CISO LENS

Submission: Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

August 2025

PUBLIC

Table of Contents

About CISO Lens

CISO Lens is the premier cyber security information sharing service for cyber security executives from the largest organisations in Australia and New Zealand.

Our members represent very large and complex organisations, including ASX/NZX listed companies, critical infrastructure and essential services providers, and large government departments. These organisations have the largest numbers of staff, the most complex environments, and support millions of customers and citizens.

Our mission is to support improved cyber resilience for Australia and New Zealand. We do this by providing a trusted, vendor-independent space for cyber security executives to collaborate, share information and insights, and support one another to lead better cyber security programs.

CISO Lens' member organisations represent:

- about 54 per cent of the total market cap value of the ASX All Ordinaries index
- employ more than 1.5 million people, mostly based in Australia
- operated with a combined annual security budget of more than $2.7 billion in FY24
- collectively account for between 35-40 per cent of security spend in the Australia / New Zealand region.

We work closely with our member organisations to understand and address the shared challenges they face, and advocate for government and industry reform to improve national cyber risk management efforts.

Executive Summary

CISO Lens welcomes the opportunity to contribute to the design of Horizon 2 of the *2023-2030 Australian Cyber Security Strategy*. As Australia's premier strategic information sharing and analysis community for cyber security executives from the nation's largest and most complex organisations, we are proud to represent the interests of our members to inform this important strategy.

Over the next three years, Australia's cyber risk environment will be shaped by escalating geopolitical tension, continued rapid adoption of cloud and artificial intelligence (AI), and persistent supply chain vulnerabilities. Our members highlight advanced persistent threats (APTs), cybercrime groups, and cloud security risks as pressing concerns, while traditional issues of phishing and social engineering remain common attack vectors. Despite important progress delivered to date under Horizon 1, our members are concerned that Australia remains largely unprepared to deal with these challenges and call for greater focus on national preparedness.

The strategy's six cyber shields provide a strong foundation, with Shields 1 (Strong businesses and citizens), 3 (World-class threat sharing and blocking), and 4 (Protected critical infrastructure) viewed as most beneficial. However, limited transparency on progress and tangible impact remains a concern. An annual public reporting cycle, coupled with the proposed Cyber Security Policy Evaluation Model, will build industry confidence regarding progress and investments.

We support the proposed direction and priorities for Horizon 2 and offer recommendations to help inform the design of specific initiatives. Horizon 2 must deliver coordinated, measurable outcomes that strengthen preparedness, simplify regulation, and address systemic cyber risks.

On behalf of the CISO Lens community, we thank the Department of Home Affairs for its commitment to early and open engagement on the strategic issues shaping Australia's cyber security. Like many cyber security professionals across Australia, we maintain a keen interest in supporting the continued strengthening of Australia's cyber security posture.

Questions regarding this submission can be directed to [redacted]

Capturing industry feedback

This submission is informed through consultation with security executives and security operations leads across the CISO Lens community.

We spoke to our members about the proposed strategic direction and priorities for Horizon 2 of the *2023-2030 Australian Cyber Security Strategy*, and the various questions posed in the discussion paper.

We focused our consultation on themes and topics which are directly relevant to large and complex organisations operating in Australia, and which are of most interest to our members. We did not consider all 50 questions posed in the discussion paper.

As CISO Lens does not publicly identify its members or their organisations, all feedback has been anonymised for the purpose of inclusion in this submission.

Feedback

The following section provides responses to several questions posed in the discussion paper. Our response is focused on questions that are most relevant to CISO Lens' members and their role in supporting security outcomes at large and complex Australian organisations.

Developing the vision for Horizon 2

1. Developments that will shape cyber security risk in Australia over the next 1-3 years

Our members hold the view that, over the next three years, the cyber risk landscape in Australia will be shaped by a convergence of geopolitical tension, rapid technology adoption (including cloud and Artificial Intelligence), supply chain vulnerabilities, and the growing threat posed by increasingly capable APTs and cybercrime groups.

In May 2025, we surveyed cyber security executives and operational security leaders across our community, seeking their views on the major cyber threats facing Australia and their individual organisations over the next 1-3 years. We also captured sentiment regarding national and organisational preparedness to effectively manage these threats.

