INFORMATION SHARING GUIDELINES

Central to CI-ISAC's mission is the requirement to enrich our members' cyber security operations with trusted collection, analysis and sharing of cyber threat intelligence (CTI) across the membership.

Preamble

These guidelines have been developed and optimised by CI-ISAC to incorporate existing experience, as well as an orient towards cross-sector sharing. CI-ISAC will work with members to evolve these sharing guidelines as the ecosystem expands with the objective of building true situational awareness across all CI sectors in Australia. Members are encouraged to submit feedback and suggestions for improvement directly to feedback@ci-isac.org.au.

Principles

CI-ISAC's mission is to a build robust, highly trusted cyber intelligence-sharing *community* and cyber capabilities for Australian Critical Infrastructure owners and operators within and across all sectors to ensure a collective, proactive cyber-defence posture. To achieve this mission, it guides all its actions through the four Principles of Frankness, Confidentiality, Cooperation and Non-competition. Members' strict application of information security policies is critical to uphold these Principles.

Member Guidance on Sharing Information into CI-ISAC

Information gathered, shared and analysed within the CI-ISAC ecosystem is guided by Key Member Questions (KMQs), detailed in the Operating Rules, which are enduring, strategic questions that provide the analytical framework around which all CI-ISAC subordinate Information Requirements (IRs) are shaped.

- While specific sharing requirements are guided by the KMQs and IRs, members are encouraged to share information on cyber threats from their own (or impacted 3rd parties) environments to enable CI-ISAC to (1) prioritise analysis activities and (2) build a holistic picture of the Australian threat-landscape to inform members' situational awareness.
- CI-ISAC facilitates a non-competitive, trusted environment focussed on the sharing of cyber threat intelligence and supporting members to uplift their defensive capabilities.
- Confidentiality and a strict data handling policy exists to protect shared information, with CI-ISAC ensuring that any member identifying information is redacted prior to analysis taking place. Trust in the CI-ISAC ecosystem is key to members sharing timely information on threats so this can be (1) analysed to support the reporting entity and (2) used to inform other members to proactively defend themselves.
- Members are encouraged to share information on the threats targeting/impacting their organisations – malware, phishing attacks and security incidents, which CI-ISAC will validate, enrich and build context before sharing with the broader community.
- At no point should member-sensitive elements of information (MSEIs) be shared into the CI-ISAC – Personally Identifiable Information, confidential company information, credit card numbers, leaked company data, etc.
- The key objective of information sharing in the ecosystem is to get relevant threat/incident information from one member, via the National Intelligence Office (NIO) to build context and send out to all members to improve their cyber risk management.

Member Sensitive Elements of Information (MSEIs)

The Operating Rules generally prohibit the sharing of MSEIs between members to ensure information security, as well as define exceptions when such information may be shared. Where shared under the Rules, all MSEIs must be categorised at TLP RED.

Information Processing: What to Share

When considering what information to share, members should understand the balance between the value of the information to the cyber security purpose established by the Operating Rules against the sensitivity of the information and possible damage to the sharing member's interests if disclosed to the wrong party.

The value of information can be assessed against its applicability to an element of the CI-ISAC ontology, which provides a simplified operating model to guide CTI analysis and development of the Information Requirements (IRs).

This balance is illustrated by the broad information sharing guidance in Table 1 below. Further guidance on what information should and should not be shared is contained in **Schedule 1**.

	Share	Don't Share
Strategic	• Broadly observed themes – e.g., increase in targeted phishing, malware targeting credentials.	• Strategic security investment plans. • Project / Investment choices on security uplifts/projects.
Operational	• Tactics, Techniques, Procedures (TTPs) relating to attacks/incidents. • Security Control controls bypassed (TLP: RED). • Attributed Threat Actors / Actors being tracked as a priority.	• Organisation / Client / Personally Identifiable Information. • Security Control details. • Legally sensitive information.
Technical / Tactical	• Technical indicators from incidents, including 3rd parties. • Technical indicators from blocked threats. • Technical indicators from active/emerging industry incidents (with permission).	• Internal IP addresses, system names, network information. • Open-source technical indicators. • Technical indicators from other peer organisations/members (without permission).

