Submission on Horizon 2 of the 2023–2030

McGrathNicol Advisory | Technology and Cyber

28 August 2025

1 Introduction

1.1 McGrathNicol welcomes the opportunity to contribute to the development of Horizon 2 of the 2023 – 2030 Australian Cyber Security Strategy.
Our firm has worked at the front line of some of the most significant cyber incidents in Australia, often in high-pressure environments where the ability to contain, remediate, and recover is measured in hours, not days. We have advised boards, executive teams, and operational staff through the lifecycle of cyber events, from pre-incident maturity building to post-incident reviews and regulatory engagement.

1.2 This perspective gives us a clear view of where policy and reality diverge, and what is required for the next stage of the Strategy to succeed. Horizon 2's goal of scaling cyber maturity across the whole economy will only be achieved if the outcomes are practical, measurable, and accessible to all stakeholders, from large, listed companies to small regional operators.

2 Shield 1 – Strong Businesses and Citizens

2.1 For many organisations, particularly SMBs, NFPs, and local government, cyber resilience is not hindered by a lack of awareness, it is hindered by a lack of execution capability. Most know they should patch systems, implement MFA, and maintain backups, but the skills, resources, or time to do this effectively are missing.

2.2 Horizon 2 should therefore ensure that funding and support go beyond campaigns and guidance documents. The national approach needs a baseline cyber maturity framework that is scaled for SMBs, aligned with appropriate frameworks such as SMB1001, NIST CSF 2.0, and the ACSC Essential 8. This framework should be practical, staged, and affordable, allowing SMBs to progress incrementally while maintaining business operations. Organisations meeting defined benchmarks could be recognised through a certification or rating system that builds trust with customers and partners.

2.3 Practical support is essential. Government should introduce co-funded uplift programs or voucher schemes to reduce the financial barrier for SMBs to deploy core security measures such as MFA, EDR, and secure email gateways. In addition, sector-based shared security services, for example in health, aged care, or local government, could provide pooled monitoring, incident readiness, and training, reducing duplication and cost.

2.4 SMBs also need confidence that, in the event of an incident, they can rapidly access qualified support. Horizon 2 should provide access to a national panel of accredited responders, pre-approved and pre-contracted, available to SMBs at a subsidised rate. This would ensure incidents are contained quickly and lessons are shared nationally. Cyber insurers could also play a role, contributing anonymised incident data through a safe-harbour reporting channel that encourages disclosure without penalising the business.

2.5 At the governance level, directors and owner-managers of SMBs should be supported to build confidence in cyber decision-making. Tailored training programs such as "Cyber Essentials for SMB Directors" would help normalise cyber as a business issue, not just a technical one.

2.6 Building on the Australian Government's current efforts, such as embedding a Zero Trust culture across the public sector by 2030, releasing guiding principles for agencies, and mandating Zero Trust adoption through the 2025 Protective Security Policy Framework, Horizon 2 should extend these initiatives into the private sector. At present, support is heavily focused on government entities; the gap lies in helping critical infrastructure operators, SMEs, and other businesses apply Zero Trust principles in a practical and affordable way. Funding, tools and industry-specific playbooks will be key to bridging this divide.

2.7 In addition, Horizon 2 should acknowledge quantum-resistant security as an emerging priority: while quantum threats are not yet a present danger, policy and investment should ensure organisations begin preparing for post-quantum cryptography and related safeguards as part of their long-term cyber resilience roadmap.

2.8 Finally, incident readiness should be normalised across sectors. This includes mandatory, regular testing of incident response plans through tabletop exercises and simulations, not just in critical infrastructure, but across sectors where digital disruption can cause material harm.

3 Shield 2 – Safe Technology

3.1 Secure-by-design principles need to become the default for products and services operating in Australia. Vendors supplying core business applications, particularly those used in critical infrastructure and essential services, should be required to demonstrate compliance with secure development standards validated through independent testing.

3.2 In procurement processes, especially in government and regulated sectors, there should be a mandatory "cyber fitness declaration" from technology suppliers and managed service providers. This would cover areas such as patching cadence, vulnerability disclosure policies, and security testing history.

3.3 Recent incidents, such as the Qantas event, have highlighted the risks created by an increasing reliance on third-party and SaaS providers. When these suppliers are compromised, the consequences can cascade through the relying organisation, sometimes with greater impact than a direct breach. Horizon 2 should therefore consider regulatory settings that hold third-party providers to the same security and resilience standards as the organisations that depend on them. This would not only create consistency across the digital supply chain but also incentivise providers to embed secure-by-design practices more rigorously.