The survey found that, at the national level, security executives and operational leaders are primarily concerned about supply chain vulnerabilities, cyber-attacks involving APTs, and the potential for a nationally significant cyber-attack. Within their own organisations, threats were viewed through a more localised lens, with top concerns rated as phishing and social engineering attacks, and cloud security risks.

Worryingly, the survey also found that despite most respondents observing some improvements to national preparedness in the last 1-3 years, 94 per cent felt that Australia was still only '*somewhat prepared*' (or worse) to manage major cyber threats.

Our members observed that although Horizon 1 of the *2023-2030 Australian Cyber Security Strategy* features actions that contribute to national preparedness, such as improved intelligence sharing and the development of sector/threat-based playbooks, Australia lacks a holistic approach to addressing this need (with the current approach described as 'piecemeal' in nature). **Our members want to partner with government to map the capabilities and capacity needed to manage current and future cyber threats, to ensure Australia has a curated plan for improving its national cyber preparedness. This should be a core focus of Horizon 2.**

2. Monitoring progress in a changing world – a conceptual framework

The *2023-2030 Australian Cyber Security Strategy* was released in 2023 with the bold and sensible vision of making Australia a world-leader in cyber security by 2030.

Backed with an investment of $586.9 million to 2030, the strategy seeks to build our national cyber capability and resilience through its focus on six 'shields', which are:

- Shield 1 – Strong businesses and citizens
- Shield 2 – Safe technology
- Shield 3 – World-class threat sharing and blocking
- Shield 4 – Protected critical infrastructure
- Shield 5 – Sovereign capabilities
- Shield 6 – Resilient region and global leadership.

In May 2025, we surveyed our members to understand the level of benefit they see arising from the strategy and each of the six shields. We asked our members to consider whether the strategy is supporting improved cyber security within their organisations, and to nominate the strategy shields they consider most beneficial.

Promisingly, 93 per cent of respondents indicated the strategy was delivering some level of benefit for their organisation. The responses show that Shield 1 (strong businesses and citizens) and Shield 3 (world-class threat sharing and blocking) are considered most beneficial by respondents. These shields are making it easier for Australian businesses to access help after a cyber incident occurs, while improving national threat intelligence sharing and blocking capabilities, among many other initiatives.

Shield 4 (protected critical infrastructure) is popular among both critical infrastructure and non-critical infrastructure organisations. This shield seeks to clarify and strengthen cyber security obligations for critical infrastructure owners and operators, while also improving the ability of these organisations to respond to cyber incidents. It is a promising sign that one-third of respondents who found this shield highly beneficial are not designated critical infrastructure organisations, likely an indication these organisations recognise the benefits of improved critical infrastructure in their broader supply chains.

Despite these positive results, respondents also observed there is currently limited understanding of the progress to implement Horizon 1 action items. Respondents also noted that many of the initiatives featured under Horizon 1 of the 2023-2030 Australian Cyber Security Strategy are yet to deliver an observable impact.

The release of Appendix B to the discussion paper, providing a detailed view of the progress to implement Horizon 1 initiatives, is a welcome development. We recommend the Department of Home Affairs now adopt an annual reporting cycle through to 2030, providing public visibility of the progress to implement strategy initiatives and articulation of the benefits this work has delivered.

Moreover, the development of the Cyber Security Policy Evaluation Model is strongly supported. We support the department's intention of developing a robust methodology that guides cyber security investments and action across the nation. We believe a 'system level' view of cyber security risk management is critical to ensuring our various actions and initiatives work in complementary ways to improve Australia's national cyber security posture.

Shield 1 – Strong businesses and citizens

3. Better targeting and consolidating cyber awareness messaging

The discussion paper proposes to better target and consolidate cyber awareness messaging across the economy, to promote improved online safety behaviours and reduce the harm from cybercrime. This concept generated considerable discussion amongst our members, who provided feedback on current initiatives and offered suggestions to inform direction under Horizon 2.

