CI-ISAC Australia | Horizon 2 feedback

Australian 2023-2030 Cyber Security Strategy

Executive Summary

This submission advocates for a fundamental shift in Australia's national cyber strategy, moving from a reactive, compliance-driven posture to a proactive, threat-informed model of collective defence.

We propose the government acts as a strategic partner and enabler, rather than a direct provider of all services. The focus should be on fostering and scaling proven, industry-led, non-profit hubs to deliver sustainable capabilities and services. Our experience with the Health Cyber Sharing Network (HCSN) pilot demonstrates this model's success. It effectively translates raw threat data into timely, actionable intelligence for organisations of all maturity levels, solving the critical 'last mile' problem.

Introduction

We welcome the opportunity to submit a response to the cyber strategy consultation. This submission addresses the future of Australia's national cyber security posture, and our response is informed by two key pillars of our unique experience.

The first pillar is our role as Australia's leading not-for-profit hub for collaborative cyber defence, the Critical Infrastructure Information Sharing and Analysis Centre (CI-ISAC). As the successful recipient of a $6.4m grant from the Department of Home Affairs, we established the Health Cyber Sharing Network (HCSN) — an Australian-first partnership. The direct, evidence-based success of this pilot, which has already demonstrated a powerful model for uplifting resilience, forms the primary basis of this submission.

The second pillar is the two years of insight gained from developing our broader cross-sector member base, which gives us a unique perspective on the shared challenges facing Australia's critical infrastructure. Our diverse network now includes over 35 health organisations and 100+ organisations from other critical sectors, collectively serving over 12 million Australians.

Our success comes from delivering what members value most: Australian-specific intelligence in a trusted environment. We commend the government for its leadership and, in the responses that follow, point to key opportunities for enhancing impact across the pillars of the strategy.

2.1 Outlook for Horizon 2

1. What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

Government is right to be focussed on the evolution of technology. How Australian entities deploy and utilise technology to defend their networks and to generate cyber resilience, and how we respond to the application of the same technologies by threat actors should be a key concern. Two key technologies stand out.

AI will remain the pacing technology for now. Using AI as part of mainstream cyber defences will become standard for entities with good cyber maturity. The capabilities resident in this technology area will grow, as will the creative applications (for both defence and offence) of AI. But what about less mature entities that struggle to defend their networks today? How can these smaller entities integrate AI into their minimal cyber defence capabilities? How can they possibly keep pace with threat actors that will apply AI technologies in blunt and sophisticated ways? This may be an area where the Government can assist. To work with technology providers to develop/deliver 'budget AI solutions' for such organisations.

Guardrails for the responsible use of AI should be an accompanying consideration. When considering guardrails, it will be important to acknowledge that threat actors will deploy AI technologies without them. When considering guardrails, the Government must be careful not to unduly restrict entities who simply seek to employ AI technologies to defend their networks. Close consultation will be needed as guardrails are considered.

Beyond AI, quantum computing looms. How this nascent technology will impact cyber resilience remains to be seen and developments will need to be monitored closely. Undoubtedly threat actors will seek to utilise the technology to develop capacities to defeat or at least challenge the idea of ubiquitous and 'unbreakable' encryption.

Government should consider whether its cyber technology analysis, horizon scanning and research and development efforts are adequate to meet this growing technology challenge. Together, AI and quantum offer volume/mass and precision to cyber adversaries. Our cyber defences will need to scale and adapt to defeat this potent threat and Government intelligence; research and development will be necessary to support industry and enable effective cyber resilience.

Finally, it will be important to remember that in addition to computer systems, networks, and data, we need to consider the people that interact with these. An ethical and human-centred approach will be important. We should not isolate or distinguish "cyber" as a domain.

Note: Consider the work underway by the Social Cyber Institute (DFAT and India) - Creating resilient ecosystems for cyberspace, for peace and stability: https://www.socialcyber.co/aus-india-tia-publications-videos

2.2 Collaborating across all levels of Australian Government

2. Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?

From our perspective as a national initiative, the most critical program we advocate for is the development of dedicated, resourced, and integrated cyber security strategies for critical infrastructure sectors at the state and territory level.

We consider the strategic approach being pioneered in Western Australia to be the benchmark for best practice. While their formal Health Cyber Strategy is still in development (August 2025), the process of creating a dedicated, resourced strategy for the health sector that is designed to integrate with the state-level plan is the best-practice model we wish to see replicated. This same principle should be extended to other critical sectors—such as energy, water, and transport—to acknowledge the distinct differences in their operational technologies, risk profiles, and resourcing levels.