3.4 Technology change also needs to address architectural issues. Zero trust models, modern endpoint detection and response (EDR), and managed detection and response (MDR) capabilities should be promoted through incentives, particularly for sectors operating on tight margins. Horizon 2 can play a role by co-funding these uplift programs for organisations unable to absorb the full cost.

4 Shield 3 – World-Class Threat Sharing and Blocking

4.1 While Australia has made progress in threat intelligence sharing, the flow of information from government to industry still often arrives too late to make a material difference during an active incident. Horizon 2 should address this by establishing a mechanism for classified-to-commercial intelligence sharing with vetted incident responders. This would allow high-grade intelligence to be acted on in near real-time without compromising national security.

4.2 We also see significant value in a national, anonymised post-incident lessons-learned repository, operated under a protected, no-fault reporting model similar to aviation's safety culture. This approach would allow patterns, vulnerabilities, and attacker techniques to be shared across industries without fear of reputational or regulatory damage.

4.3 Such a repository would be most effective if it captured data from entities that regularly have early visibility of incidents. For example, dedicated incident response teams such as McGrathNicol's DFIR practice have access to real-time threat intelligence drawn from multiple live cases, including ransomware, business email compromise, and large-scale data breaches. The insights from these cases, particularly the initial intrusion vectors, detection methods, and effective containment steps, could significantly enhance the repository's value if aggregated and shared in near real-time.

4.4 Cyber insurers are another critical source of information. They are routinely involved in a far larger volume of incidents than are ever made public, including many that are not reported to regulators under current thresholds. Their aggregated claims and investigation data can provide an unparalleled view of emerging attacker tactics, high-risk sectors, and recurring security control failures. Enabling insurers to contribute anonymised intelligence quickly to government, and, where appropriate, to vetted private sector partners, would ensure that lessons learned from non-reported incidents still contribute to the national picture.

4.5 By creating a formal channel for these trusted parties to feed information into a national system, Australia could reduce the lag between incident occurrence and sector-wide defensive action, improving collective resilience and reducing the likelihood of repeat attacks using the same methods.

4.6 Finally, automated integration between sector-specific threat feeds and the Australian Cyber Security Centre's (ACSC) platforms should be prioritised. Reducing manual processes will help organisations act on threat intelligence in minutes rather than hours.

5 Shield 4 – Protected Critical Infrastructure

5.1 Horizon 2 presents an opportunity to extend SOCI Act obligations to high-dependency suppliers of critical infrastructure, particularly where a compromise in the supply chain could have the same effect as an attack on the primary operator.

5.2 Regular red team/blue team exercises, coordinated at a national level, should become a core requirement for critical sectors. These exercises need to simulate realistic multi-vector attacks that test detection, decision-making, and coordination between operators, suppliers, and government agencies.

5.3 Operators should also be required to maintain pre-contracted incident response vendor arrangements and deploy MDR or equivalent capability. In our experience, the time lost sourcing contracts during an incident can materially increase both impact and cost.

6 Shield 5 – Sovereign Capabilities

6.1 Australia's sovereign capability should focus on building and sustaining a skilled cyber workforce and supporting domestic businesses with leading expertise, rather than attempting to develop competing technology at the scale of large global vendors.

6.2 A national cyber workforce exchange program, rotating talent between government, managed service providers, advisory firms, and critical industry, would strengthen collaboration and ensure knowledge flows between sectors. This program should include accredited responders: trusted, pre-vetted incident response providers with demonstrated capability and security clearances. Leveraging accredited responders ensures that when specialist skills are needed, such as those within McGrathNicol's DFIR practice, they can be mobilised quickly, both in Australia and in coordinated regional responses. These responders also bring access to real-time threat intelligence drawn from multiple active cases, enriching national situational awareness and speeding defensive action.

6.3 Supporting Australian technology companies remains important, particularly those delivering niche or specialist capabilities that complement global solutions. Targeted funding, tax incentives, and streamlined procurement processes should be used to help these companies grow and integrate into national security supply chains.

6.4 The current procurement process often excludes capable Australian SMEs, including accredited responders, due to disproportionate administrative requirements. Fit-for-purpose, simplified pathways would allow these businesses (whether service-based experts or specialist product developers) to play a greater role in building sovereign capability.

7 Shield 6 – Resilient Region and Global Leadership

7.1 Australia's leadership role in the Indo-Pacific must extend beyond policy statements to tangible, shared capability. Horizon 2 should fund regional capacity-building programs that deliver training, incident simulation exercises, and technology uplift to partner nations.

