2023-2030 Australian Cybersecurity Strategy

SHOGUN CYBERSECURITY
Consulting & Professional Services
https://shogun.net.au
[redacted]

Horizon 2 Discussion paper submission

August 29, 2025

Executive Summary

Shogun Cybersecurity welcomes the opportunity to contribute to the development of Horizon 2 of Australia's Cyber Security Strategy (2026-2028). As a specialist cybersecurity service provider focused on the small and medium business (SMB) market, our submission draws on over a decade of on-the-ground experience working with SMBs, not-for-profits (NFPs), and their IT service providers.

Our response is structured to clearly align with the topics and questions raised in the Horizon 2 discussion paper. Our key recommendations focus on:

- Addressing systemic barriers to cybersecurity adoption in the SMB and NFP sectors.
- Building required workforce capabilities as specialisations of foundational professions.
- Enhancing regulatory guidance and frameworks for accountability; and
- Developing pragmatic solutions that acknowledge the real-world constraints faced by Australian citizens and organisations.

---

2. DEVELOPING HORIZON 2

2.1 Outlook for Horizon 2

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?

Several critical developments have the potential fundamentally reshape the cybersecurity landscape by 2030, both in Australia, and on a global scale:

Artificial Intelligence and Technological Transparency
Large Language Models (LLMs) present unprecedented challenges due to their opaque workings and non-deterministic nature - identical inputs produce different outputs with increasingly unpredictable results. This stands in contrast to traditional algorithmic systems where outputs were relatively static and predictable, AI models are not only unpredictable but essentially impossible to reverse-engineer. This evolution toward opaque systems and not-verifiable outputs demands greater transparency in AI system development and operations as a critical cybersecurity imperative.

Geopolitical Technology Dynamics
By 2030, current geopolitical tensions are likely to accelerate technological divergence. Nations restricted from accessing existing technology ecosystems will rapidly accelerate their domestic innovation and investment in technology. We believe China is positioned to achieve world leadership in all critical aspects of technology innovation and development, potentially leaving the US and allies outclassed in technology capability, putting Australia at significant strategic disadvantage.

Identity Proofing Crisis
Identity proofing based on current methods will become increasingly difficult as fraud becomes increasingly more undetectable. We have already passed the point where humans can readily distinguish between AI-generated content and authentic material. By 2030, we predict that even computer-based systems will struggle to make this distinction, fundamentally compromising traditional identity verification methods.

Data Collection and Breach Accountability Gap
Governments and companies continue collecting mass amounts of personal data with minimal oversight and little to no consequences for breaches and the resulting cyber-enabled crime which they facilitate. This economy-wide dependency on personal information is a systemic vulnerability affecting all Australians.

2.2 Collaborating across all levels of Australian Government

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

State and local governments have been largely ineffective in cybersecurity implementation, treating it primarily as a federal responsibility. The lack of consistency in approaches and investment across states creates a "weakest link" situation where the entire country faces risk due to inaction in some jurisdictions.

Recommendation: The National Cybersecurity Coordinator should be granted powers to implement a nationwide cybersecurity approach across all government levels and mandate state and local government compliance with minimum standards.

2.3 Monitoring progress in a changing world

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

The current Cyber Security Policy Evaluation Model requires significant enhancement:

- **RACI Framework:** Clear Responsibility, Accountability, Consultation, and Information roles should be embedded for all interventions and outcomes
- **Intervention Expansion:** Figure 5's model is too basic, requiring substantially more interventions to support stated objectives.

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

For meaningful SMB sector data collection, government must engage through IT Managed Service Providers (MSPs). They have the best access to business owners, and on-the-ground insights essential for understanding this sector's cybersecurity implementation realities.

3. SHIELD-LEVEL FOCUS FOR HORIZON 2

3.1 Shield 1: Strong businesses and citizens

Consolidate our cyber awareness messages across the economy

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

Government cybersecurity messaging suffers from fragmentation and policy contradictions across different agencies with different agendas, actively undermine the overall effectiveness.

Centralised Coordination: We recommend that all government cybersecurity communications should flow through the National Cybersecurity Coordinator's office to ensure consistent messaging from all arms of government, and avoid the current problematic situation where every agency appears to operate independently.