We note the Australian Government leads a variety of public campaigns regarding scam awareness, privacy and data protection, and cyber security. Each campaign has a lead federal government department or agency, and is typically amplified by other arms of government (local, state and federal) and the private sector.

Key campaigns include:

- *Privacy Awareness Week* (June), led by the Office of the Australian Information Commissioner (OAIC)
- *Scam Awareness Week* (August), led by the Australian Competition and Consumer Commission (ACCC)
- *Cyber Security Awareness Month* (October), led by the National Office of Cyber Security
- *'Act Now. Stay Secure'* campaign, led by the Department of Home Affairs / National Office of Cyber Security.

Discussion with our members reveals considerable support for the *'Act Now. Stay Secure'* campaign. This campaign is viewed positively for its messaging about online safety, cybercrime risks and response strategies. Similar sentiment exists for *Scam Awareness Week*, which is seen as

complementary to reducing online safety and cybercrime risks. Conversely, it was noted that the 2025 *Privacy Awareness Week* campaign was lacking a clear 'call to action' that members could amplify throughout their organisations and wider customer groups.

Cyber Security Awareness Month generated considerable discussion among our members. There was strong suggestion that its focus should now shift from 'awareness' to 'action'—consistent with the broader Horizon 2 approach of embedding good cyber security practice across the economy.

Members feel the '*Act Now. Stay Secure'* campaign is doing a good job of raising awareness of key cyber risks across the economy and, rather than duplicate this messaging during *Cyber Security Awareness Month*, the latter campaign should instead drive uplift of priority actions across key sectors and/or demographics. To that end, **we support government's efforts to better target and consolidate cyber awareness messaging across the economy, to ensure these campaigns drive actual change in online safety and cyber security behaviours.**

Of note, several members representing large public facing organisations reported that while they were eager to amplify and support the above-mentioned campaigns, in many cases their requests for early access to campaign materials had previously gone unanswered (or had been refused by lead departments/agencies). This had the effect of delaying necessary work by their media and communications teams to align key messages and materials.

If government wants industry to amplify and promote its scam awareness, privacy and data protection, and cyber security campaigns, **we recommend that campaign leads do more to share campaign strategies and resources with large public-facing organisations prior to public launch, to support an aligned public-private approach**.

4. Improving cyber security, privacy and data protection regulation

We strongly support the department's efforts to harmonise and simplify cyber regulation to promote best practice and efficiency. This should remain a key focus of the strategy.

The call for harmonisation of existing laws, standards and frameworks is a regular topic of conversation amongst the CISO Lens community. Private sector organisations, particularly those operating in designated critical infrastructure sectors, are required to comply with a multitude of cyber security, data protection, privacy and risk management frameworks overseen by different regulatory bodies.

For example, a financial services organisation will experience interest in various aspects of its cyber security program from the Department of Home Affairs, the Australian Prudential

Regulation Authority, the Australian Securities and Investments Commission, the Office of the Australian Information Commissioner, and potentially also the Reserve Bank of Australia.

Although cyber regulation is typically seen as beneficial to improving organisational security posture, the variety of regulators involved and the myriad reporting obligations they impose place a significant burden on organisations. Data collected for our 2024 Member Benchmark found that organisations were investing about 12 per cent of their security team headcount responding to external audits and reviews, including reporting to regulators. This is time drawn away from protecting their organisation, its data, systems, and customers. Compounding the challenge for industry is that audits are often seen as uncoordinated and overlapping in scope.

Although we acknowledge that cyber risk management is an area where many government agencies share and complement one another's powers to support improved resilience, **there is a strong desire to see government untangle and simplify regulatory oversight of information security, cyber security and data protection in the private sector.**

Our members welcome further engagement with government to explore options for consolidating the existing arrangements into a streamlined regulatory framework, providing holistic regulation of information security, cyber security and data protection at private sector organisations.

Shield 2 – Safe technology

5. Managing foreign ownership, control or influence risks

The discussion paper asks: '*What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?*' We note the Department of Home Affairs has recently published guidance to help organisations better identify, assess and manage these risks.[1]

Feedback from our Australian Prudential Regulation Authority (APRA) regulated members indicates *CPS 230: Operational Risk Management* has been beneficial in assisting them to identify, assess and manage foreign ownership, control and influence risks relating to technology.