The benefits of this integrated, sector-specific approach are tangible:

1. **Strategic Clarity and Efficiency:** In jurisdictions with a dedicated strategy for a given sector, engagement and decision-making are significantly accelerated. There is a clear understanding of priorities, allowing organisations like the CI-ISAC to align our efforts and demonstrate how we contribute to existing objectives.

2. **Uplifting Foundational Capabilities:** A core challenge across Australia is the stark difference in cyber security resourcing and maturity between jurisdictions. For example, some jurisdictions currently lack the resources for fundamental tools like a Security Information and Event Management (SIEM) system, a gap that a formal strategy can address.

Interestingly, our experience has also shown that jurisdictions *without* a dedicated strategy can sometimes be quick to engage. In these cases, CI-ISAC is viewed as a "force multiplier" – an external catalyst to enable and advance a conversation that is otherwise progressing slowly. While this leads to positive engagement, it highlights a reactive posture rather than a proactive and sustainable one and can lead to inefficient cyber spending.

We advocate for strategy to be fundamentally threat-informed, this approach uses specific Cyber Threat Intelligence (CTI) about adversaries—their motives, tools, and methods—to

prioritise defensive actions. It allows an organisation to focus limited resources on likely and most damaging real-world attacks. This is the essence of maturing a cyber security program: moving from asking "Are we compliant?" to "Are we resilient against known threats targeting us?"

Recommendation:

We strongly advocate for a nationally consistent approach where resources are allocated to assist every state and territory in developing and implementing a suite of dedicated, sector-specific threat-informed cyber strategies.

Furthermore, a successful strategy must explicitly acknowledge and bridge the extensive differences **between and within** the public and private sectors. Government and industry operate with different drivers (public service vs. profit), constraints (procurement rules vs. market pressures), and risk appetites. A strong strategy provides the common language and shared objectives necessary to overcome these divides.

2.3 Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes

3. Does the high-level Model resonate and do you have any suggestions for its refinement?

The goals and interventions are not comprehensive enough and an evaluation model of the very broad outcomes sought is not sufficient. At the highest level, Australia needs a national cyber security framework that actually addresses the changing strategic environment as explained in the Paper.

A useful starting point would be the NIST framework that contains the Core Functions of Govern, Identify, Protect, Detect, Respond, and Recover. At a whole-of-nation level, this could be adapted to:

- **Govern** – Establish and monitor Australia's cyber-security strategy, expectations, and policy for managing risk, reducing vulnerabilities, being better prepared and improving resilience.

- **Identify** – Help determine the current cyber-security risk and vulnerabilities to Australia and the actions and responses for improving preparedness and resilience.

- **Protect** – Use safeguards to prevent or reduce cyber-security risk and vulnerabilities and improve preparedness and resilience.

- **Detect** – Find and analyse possible cyber-security attacks and compromises.
- **Respond** – Take action regarding a detected cyber-security incident.
- **Recover** – Restore assets and operations that were impacted by a cyber-security incident.
- **Learn** – Adapt and transform as a result of the cyber-security incident.

Assessing and prioritising cyber-security outcomes could be achieved within a framework such as NIST, and those outcomes could be more encompassing than those listed in the Paper. Furthermore, current and target states could be created for each selected core outcome and metrics could be identified to help prioritise and demonstrate progress from current to target states. These could be brought together into a template.

Such a notional template could have: selected framework outcomes (functions, categories, or sub-categories); current policies, processes, and procedures; current practices; target priority outcomes; target policies, processes, and procedures; target practices; target roles and responsibilities; target selected informative references; measurements; and artefacts and evidence.

Framework Tiers could also be used to assess maturity – such as:

- Tier 1: Partial.
- Tier 2: Informed.
- Tier 3: Repeatable.
- Tier 4: Adaptive.

Thus, the maturity of outcomes, policies, processes, procedures and practices could be assessed over this range that would reflect a progression from partial (informal, unstructured and reactive); through informed (established and documented), repeatable (systematically integrated and applied consistently) to adaptive (continuously improved through proactive learning, innovation, and transformation).

The Government needs to acknowledge that the volatility, uncertainty, complexity and ambiguity (VUCA) of today's environment makes disruptions inevitable. Managing risks and consequences, addressing vulnerabilities, being better prepared, and building stronger resilience all call for a new paradigm – one where cyber preparedness drives the pre-attack phase (using risk management through the "govern, identify, protect and detect", functions) and the post-attack phase (using consequence management through the "respond, recover and learn" functions).