Address Policy Contradictions: The government actively undermines its own cybersecurity messaging and stated policy goal by implementing counterproductive and contradictory legislation:

- The social media ban for minors removes educational opportunities for teaching online safety in controlled school and home environments, instead releasing inexperienced 16-year-olds into digital spaces without prior exposure. This undermines messaging around educating children about online safety and encouraging them to consider cybersecurity as a career.

- While some government campaigns promote good cyber-hygiene and strong cybersecurity tools such as secure messaging apps, multi-factor authentication, and password managers, law enforcement and intelligence agencies simultaneously advocate for encryption backdoors, powers to compel vendors to undermine the security of their platforms, and mandatory collection of masses of personal information. These sorts of direct contradictions undermine create confusion about government priorities and undermine confidence in the government's cybersecurity competency.

Increasing cyber literacy in our schools

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 fundamental challenge in achieving gender balance in cybersecurity fields is cultural rather than educational. Addressing low female participation requires confronting inherent social biases that develop early among young people, particularly attitudes that position STEM fields as exclusively masculine domains where women are perceived as inferior or unwelcome. Self-entitlement and hostility among young boys towards girls they perceive as threatening their dominance in a field they regard as their natural strength is the single biggest factor driving girls and women away from STEM and cybersecurity more specifically.

Target resilience uplift to small and medium-sized entities

How can Government encourage SMBs and NFPs to uptake existing cyber resources?

The government must recognise it fundamentally misjudged the small business cybersecurity problem. The primary barriers to uptake and investment are not ignorance or lack of guidance and educational resources, as the original strategy seems to have presumed.

Root Cause Analysis:
Based on our extensive experience working with small business, owners face three systemic obstacles which prevent them from engaging more proactively with existing government

resources, and acting on cybersecurity in general. In our assessment, they are insurmountable under the current strategy:

- Time poverty – Time is a finite resource, and small business owners are already at full capacity running their business. Free resources are useless to someone without the time to consume or implement them.
- Technological illiteracy – this is itself a symptom of time constraints, but there are other contributing factors, such as age and natural aptitude. The lack of understanding creates a psychological aversion to engaging on the topic.
- Limited financial capacity – With neither the time nor the skills themselves, the only recourse to small business owner is to seek external assistance, however under current market conditions this is generally unaffordable to SMBs.

These are systemic obstacles embedded in our economic structures, they cannot be overcome merely with policy and/or education.

Practical Solutions:

Tangible Financial Support*:* Money is really the only practical lever available to the government within the strategy's timeline. SMBs must be provided substantial financial support to if they are to be more proactive in addressing cybersecurity.

Facilitate Passive Engagement*:* Establish government-funded "cybersecurity outreach" organisations that proactively engage small businesses rather than expecting them to seek resources on their own.

Offer Financial Incentives*:* Create tangible incentives including tax credits, subsidies, and discounts on government services for businesses engaging with cybersecurity programs.

Improved Visibility*:* Small business owners don't go to government first for cybersecurity help—they ask family/friends in IT or rely on their IT service providers. Improve resource visibility among these crucial referral sources.

How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector?

The Government must acknowledge that ignorance and lack of guidance are not impeding small business cybersecurity action, rather it is that small businesses are literally incapable of taking meaningful action independently, due to the constraints highlighted above.

Suggested Strategic Adjustments:

- Stop relying on fear-based messaging as the primary motivator, this doesn't resonate with small business owners.
- Introduce tangible financial incentives, such as tax credits or rebates, with clearly demonstrable ROI.
- Address misconceptions that cybersecurity is purely a technology problem that can be fully outsourced to an IT service provider – it is at best a shared responsibility, and small business owners are ultimately accountable.
- Make cybersecurity a competitive advantage through government procurement requirements.
- Address affordability issues – security features are often price-gated behind enterprise plans and unaffordable to small businesses; Service providers only want to work with big businesses with deep pockets.

- Encourage large businesses to assist their smaller suppliers and partners with building cybersecurity capabilities.
- Extend regulatory/professional licensing requirements to embed minimum cybersecurity standards across all industry verticals.