With the backdrop of a rapidly evolving geopolitical environment, and a large reliance on foreign technology by Australian organisations, **we encourage government to explore options for**

[1] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/foreign-ownership-control-or-influence-risk-assessment-guidance

applying similar obligations to other regulated sectors, to support them in better managing foreign ownership, control or influence risks associated with technology vendors.

This should be considered in the context of broader efforts to harmonise and simplify cyber regulation to promote best practice and efficiency.

Shield 3 – World-class threat sharing and blocking

6. Australia's proactive cyber security posture

The discussion paper asks whether '*government should scope and define what Australia's proactive cyber security posture should look like for industry?*' It also asks '*what government could do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem?*'

We support the shift toward a proactive cyber security posture for Australia and consider it essential that government and industry approach this task together (rather than government scoping and defining this item for industry to adopt). Government's strength is its convening power to facilitate national collaboration; while industry has a first-hand appreciation of the cyber risks experienced by private organisations, and strategies for managing those risks.

Discussion with our members identifies several potential attributes of a proactive cyber security posture. These are explained below.

Greater use of intelligence-informed 'indicators and warnings'

'Indicators and warnings' is about spotting the early signs of trouble and acting before it lands. Indicators are the observable shifts, like unusual system activity or changes in adversary behaviour, that hint at intent or capability. Warnings turn those signals into timely assessments for decision-makers, giving them the chance to prepare, deter, or respond. The value lies in moving from a reactive stance to a proactive one, focusing attention and resources on the threats that matter most and reducing the risk of being caught by surprise.

We recommend the development of cyber security indicators and warnings for Australia, to sit at both the national and sectoral levels—giving insight into risk changes that affect the nation, and likewise individual sectors and industry groups. Having an agreed set of indicators and warnings can assist with proactively adjusting national and sector-level controls to better manage threats before they can cause harm.

From resilience to preparedness

Much of the discourse about our national cyber posture focuses on resilience. That is, supporting government, business and the community to 'bounce back' after an incident occurs. This has generated considerable focus on improving our ability across the nation and as organisations to respond to, and recover from, malicious cyber activity to minimise harm to the community. This is a valid and reasonable approach to take, and one that recognises the reality of Australia's current cyber risk environment (i.e., where a new incident is reported every six minutes).

A proactive cyber security posture for Australia should emphasise preparedness—being the capability and capacity of an entity to effectively anticipate, plan for, respond to, and recover from threats, to minimise the adverse impacts they have. It builds on the resilience concept by placing greater focus on the actions an entity can take to anticipate and mitigate potential incidents, while retaining the essential response and recovery elements.

The preparedness concept is widely adopted in the emergency and risk management domains, to assist governments and other organisations in ensuring they have the knowledge, tools and resources needed to combat major threats.

For Horizon 2, **we recommend that government partner with the private sector to develop a plan for improving Australia's national cyber security preparedness**, to ensure Australia has the capability and capacity needed to effectively manage current and future cyber threats (i.e., a dedicated hazard preparedness plan).

Start with a focus on the threats of greatest concern to security executives

In May 2025, we surveyed our members to understand the major cyber threats facing Australia over the next 1-3 years, and their views on our national preparedness to effectively manage those threats. The survey found that respondents were principally concerned about supply chain vulnerabilities, cyber-attacks involving APTs, and the potential for a nationally significant cyber-attack. Worryingly, 94 per cent of respondents felt that Australia was only 'somewhat prepared' (or worse) to manage these threats. **We recommend these themes be prioritised when developing the attributes of a proactive cyber security posture, and when testing and validating the approach with industry.**

7. Roles and responsibilities of government and industry during a crisis / conflict

The discussion paper asks whether '*the roles and responsibilities of government and industry are clear for cyber security in a conflict or crisis scenario?*' It also asks '*what activities, such as cyber exercises, could Government* undertake to make you feel better prepared to respond in a cyber conflict or crisis?'

We have examined this issue extensively through our work on Project Robust. This project was established to unite government and industry to identify and pursue opportunities to strengthen Australia's national cyber incident management arrangements.