Government could start with five basic principles:

- Set Clear Roles and Responsibilities.
- Develop, Implement and Evolve a Comprehensive Cyber Strategy.
- Embed Cyber Security in Existing Management Practices.
- Promote a Culture of Cyber Preparedness and Resilience.
- Plan for a Significant Cyber Security Incident.

In relation to the last principle, the government needs to ensure that preparedness and cyber resilience are built into the culture of organisations. This means:

- Anticipating and planning for cyber and sustained campaigns, based on an understanding of the threats and the potential non-cyber harms that could arise.

- Designing processes and establishing contingent capabilities to absorb and recover from incidents and extreme emergencies.

- Adopting information governance practices that can limit the impact arising from confidentiality breaches, data integrity compromises, and more devastating cyber attacks.

- Learning from incidents and adapting to strengthen the preparedness and resilience posture.

4. Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

Monitoring cybersecurity outcomes, whether for a nation or an organisation, really benefits from the NIST framework as a starting point for data and feedback. Any solid framework aims to dial down risk by improving how we manage cyber threats to our objectives.

Ideally, we need to measure our risk exposure, weighing up the costs versus benefits of reducing it. Clearer measurements – of risk, spend, and return on cyber efforts – lead to smarter strategies and investments. Regular self-assessment, or external reviews, should sharpen investment decisions. For instance, tracking cybersecurity maturity and trends helps convey meaningful risk information to all stakeholders, providing a firm basis for improvement.

Cybersecurity is an investment, so its effectiveness must align with overall organisational goals. Understanding the link between those goals, supporting cyber outcomes, and their practical management is crucial.

While no single framework measures everything, a NIST-aligned approach is effective way to begin by helping us:

- **Define Goals:** Shape desired security "states" based on cyber elements.
- **Gauge Current State:** Evaluate our existing cyber risk management.
- **Prioritise Outcomes:** Pinpoint key cybersecurity outcomes.
- **Track Progress:** Assess movement from current to future security states.
- **Verify Implementation:** Measure how thoroughly controls or guidance are applied.

Developing good cybersecurity metrics is evolving, so we must be thoughtful. The trick is optimising measurements without relying on 'bogus' indicators. Managing cyber risk demands discipline and regular review.

Crucially, we must know why measurements are used and how they contribute to overall cyber risk management, acknowledging their limitations. While 'lagging' measures verify objectives post-achievement, 'leading' measures can predict risks and impacts. Therefore, tailoring how measurements are incorporated into any framework, with full appreciation of their usefulness and limitations, is essential.

3. Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

5. What could government to do better target and consolidate its cyber awareness message?

Government should embed cyber awareness into the national curriculum, treating it as a core subject from a young age. This would establish it as a fundamental life skill for the modern world, just as crucial as reading, writing, and arithmetic. By doing so, understanding online risks would become second nature for the next generation, creating a more resilient society from the ground up. The work of the Cyber Coordinator, particularly in increasing public awareness is phenomenal but we question whether mainstream Australia is getting the message? There is some presence on free-to-air TV but more could be done. A hard-hitting TV campaign, akin to the late 80s AIDS prevention campaign, would help greatly.

6. What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?

The Health Cyber Sharing Network (HCSN) is a leading example of a successful, high-impact pilot funded by the Australian Government and delivered by CI-ISAC Australia. Over the past six

months, the HCSN has rapidly scaled to a diverse cohort of over 35 organisations, covering 12 million Australians, demonstrating a powerful new model for uplifting the cyber resilience of Australia's health sector.

The HCSN's success lies in its design as a capability-building engine that goes beyond awareness raising. It is an Australian-first innovation that provides a trusted, sector-specific, and nationally focused environment for collaboration and cyber threat intelligence sharing. By delivering timely, relevant, and actionable intelligence, the program empowers members to move from a reactive posture to a proactive and collective defence, directly strengthening the security of the entire health ecosystem.

The HCSN contributes greatly to cyber preparedness by providing organisations with rich-context advisories that allow them to act proactively during the pre-attack phase described above (using risk management through the “govern, identify, protect and detect”, functions); and the post-attack phase (using consequence management through the “respond, recover and learn” functions), through industry-specific and trend analysis to describe and explain what’s worked effectively.

National Reach and Market Coverage - The HCSN's 35+member cohort represents a comprehensive cross-section of the Australian health sector, covering a significant portion of the Australian population and demonstrating the model's applicability and value across the entire maturity spectrum.

Collectively, the HCSN has a direct and indirect service reach that conservatively covers well over **12 million Australians**, demonstrating the program's systemic importance and its capacity to protect a vast portion of the population by uplifting the security of their health providers.