TABLE 1: Broad information sharing guidance.

Additional Supporting Information

The CI-ISAC ontology integrates the Diamond Threat Model with the kill chain steps derived from the MITRE ATT&CK model to build a unified operating model.

This model allows the derivation of a comprehensive set of Priority Intelligence Requirements (PIRs) and Member Information Reporting Needs (MIRNs), as a subset of the IRs, to help to answer KMQs. The CI-ISAC CTI ontology and its relationship with PIRs and MIRNs is diagrammatically summarised at Figure 1 below.

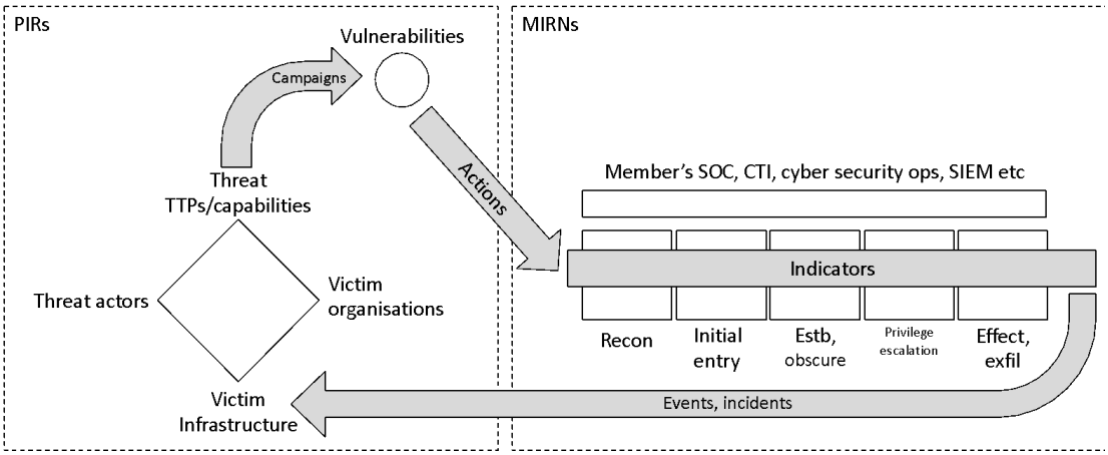

FIGURE 1: CI-ISAC CTI ontology

How CI-ISAC Helps Members Learn How to Share

CI-ISAC plays the role of a neutral/impartial third party that can bring the different cyber security lines of business in a member organisation together to talk through the internal processes needed to make sure that all stakeholders understand the benefits of sharing for their own organisation and the nation. Stakeholders might include CTI, SOC, Risk, Governance and Compliance, Audit, Legal and possibly managed security providers (vendors) depending on how a member structures their cyber security strategy and operations.

CI-ISAC will work with member organisations to facilitate the production of internal delegations of authority that ensure that members' employees determine the different types of cyber threat intelligence their organisation can share immediately and what needs escalation prior to being shared with CI-ISAC.

This means establishing a clear set of pre-approvals that allow defenders to have clear support from their organisation's management to share CTI in a timely manner. In cases where the CTI available to be shared has potential reputational, legal, or other risks attached, the agreed delegation should provide clear steps and timelines that escalated approvals for this sharing activity might need.

A Fundamental Benefit of CTI Sharing: Network Effects

CI-ISAC supplements the CTI Operations that our members (or their contracted vendors) already conduct to deliver the following benefits:

- Enriches members' understanding of the wider threat landscape through an ecosystem approach.
- Enhances members' own future security operations and CTI production activities through optimising their collection activities in their own environments.
- Building a holistic picture of relevant threats targeting members by combining submissions across sectors and applying structured intelligence analysis techniques.