Most of our members believe there is a high likelihood of a nationally significant cyber-attack impacting Australia in the next 1-3 years, with many also lacking confidence in Australia's preparedness to respond effectively to it. In fact, most would rate our current national response ability as either *basic*, *poor* or *very poor*.

A key concern for our members is that **Australia's current national cyber incident management arrangements, in particular the Australian Cyber Response Plan (AUSCYBERPLAN), are government-centric and do not adequately articulate the role and responsibilities of private sector organisations in the management of cyber crises**. Moreover, these arrangements lack critical detail about how the plans will work in practice, leaving the private sector unclear about key governance and coordination arrangements.

This is significant because the private sector will play a critical role in any national-level response to cyber crises. As owners and operators of a significant portion of Australia's critical infrastructure, essential services and data assets, and first-line responders to incidents involving the IT networks underpinning these services, the role of the private sector cannot be understated.

To address this concern, and in response to the questions posed in the discussion paper, we recommend that government:

- **Prioritise engagement with the private sector to further define roles and responsibilities under Australia's national cyber incident management arrangements**, including clarifying how key governance and coordination mechanisms will operate.
- **Partner with the private sector to develop a plan for improving Australia's national cyber security preparedness**, to ensure Australia has the capability and capacity needed to effectively manage current and future cyber threats (i.e., a dedicated hazard preparedness plan).

Shield 4 – Protected critical infrastructure

8. The Security of Critical Infrastructure Act

The discussion paper poses several questions regarding industry experience with the operation and effectiveness of the Security of Critical Infrastructure Act 2018 (SOCI Act).

Feedback from our members regarding the SOCI Act is mostly positive, with members understanding their obligations and the role of the Department of Home Affairs as the regulator. The requirements of the SOCI Act are generally considered beneficial to improving the security posture of regulated organisations. Moreover, the regulatory burden is considered proportionate to the risk and outcomes being sought, and the department's emphasis on education before enforcement is appreciated.

Among our members, there has been discussion about whether **SOCI Act obligations should be extended to essential services sectors that form part of the broader national supply chain**. Examples include the government sector (specifically law enforcement, public safety and emergency services), critical manufacturing and storage, waste management and recycling. These essential services sectors, and others like them, form a critical component of the national supply chain and can also benefit from security uplift driven through the SOCI Act.

We recommend government explore options for extending SOCI Act requirements to high-criticality essential services sectors not currently captured under the regulations.

Shield 5 – Sovereign capabilities

9. ICT Concentration Risk

The concentration risks raised by our members focus on hyperscalers like Google, Microsoft M365/Azure and Amazon AWS. As organisations consolidate more services into these providers, the risks compound. The CrowdStrike outage in 2024 showed how a single disruption can cascade globally. The sheer volume of data concentrated in a few providers also makes them prime targets for APTs and other adversaries.

Resilience is another concern. If a hyperscaler suffers a major incident, their ability to support all customers is inevitably constrained. Transparency is also limited—particularly around operations in higher-risk jurisdictions and how infrastructure is segregated across regions. This lack of clarity makes it harder for organisations to assess how their risk profiles shift as they move deeper into the cloud.

We do not expect consumers to move away from hyperscalers to reduce concentration risk. Instead, mature organisations are pursuing redundancy through multi-region or logically isolated environments, while strengthening business continuity and disaster recovery arrangements to maintain critical functions during outages.

Members report that attempts to secure meaningful assurance from hyperscalers are largely futile. Responses are typically templated, offering high-level assurances with little visibility of how they are validated. **For Horizon 2, we see a role for government to apply greater national pressure on large vendors to provide deeper, more credible assurance of their security posture and how they manage concentration risks.**

Final Remarks

We thank the Department of Home Affairs for its commitment to early and open engagement on the strategic issues shaping Australia's cyber security.

Our members have a keen interest in shaping the future direction and priorities of the *2023-2030 Australian Cyber Security Strategy*, and the initiatives that underpin its delivery.

Through continued public-private partnership and clear focus on delivering high-value, high-impact initiatives, we can realise the vision of being a world-leader in cyber security by 2030.