Service Delivery Models:

The IT managed service provider business model is fundamentally predicated on "monthly recurring revenue" from reselling software and cloud services. This is a low margin model, so profitability depends on service delivery with as little client interaction as possible. Additionally, service providers in the SMB market are not generally equipped to provide the kind of "high touch" consultative services that addressing cybersecurity properly requires – particularly in the areas of governance, risk, and compliance.

For these reasons, small businesses, and especially sole traders and micro businesses, often struggle to access cybersecurity services because they are not profitable for IT service providers. This is a serious market failure and justifies substantial government intervention. We suggest one of the following approaches:

- **Option A:** Establish a "supplier of last resort" with universal service obligations for businesses too small to be commercially viable
- **Option B:** Create a subsidised cybersecurity services panel with government-set pricing and vetted providers. The existing small business resilience service could be extended to match and refer small businesses to suitable service providers from the panel.

Exploring cyber security standards for small businesses and not for profit

What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs?

Existing cybersecurity frameworks, developed prior to the cloud revolution and with mature enterprises in mind, are fundamentally incompatible with small business contexts. The Government's persistent promotion of the Essential 8 as suitable for SMBs has been particularly damaging, as this framework was designed specifically for government environments with controlled, on-premise infrastructure. This has contributed to a perception among small businesses that cybersecurity is too hard, too complex, and highly technical in nature

The OpenCASE Framework:
Shogun Cybersecurity supported development of the Open Cybersecurity Architecture for Small Enterprise (OpenCASE) framework (https://opencase-framework.org/). It has been designed from the ground up to cater specifically for modern, cloud-native small businesses.

Key OpenCASE Features:

- **Clear Prioritised Structure:** Defined 11 priorities with 3 implementation levels in each.
- **Freely Available:** Creative Commons licensing eliminates cost barriers to adoption.
- **Transparent:** Fully open for external review and critique.
- **Open Source:** Community-driven improvement process.
- **Honest Messaging:** Sets clear expectations of complexity and effort required, no misleading branding which falsely implies simplicity.
- **Modern Business Focus:** Designed for distributed, cloud-centric environments.

Government Role:
While we steadfastly believe the OpenCASE framework represents the best option for modern small businesses, we also recognise that monoculture is a weakness and freedom of choice is

important in a dynamic market. Rather than mandating any single standard, we believe the Government's role should be to assess and compare emerging SMB frameworks, developing guidance to help businesses choose appropriate standards through existing touchpoints like the Small Business Cyber Resilience Service and Cyber Wardens training. Given the emerging nature of SMB cybersecurity standards compared to those in the enterprise space, we believe that such guidance from the Government will play a vital role in legitimising these frameworks in the eyes of industry.

Additional cyber security challenges for the NFP sector

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?

NFPs face unique systemic challenges beyond typical business constraints:

Organisational Culture Issues:
NFP board members typically come from mission related backgrounds and lack corporate governance experience. Consequently, they tend to view cybersecurity as a burdensome overhead that detracts from mission objectives. We believe this attitude partly stems from discrepancies in director duties between companies and NFPs, with minimal legal consequences for directors of NFPs in the wake of cybersecurity incidents or failures to adequately manage cybersecurity risk.

Regulatory Framework Gaps:
In addition to differences in director's duties, NFPs have no sector specific statute or regulation which mandates action on cybersecurity or cyber-risk. Even ACNC guidance only references the Privacy Act as being potentially applicable legislation, and many NFPs were covered by the small business exemption until it was recently removed.

Volunteer Dependency:
The high reliance on volunteers among NFPs stems not just from purely financial constraints, but also from cultural resistance to operational expenditure not directly supporting mission outcomes. Consequently, internal roles are often filled based on a willingness to volunteer or to work for below market rates, rather than being suitably qualified.

Suggested Interventions:

- Revise ACNC Act and/or Governance Standards to include legally enforceable cybersecurity requirements with meaningful consequences.
- Research and publish revenue-based cybersecurity spending benchmarks for NFPs.
- Investigate the creation of a volunteer "cyber corps" connecting experienced cybersecurity professionals with under-resourced NFPs (sub-$3M revenue threshold)

The role of cyber insurance in strengthening cyber resilience

Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs?