Demonstrable Impact and Early Successes - The HCSN's success is evidenced by tangible impacts achieved within the first months of onboarding

- **Superior Intelligence Delivery:** The program provides intelligence that is demonstrably faster and more relevant than other sources and has sped up daily, weekly and quarterly organisational processes.

- **Immediate Strategic Influence:** The HCSN acts as a strategic catalyst that has sped up decision making in critical parts of the sector.

- **Quantifiable Return on Investment:** The program has already delivered clear financial value.

- **The Australian Advantage:** Members consistently praise the program's national focus. This local context is the program's key differentiator and the primary driver of its high-impact, actionable intelligence.

Scaling the ISAC concept across sectors: An opportunity exists for Government to scale up the HCSN Success to establish additional Cyber Sharing Networks across additional priority sectors such as Higher Education & Research, Transport and Logistics, Water and Manufacturing.

Forming part of the broader CI-ISAC ecosystem, further economies of scale are now possible with the foundations well laid as part of the HCSN. Stakeholders with technical cyber security expertise are able to both contribute observations to help build the national threat picture, or collaborate to build knowledge, capture lessons learnt, or work with the CI-ISAC team to inform cyber threat profiles on the priority threats facing Australian Critical Infrastructure. CI-ISAC acts as the 'glue' ensuring information is triaged, analysed and curated before being disseminated in an accessible form that can benefit all members, regardless of maturity.

7. How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?

The government has invested in commendable cyber resources like the Cyber Wardens programme, yet there's a puzzle: small businesses and charities simply aren't using them. Our experience building the Health Cyber Sharing Network, which includes many under-resourced non-profits, shows this isn't due to a lack of will. It's a classic "last-mile" problem.

These excellent resources are often designed with an assumption that the user has spare time, some technical expertise, and the headspace for strategy—three things the manager of a small care home or a local charity simply doesn't have. It's a fundamental misalignment with their operational reality.

To fix this, the government's strategy needs to shift from just providing resources to actively building capability; preferably in partnership with the NFP sector (as Government is doing with CI-ISAC as we build the HCSN)

The most effective way to do this is to fund and foster a network of specialised, non-profit hubs for key sectors like aged care, education, and social services. These industry-led hubs would act as the trusted local partners, translating generic government advice into practical, sector-specific steps.

Crucially, this funding should also subsidise hands-on help. Instead of just giving a small business a login, this would mean funding their access to practical workshops, expert advice, and strategic guidance that builds real skills. This is a direct investment in resilience, not just awareness.

We are not trying to reinvent the wheel. A key part of our role is already to act as a trusted guide, pointing our members to the best government programmes. By investing in these hubs, the government would be creating the "last mile" delivery network needed to ensure its own valuable resources actually reach and strengthen the organisations they are designed to protect. Government should aim to do this itself, and there are NFP entities who would gladly work with Government to deliver such services.

8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?

As noted above, the Government cannot and should not aim to do this work themselves. Partnering with industry and the NFP sector is key. Government should decide where it can best apply its unique skills and leave the rest to its partners. As programs like CTIS 1.0 demonstrated, Government needs to choose its partners carefully ensuring agility, capability, value for money and sovereignty is front of mind. While it is acknowledged that private, for-profit, entities possess significant and sometimes unique capabilities, reach and depth, and need to be involved in delivering the strategy's outcomes, they are not purpose-driven organisations. In contrast, NFPs are natural, sovereign, partners for Governments and they can be more involved in delivering the Cyber Strategy. Government might consider conducting a survey of available NFPs with capabilities to support the Cyber Strategy out to 2030.

9. What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?

A key challenge for SMBs and NFPs when it comes to cyber is any form of available resource (human or capital) to build security controls into an already stretched technical infrastructure. In terms of standards, a recently launched framework (OpenCase - https://opencase-framework.org) presents a pragmatic, risk-based approach that can be adopted by SMBs/NFPs. While the framework itself is new, the benefits of OpenCase are that it is 1) open source 2) pragmatic and 3) mirrors a 'levels-based' maturity approach that can be adopted over time as resources allow. OpenCase has been specifically designed for small/micro businesses and is not meant to represent a catch-all for medium/larger entities that may want to consider alternate frameworks such as SMB1001 (paid) or the Essential 8.

Regardless of choice, taking a structured approach to building risk-informed security controls is a mandatory first step to cyber security uplifts across the SMB/NFP sectors.

