areas.

Why the Sunshine Coast?

The Sunshine Coast provides much needed infrastructure, the fastest east coast fibre connection to Asia and the USA, a NEXT DC data centre that has ACSC, NSA security clearance, a new city centre where every new building has fibre connectivity, a university seeking to address cyber security skill development and a local council committed to growing the tech sector.

How has Sunshine Coast Council supported your local investment?

Communicated the Sunshine Coast business case to directors to assist in the location decision making process.

Introductions to key local and state government partners i.e., LGAQ, TAFE etc.

Introductions to key industry bodies and commercial partners i.e., Silicon Coast, SCTechIA, NEXTDC, Walker Corporation.

Promotion of CI-ISAC job opportunities via "Sunshine Coast Jobs Hub".

Council is a foundational member for the local government industry group and have introduced colleague councils who will benefit.

What do members need to participate?

CI-ISAC's products and services have been designed to ensure that members can make better risk-informed decisions without being cyber experts. Our members range from small energy startups with one IT staff member to large multi-nationals with huge security teams.

Additionally, CI-ISAC focuses on quality over quantity, helping to filter through the swathes of open source information to build context on relevant threats and then delivering this intelligence to members to inform their risk management.

CI-ISAC extends your existing security capabilities to help guide your efforts by keeping members abreast of threats relevant to Australian Critical Infrastructure companies so that they can assess these against their own systems and proactively defend against cyber attackers.

Additional Resources

- **Overview of the CI-ISAC platforms** – https://ci-isac.org.au/media/videos/CI-ISAC+-+Threat+Sharing+Platform.mp4
- **Sample Threat Advisory** - https://www.linkedin.com/pulse/nokoyawa-ransomware-attacks-ci-isac
- **CI-ISAC launch video** - https://www.youtube.com/watch?v=yo3DClXKHng
- **Public Industry Reports** – for specific industry reports see "Sector Overview" link on https://www.ci-isac.org.au/members-sectors.html

A selection of founding Member Stories:

  - Dave O'Loan, **AARNET** - https://vocalvideo.com/v/ci-isac-australia-aarnet
  - Nikki Peever, **CAUDIT/AHECS** - https://vocalvideo.com/v/ci-isac-australia-client-reviews-nikki-peever-d1cln7kx
  - Peter Soulsby, **DXC Technology** - https://vocalvideo.com/v/ci-isac-australia-dxc-peter-soulsby
  - Mark Reynolds, **Sunshine Coast Council** - https://vocalvideo.com/v/ci-isac-australia-scc

- CI-ISAC CEO, David Sandell joins the **InnovationAus podcast** to talk about "Fighting critical infrastructure threats as a community" https://www.innovationaus.com/fighting-critical-infrastructure-threats-as-a-community/
- "**The Value of Sharing Cyber Threat Intelligence**" co-authored by Dr. Gary Waters and Kevin Vanhaelen, Strategic Advisors of CI-ISAC Australia https://www.linkedin.com/pulse/value-sharing-cyber-threat-intelligence-ci-isac
- "**The Power of Collective Defence**" speech excerpt taken from an AISA Sydney conference talk given by CI-ISAC CEO, David Sandell. https://youtu.be/qt025Rcyl_Y
- CI-ISAC establishes the **Academic Research, Development and Engagement Group** (ARDEG) with support from Associate Professor Atif Ahmad from the University of Melbourne (Chair) and Professor Andrew Bradley from the University of the Sunshine Coast (Deputy Chair) https://www.linkedin.com/pulse/introducing-ci-isacs-academic-research-development-engagement
- **Latest Prospectus** – https://www.ci-isac.org.au/pdf/CI-ISAC-Prospectus.pdf

CI-ISAC AUSTRALIA

CRITICAL INFRASTRUCTURE
Information Sharing and Analysis Centre

www.ci-isac.org.au

P: 1300 556 210

W: www.ci-isac.org.au

E: info@ci-isac.org.au

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

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