CI-ISAC members become 'co-owners' of a trusted 'hub & spoke' intelligence network, which enables the generation of analytical network effects that broadens and deepens the understanding of Australia's critical infrastructure threat landscape. These network effects are the incremental intelligence benefits gained by an existing user for each new user that joins the network. It is a phenomenon whereby increased numbers of entities sharing intelligence improves the quality and value of intelligence overall for all members of the network (a synergistic effect). It also allows more threat intelligence content and services to be created and shared.

Schedule 1 - Information Requirements (IRs)

Priority Intelligence Requirements (PIRs)

ID	IR	Reporting TLP[1]
PIR 1	Who are the threat actors targeting Australian CI?	WHITE
PIR 2	What TTPs are threat actors targeting Australian CI employing?	WHITE
PIR 3	What vulnerabilities are threat actors targeting?	WHITE
PIR 4	What indicators are provided by those TTPs?	WHITE
PIR 5	What Australian CI victim infrastructure are threat actors targeting?	WHITE
PIR 6	What infrastructure components: endpoints, OSI layers (e.g. transport layer or application layer), OT, middleware layer/hypervisor, cloud, gateways, and boundaries, IDAM etc?	WHITE
PIR 7	Who are the target victims? Which sectors?	Ordinarily WHITE; GREEN if victim specifically named unless already in the public domain
PIR 8	What critical vulnerabilities have emerged that operators must apply mitigations against?	WHITE
PIR 9	What Australian CI supply chain partners and providers are being targeted?	WHITE
PIR 10	What TTPs are threat actors targeting supply chain partners employing?	WHITE

Member Information Reporting Needs (MIRNs)

ID	IR	Reporting TLP
MIRN 1	What reconnaissance TTP indicators have been detected?	GREEN
MIRN 2	What initial entry TTP indicators have you detected?	AMBER
MIRN 3	What establishment or lateral movement indicators have you detected in your systems?	AMBER
MIRN 4	What malware command and control indicators have you detected in your system?	RED
MIRN 5	What privilege escalation to directly command and control ICS have you detected in your systems?	RED
MIRN 6	What privilege escalation to access sensitive or privacy information have you detected in your systems?	RED
MIRN 7	In the event of a successful attack, what adversary behaviours or ransom demands have you observed?	RED (see also MSEI 7 below)
MIRN 8	What are your priority threats to monitor or hunt for?	GREEN
MIRN 9	What specific indicators are you hunting for?	AMBER

[1] Where member reporting may concern multiple IRs, the report is to be classified at the highest TLP of all of the IRs reported.

Member Sensitive Elements of Information (MSEIs)

ID	Element of information	Reporting strictly only on exception in accordance with Operating Rules (all reports at TLP RED)
MSEI 1	Detailed technical information (IP addresses, internal network credentials or privacy or [personal] sensitive information) potentially disclosing specific operational technology or IT environment vulnerabilities.	
MSEI 2	Identity of the reporting member if anonymity election is exercised.	
MSEI 3	Evidence of blatant neglect that could be potentially damaging to the reputation of the reporting member if made public.	
MSEI 4	Possible evidence of reporting members' breaches of Australian law.	
MSEI 5	Evidence of blatant neglect that could be potentially damaging to the reputation of the reporting member if made public (unless already in the public domain).	
MSEI 6	Any information or data potentially discoverable if litigation is *pending or reasonably foreseeable.*	
MSEI 7	Any consideration by a member to pay ransom or any quantum paid.	
MSEI 8	Evidence of a very probable or almost certain cyber security incident not yet reported to regulators that could identify a specific member.	
MSEI 9	The identity of supply chain partner whose systems are compromised (unless already in the public domain).	
MSEI 10	Any information subject to protections afforded by law e.g. 'protected' information under SOCI, AML&CTF, international agreements etc.	

Change Log

Version	Date	Author	Description
1.0	18th July 2023	HE	Initial version of sharing guidelines
1.1	9th August 2023	DS	Updated description (p1 + p2) of 'member environment' to include 3rd parties.
1.2	28th November 2025	DS	Updated link to data handling policy (from guidelines)