10. What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

While there are some NFPs with high levels of cyber maturity - such as CI-ISAC - Australian NFPs are often resource limited and typically possess low cyber maturity. Many NFPs will deploy minimum viable cyber defence capabilities that are managed by volunteers of mixed competence. Government should not underestimate how hard it is to grow a healthy NFP business. Unable to attract investment capital, NFPs only succeed on the back of motivated volunteers and dogged persistence driven by a strong sense of purpose. NFPs are also 'close to the ground' and are member focused. These attributes make the NFP sector a powerful partner for Government. We think the success of CI-ISAC makes this point. If Government wishes to more effectively harness NFPs consideration needs to be given to supporting the scaling of those NFPs with capabilities to support Strategy delivery.

Chosen not to respond:

11. Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?

12. How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?

13. How could the government further support businesses and individuals to protect themselves from ransomware attacks?

14. Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

15. How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? and

16. Which regulations do you consider most important in reducing overall cyber risk in Australia?

17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

3.2 Shield 2: Safe technology

Chosen not to respond:

18. What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?

19. How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?

20. What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

21. How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?

22. Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?

23. What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?

3.3 Shield 3: World-class threat sharing and blocking

24. What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?

For Australia to proactively address cyber threats, a shift from reactive incident management is imperative. The current approach of responding solely to breaches is unsustainable; it's akin to perpetually addressing symptoms rather than preventing the underlying issues. However, the solution does not lie in establishing additional committees or forums. The focus must be on instigating tangible, real-world action, rather than merely increasing discussion.

The government's most effective role is to act as a strategic partner and enabler, scaling up or supporting proven models that are already delivering results, creating the right conditions for industry to win. This means backing the specialists who can do the heavy lifting: turning a flood of raw data into sharp, practical instructions that enable immediate defensive action.

Most organisations are drowning in information but starved of insight. They don't need another report that gathers dust; they need timely advice that fits the fast cadence of their business and security teams.

With this foundation, industry can build a culture of active defence. It's about creating a trusted community where intelligence is put to work. It's about looking beyond your own backyard, because an attack on a bank is often a warning shot for a hospital. Seeing those cross-sector patterns is what allows us to get ahead.

This is where intelligence transitions from a theoretical concept into an indispensable tool. It enables a business to cease broad, unfocused expenditure on cybersecurity and instead concentrate its resources on the threats it is most likely to encounter. The warning changes from a vague alert that adds to the noise, to a clear, operational command: "This ransomware group is actively targeting Australian logistics firms using this unpatched software. Patch it now." This is intelligence that a busy security team can use immediately, without adding to their workload.

Ultimately, this is about turning intelligence into an operational asset. It's about embedding it into daily workflows, from vetting suppliers to hardening defences. By embracing this collaborative, action-oriented approach, we can build a more resilient nation, ready to anticipate and prevent threats, not just discuss them.

25. Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?

Yes, but as a collaborative partner. The government's role is not to dictate a rigid, one-size-fits-all technical posture, but to work with industry to define and champion a set of core principles and capabilities that constitute a proactive defence. The CI-ISAC HCSN pilot shows that a proactive posture is not a static checklist, but a dynamic capability built on:

- **Australian-focus:** A core finding from the HCSN pilot is that one of the most significant drivers of member value is the program's explicit focus on the Australian threat landscape, regulatory environment, and technology ecosystem. Members consistently and emphatically contrast the relevance of our intelligence with that of global commercial feeds and international ISACs, which are often described as too generic or overseas-focused to be consistently actionable.

- **State-government and public-private integration:** A proactive posture requires seamless collaboration between all levels of government and the private sector. The current system is often siloed. The HCSN pilot has demonstrated a successful model for integration, where a non-profit, industry-led hub can act as a trusted intermediary. It's notable that state governments of different maturities have engaged substantially

with us. For example, our engagement with a state health department was the direct impetus for a "whole-of-government" sharing conversation with the state's CISO, and the development of SIEM capabilities. Furthermore, we are effectively augmenting state-level capabilities, with Local Health Districts using our intelligence to patch niche medical systems not covered by their own state eHealth alerts.

- **Sector-specific technology advisories alongside cross-sector:** CI-ISAC has built out its coverage of operational technologies (OT) specific to the Australian health sector, including through reference to TGA approved technologies. This builds a sector specific knowledgebase alongside our cross-sector insights.

- **Intelligence-led Defence:** Moving beyond reactive patching to using timely, predictive intelligence to *anticipate* adversary tactics and *prioritise* defences. The network effect created by CI-ISAC has sped up response time and reliability of advisories.