7.2 Joint threat intelligence initiatives should be established with trusted regional partners, targeting region-specific threats and enabling coordinated disruption activities against hostile actors.

7.3 Internationally, Australia should continue to advocate for norms and frameworks around ransomware, including coordinated sanctions and "safe-harbour" reporting arrangements that encourage disclosure without punitive consequences.

8 Cross-Cutting Recommendations

8.1 Horizon 2 must be designed with a clear path from **policy to practice**. Funding should be allocated not only to strategic initiatives but to their operational rollout. The Cyber Security Policy Evaluation Model should measure

outcomes that matter, for example, the percentage of incidents detected before data exfiltration, or the average time to recovery after a breach.

8.2 Ransomware resilience needs a stronger national approach. Expanding no-fault, mandatory ransomware reporting will improve visibility, and creating a national anonymised ransomware tactics, techniques, and procedures (TTP) database will accelerate response times for accredited responders.

9 Conclusion

9.1 McGrathNicol supports Horizon 2's ambition to scale cyber maturity across the Australian economy. We believe that with a greater focus on practical execution, governance accountability, and operational resilience, Horizon 2 can deliver measurable improvements in the nation's ability to withstand and recover from cyber threats.

Appendix A – Response to Consultation Questions

Are the right outcomes identified for Horizon 2? What changes or additions would you suggest?

The six Cyber Shields remain a sound organising framework and the outcomes identified are broadly appropriate. Where the Strategy needs strengthening is in addressing the execution gap for SMBs, in managing the risks posed by third-party providers, and in preparing for emerging technology risks such as quantum computing.

- SMBs need a scaled, practical, and affordable pathway to improve maturity, not just awareness campaigns.
- Third-party and SaaS providers should be required to meet the same baseline security and resilience standards as the organisations that rely on them.
- Horizon 2 should also begin preparing Australia for post-quantum security while embedding Zero Trust models into the private sector.

What should government, industry, and the community prioritise to achieve these outcomes?

The success of Horizon 2 will depend on focusing resources on measures that lift maturity across the whole economy, particularly among SMBs, while also driving consistency in supply chain resilience. Funding and regulation must work together to ensure outcomes are practical and enforceable.

- A national cyber maturity framework tailored for SMBs, with staged implementation and certification options.
- Co-funded uplift programs, vouchers, and sector-based shared services to make core protections affordable for smaller organisations.
- A national panel of accredited responders available to SMBs at subsidised rates, ensuring rapid response and intelligence capture.
- Stronger regulation of third-party and SaaS providers, ensuring supply chains meet the same standards as their customers.
- Investment in Zero Trust adoption across the private sector and early planning for post-quantum cryptography.

What role should government play in achieving these outcomes?

Government's role should be to set clear minimum standards, provide targeted funding and incentives, and create the regulatory environment that drives consistency across all sectors. It should also ensure intelligence flows quickly and securely to trusted industry partners, and that national lessons are captured and shared without fear of reprisal.

- Act as custodian of a no-fault lessons-learned repository, encouraging early and open reporting.
- Provide funding and co-investment to support uplift in sectors where cost barriers are greatest.
- Lead national workforce initiatives, including structured exchange programs that involve accredited responders and industry specialists.
- Reform procurement so capable SMEs and accredited responders can participate directly in national cyber initiatives.

How can the outcomes be measured effectively?

Measurement must go beyond compliance statistics to demonstrate whether resilience is actually improving. Indicators should focus on maturity, responsiveness, and recovery.

- The percentage of SMBs and larger entities achieving the national baseline.
- Average detection, containment, and recovery times for incidents.
- Uptake of Zero Trust and post-quantum planning across sectors.
- Timeliness and usefulness of intelligence provided to responders.
- Participation in the workforce exchange program and contributions to the national lessons repository.

Are there specific risks or barriers to achieving the outcomes in Horizon 2?

Several structural risks could undermine Horizon 2 if not addressed. Skills shortages will continue to limit the availability of specialist expertise, while cost and complexity will remain barriers for SMBs. Reluctance to share incidents, fragmented regulation across jurisdictions, and restrictive procurement rules may also prevent meaningful progress.

How can these risks be addressed?

Mitigating these barriers will require a combination of workforce, regulatory, and funding reforms.

- A national cyber workforce exchange to build capacity across sectors, particularly in areas like DFIR.
- Co-investment programs to lower financial barriers for SMBs.
- Safe-harbour provisions for incident and ransomware reporting to encourage early disclosure.
- Harmonisation of federal and state regulations to reduce duplication and inconsistency.
- Simplified procurement models to ensure accredited responders and capable SMEs can contribute quickly and effectively.