- **Collective Defence:** No single organisation can defend itself alone. A proactive posture requires building trusted communities for bi-directional information sharing. The CI-ISAC has rapidly built this trust, evidenced by members proactively sharing technical indicators for malware back into the community and mature organisations requesting to lead on systematic challenges like third-party risk.

- **Supply Chain Resilience:** Extending security beyond the organisational boundary to the entire digital supply chain.

- **Adaptive and Inclusive Security for maturity levels:** Ensuring the national posture is effective for all, from the least-resourced to the most mature organisations.

The government's role is to establish this vision as a national strategic priority, while empowering industry-led bodies like ISACs to translate these principles into sector-specific, practical frameworks.

The core challenge with a top-down government mandate is the sheer diversity of our critical sectors. You have major banks with vast security budgets on one hand, and smaller but equally vital utility providers or local councils on the other, many of whom are stretched thin. This is why the government's role as a *facilitator* and collaborative partner is so crucial. Its focus should be on championing and supporting collaborative, industry-led platforms such as CI-ISAC that bring the best out of public and private. These platforms can provide scalable solutions and practical intelligence that are useful to everyone—from the corporate giant to the small supplier, government and industry. This approach helps to raise the standard for all, rather than creating a two-tier system.

26. How could government further support industry to block threats at scale?

Building on the principles of an intelligence-led defence, blocking threats at scale requires moving from fragmented, individual efforts to a coordinated, ecosystem-wide defence. The government can best support this by investing in the trusted, central hubs that enable this coordination.

- **The Problem:** Industry is currently trying to "drink from the firehose of information". Multiple, uncoordinated threat feeds from government and commercial sources create noise and overwhelm resource-constrained teams.

- **The Solution:** The government should formally endorse CI-ISAC as the primary mechanism for curating and disseminating high-confidence, actionable intelligence. The HCSN has proven this model's effectiveness, delivering intelligence that is **faster** than other channels and so relevant that **"nearly every advisory leads to action"**.

Lowering Barriers to Automation: To block threats at scale, intelligence must be machine-readable and automated. However, many organisations lack the resources to implement the necessary tools. Government can directly support this by co-funding the development of practical enablement resources,

Incentives for critical sectors to share with ISACs: the government should encourage our most insightful sectors—like telcos and banks—to share what they see. These industries are not only critical themselves; they are the bedrock for almost every other sector. When they contribute their intelligence to a collaborative community like CI-ISAC, our intelligence team analyses to spot wider attack patterns and methods. This collective insight, turned into practical warnings, allows everyone - from any CI sector - to get ahead of threats instead of just reacting. It effectively creates a national 'sensor network' that benefits us all.

While blocking threats is a vital part of any layered defence, we simply can't block everything. Clever attackers can disguise their activity to look like normal traffic, or bypass technical controls entirely by targeting people through social engineering.

Mature organisations can and should block known threats on their own networks. The challenge comes with trying to block on behalf of others at scale. The risk of a single false-positive is immense—if a legitimate customer website or a critical cloud service is mistakenly blacklisted, it can cause huge downstream disruption. This doesn't just lead to reputational damage; it could open the door to serious legal challenges for the entity that applied the block. That's precisely why we need a more holistic approach, moving beyond just blocking to embrace the kind of collaborative intelligence that strengthens everyone's defences.

27. How could the use of safe browsing and deceptive warning pages be amplified?

Rather than just relying on the global blacklists from Tech Giants like Google or Microsoft, the Government could help build a national "bad list" focused squarely on the threats hitting people here in Australia. The idea would be to pool together all the intelligence we already have. Government bodies like the ACSC, AFP, big-4 banks, and telcos could feed what they see into one central, trusted database. This would cover everything from those fake 'Australia Post' delivery texts to phishing sites pretending to be myGov or the ATO, creating a stream of threat data that is far faster and more relevant than anything a single company could gather alone. A trusted, central hub like CI-ISAC would be the natural partner to help curate and disseminate this national 'bad list', ensuring it is both timely and reliable..

Agentic AI, as employed by CBA could further improve risk scoring with tolerances being adjustable by end users to mitigate the risk of business disruption. Reference: https://www.commbank.com.au/articles/newsroom/2025/08/commbank-customer-scam-losses-fall-truyu.html

28. What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?

A thriving ecosystem is built on **trust, a clear value proposition, and the removal of barriers to participation.**

What is needed:

- **A Trusted, Neutral Hub:** A non-profit cross-sector ISAC is the ideal model. It provides a confidential "safe space" for sharing that a government body or a commercial entity cannot replicate. The rapid establishment of trust within the CI-ISAC HCSN is a testament to this. A proper national hub does two things that these small groups can't. First, it does the heavy lifting of turning a flood of raw data—like IP addresses and code vulnerabilities—into clear, practical intelligence. For many organisations it provides them with an intelligence capability that they do not otherwise have, and provides them with answers to the crucial questions of 'who, what, and why' so organisations aren't left drowning in alerts. Second, it caters to everyone, from the big banks with mature cyber teams to smaller organisations in sectors like healthcare, which are often playing catch-up and need more hands-on support. The pent-up demand for a more formalised approach to information sharing has been evidenced with the HCSN, showing that reluctance to share sensitive information is not inherent to industry but depends on the market model incentivised by the government. A trusted, not-for-profit national platform with clear rules and robust security can overcome legal or reputational barriers to entry.

- **A Clear ROI:** The ecosystem thrives when participation provides demonstrable value. The HCSN achieved this by providing unique **"Australian relevant intelligence"** that members were not getting elsewhere.

- **Government as a Partner:** A thriving ecosystem requires the government to be an active participant, not just an observer. This means sharing timely intelligence into the ISACs and, crucially, using the ISACs as a primary channel to receive anonymised, aggregated intelligence back from industry, which is then automatically shared with the ACSC's CTIS to help inform the national threat picture.

Other Sectors & Barriers to Creation:

- The success of the Health Cyber Sharing Network provides a clear blueprint for other sectors. It's a model that would work perfectly for any part of our critical infrastructure with a mix of large and small organisations and complex supply chains—sectors like Legal, Education, Water, and Manufacturing immediately come to mind.

- The main hurdle to creating these new hubs is the classic 'chicken-and-egg' problem. A sharing community needs a critical mass of members to be valuable, but you can't attract that critical mass without first having a clear value to offer. This is where government seed funding is essential. It's the role the government played so successfully with the HCSN—providing the initial push needed to overcome that start-up phase and build real momentum.

- However, the answer isn't to simply create a dozen separate, siloed groups. Our experience has shown that this approach would not only be financially unworkable in an economy the size of Australia's, but it would completely miss the point. The real value comes from sharing intelligence between sectors, not just locking it away within them. After all, a threat to the energy grid is also a threat to a hospital.

29. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

To make intelligence sharing truly effective for both cyber security and scams, we must move beyond just swapping data. For over two years, CI-ISAC has proven a model that successfully aligns and operationalises intelligence for members of all sizes.

Aligning Intelligence for the Australian Context
Our national intelligence team does the heavy lifting, analysing threats to provide clear warnings on the 'who, what, and why' that is specific to the Australian environment. This alignment is crucial. It demystifies the global threat landscape, making it directly relevant even for members

without a dedicated intelligence function. The result is intelligence so trusted that it is used for board presentations and integrated into operational workflows, with members describing it as "the highest quality" and "easier to digest" than other sources.

Operationalising Intelligence for All Maturity Levels
Crucially, for intelligence to be operationalised, it must solve problems, not create them. Too many security tools and raw data feeds simply add to the noise, generating thousands of alerts that overwhelm teams. Our solution is to provide curated, high-confidence intelligence that cuts through this noise. This is not just a convenience; for smaller or less mature organisations, it is the difference between effective defence and paralysis.

By delivering clear, contextualised recommendations, we provide these organisations with an intelligence capability they could not otherwise afford, empowering them to focus their limited resources on the threats that truly matter. This transforms cyber security from a source of constant stress into a manageable and proactive function for all, regardless of size or maturity.

30. Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

No, the roles and responsibilities are not sufficiently clear. While high-level plans exist, our engagement with the health sector reveals that for many frontline organisations, there is significant uncertainty about communication channels, operational expectations, and the division of responsibilities during a major national cyber crisis.

The government could further support industry by encouraging more practical, collaborative exercises, facilitated through trusted intermediaries.

- **Conduct Sector-Specific, ISAC-Facilitated Cyber Exercises:** The government should partner with ISACs to design and run regular cyber exercises tailored to the specific threats and operational realities of each critical infrastructure sector.

- **Executive Tabletop Exercises:** A key gap identified by our members is the need to engage leadership. One member specifically requested a "structured tabletop for their executive". An ISAC-facilitated exercise involving CISOs and their executive teams would be invaluable for clarifying roles and improving strategic decision-making under pressure.

- **Technical Supply Chain Scenarios:** Given that third-party risk is the number one concern across the health sector, a technical exercise simulating a major software

supply chain compromise would be a highly effective way to test and improve collective response plans.

- **Crisis Communication Drills:** An exercise focused solely on communication pathways between industry, the ISAC, and relevant government agencies (like the ACSC and the National Emergency Management Agency) would help clarify roles and ensure a more coordinated national response.

By leveraging the trusted relationships and sector-specific expertise of ISACs to facilitate these activities, the government can transform crisis preparedness from a document on a shelf into a practiced, resilient, and national capability.

31. How could government better incentivise businesses to adopt vulnerability disclosure policies?

The biggest barrier to businesses adopting vulnerability disclosure policies (VDPs) isn't technical; it's cultural. Right now, there's a genuine fear that reporting a flaw, even one found in good faith, will invite more trouble than it solves. Business leaders are asking themselves: "Will this trigger an audit? Will we be penalised under regulations like the SOCI Act?" Until the government addresses this fear directly, any other incentive will have limited effect.

The single most effective step would be to create genuine ‘safe harbour’ provisions. This would legally shield businesses from regulatory penalties when they act responsibly on vulnerabilities reported through a VDP. Trust is paramount here, and it can be massively amplified by encouraging the use of neutral, industry-led intermediaries—bodies that can act as a trusted buffer between a business and the regulator. A company is far more likely to report a flaw to an industry body, knowing it won’t automatically trigger a formal incident report and the associated regulatory headache.

Once that fear is removed, the government can make adopting a VDP an obvious business advantage. This means offering practical financial support—like R&D-style tax credits for implementation costs or working with insurers to secure lower premiums for companies with a proven VDP. Alongside this, publicly championing businesses that get it right would create a powerful reputational incentive, turning a security measure into a badge of trustworthiness.

Ultimately, this is about changing the dynamic from a compliance exercise to a collaborative partnership. It’s about moving away from a culture where vulnerabilities are hidden for fear of punishment, towards one where they are openly reported because it's safe, sensible, and recognised as a mark of a mature and responsible organisation.

32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

Yes, and urgently. At present, Australia puts security researchers who find critical flaws in a difficult position. If they report a vulnerability to a business, they risk being met not with thanks, but with potential threats of legal action. This isn't a theoretical problem; it's a real effect that discourages the people who can help identify gaps in our defences.

This legal uncertainty forces researchers into a dangerous choice: stay silent and let the vulnerability persist, report it and risk prosecution, or turn to the black market where a zero-day vulnerability can fetch a significant price. By failing to provide a safe, legal channel for disclosure, we are inadvertently pushing talent towards the shadows, and leaving our critical infrastructure exposed.

A national, government-backed Vulnerability Disclosure Program would solve this by providing one simple thing: a clear, legally safe harbour. It would tell researchers that if they act in good faith, they won't be treated like criminals. For businesses, especially those covered by the SOCI Act, it would provide a structured way to find and fix risks before they become a full-blown incident with all the regulatory repercussions that entails.

Without this approach, Australia is falling behind our international partners. The US, UK, and the EU have already established clear frameworks to protect security researchers. This isn't just about aligning with global standards; it's about fundamentally shifting our national cyber security culture from one of legal fear to one of smart, effective collaboration.

3.4 Shield 4: Protected critical infrastructure

Chosen not to respond:

33. How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

34. Are there significant cyber security risks that are not adequately addressed under the current framework?

35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

37. How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

3.5 Shield 5: Sovereign capabilities

Chosen not to respond:

39. What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow

40. What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

41. What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?

42. How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?

43. How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?

44. How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?

45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

3.6 Shield 6: Strong region and global leadership

46. Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

Yes, public attributions, advisories, and sanctions are powerful and essential tools, but they are largely reactive. To truly get on the front foot and deter growing malicious activity, Australia must develop a more proactive stance, grounded in a clear and legally sound doctrine of 'Active Defence'.

It's crucial to be clear: this isn't simply about 'hacking back'. Instead, Active Defence covers a spectrum of proactive measures. This includes authorised operations to gather intelligence on threat actors and their methods before they strike, as well as using a broader

range of policy tools to actively shape their behaviour and disrupt their operations. It's about moving beyond our own networks to understand and influence the adversary.

Developing such a capability must be firmly grounded in international law, building on established principles like those outlined in the Tallinn Manual. By formally adopting and developing a doctrine for Active Defence, Australia can shift from simply responding to incidents to actively raising the cost for our adversaries, creating a far more effective deterrent and a more resilient national posture.

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

Yes, this can be achieved through international conventions (treaties) which, as a source of national (domestic) law, lead to countries ratifying conventions adopting the same rules and norms

Chosen not to respond:

48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?

49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

50. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?

---

v1.0 | 27.08.2025