SMBs face significant challenges in accessing cyber insurance, largely due to general insurance brokers lacking domain specific knowledge to properly assess and advise their clients, or identify suitable insurance options. There is a heavy reliance on proposal forms provided by the insurers, which are not typically written with small businesses in mind.

Proposal Form Problems:

- Questions are overly technical, beyond typical small business owner comprehension.
- One-size-fits-all risk assessment approaches written for large enterprises with legacy IT infrastructure disadvantage SMBs with modern, cloud-based environments.

- Length and complexity require disproportionate time investment to fill out, discouraging small businesses from applying at all.
- Perception of technical prerequisites implied by questions create false barriers, causing some SMBs to abandon applications.

Market Education Gaps:
SMBs also tend to hold dangerous misconceptions about cyber insurance, either assuming they won't be eligible due to inadequate internal cybersecurity, or viewing insurance as an alternative to implementing security measures rather than as a complementary risk mitigation strategy.

Ransomware and cyber extortion

How well do you consider you understand the threat of ransomware, particularly for individuals and small entities?

As specialist SMB cybersecurity providers, we observe that ransomware operators have strategically shifted focus over the past 5 years to target SMBs as they have become the more profitable targets. Compared to enterprises, SMBs are less likely to have viable backups and have lower capacity to absorb operational disruption, creating greater incentive to pay ransom demands (especially if such payments are covered by their insurance policy).

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

Focus on Preparation: More emphasis should be given in government guidance to preparation through regular backup of ALL critical data, including SaaS applications, proper backup methodologies, and periodic restoration verification.

Gap Awareness: Many small businesses misunderstand the recoverability offered by standard cloud storage services they depend on. Better education around the nature of cloud storage as not equivalent to backup, emphasising value of multiple/offline copies and verification of restoration capability.

Offensive Capabilities: Consider deploying the Government's offensive cyber capabilities against threat actors targeting Australians to disrupt campaigns, recover encryption keys, and delete stolen data.

Enhance support for citizens and victims of cybercrime

Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector?

Marginalised online communities where real-life identities are hidden for personal safety reasons face disproportionate risks from data breaches and deliberate "doxing." LGBTQIA+ people, sex workers, and domestic violence victims face profound, long-lasting impacts and physical danger from identity exposure.

These communities are frequently targeted by hate groups and marginalised by platform operators and financial institutions through de-platforming and de-banking practices, forcing adoption of riskier behaviours and usage patterns.

Strengthening Australia's identity crime response

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

We believe that the Government's focus should shift from victim support to preventing identity crime through systemic reform. The underlying weakness enabling identity crime is dependency on personal information for identity proofing - information that was never truly private to begin with, and is now widely compromised through successive mass data breaches.

Fundamental Reform Required:
Current identity proofing methods which rely on collection of personal information and government issued documentation must be replaced more modern methods. We advocate for cryptographic solutions designed to be fraud and tamper-resistant. Technologies including public key cryptography, blockchain/distributed ledger, and zero-knowledge proofs present promising alternatives.

Avoid Centralisation Risks:
Centralised systems like MyID create giant honeypots for attackers and critical single points of failure. Investment in new solutions should focus on distributed systems which are designed ground up to be fault-tolerant against targeted disruption methods, such as distributed denial of service attacks.

Harmonise and simplify cyber regulation

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

The Privacy Act represents the most significant regulatory failure in Australian cybersecurity. Despite broad applicability, it has been ineffective at driving cybersecurity investment due to historical small business exemptions, an under-resourced and under-powered regulator incapable of enforcement, and reluctance by the regulator to impose meaningful penalties.

Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation?

For SMBs and NFPs, the *lack* of applicable regulation negatively impacts cybersecurity maturity. These entities will not invest in non-mandatory requirements, and even mandatory compliance typically receives only minimum viable investment.

3.2 Shield 2: Safe technology

Ensure Australians can trust their digital products and software

What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks?

The IoT Cyber Security Certification and associated IoT Security Trust Mark represent current best practice for edge devices and Consumer Energy Resources (CER), providing the most robust voluntary framework currently available.

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

An "Australian Standard" style approach requiring consumer edge and IoT devices sold in Australia to demonstrably meet minimum cybersecurity standards will provide a familiar and easily understandable consumer confidence mechanism.

Supply chain risks

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

Identifying foreign ownership and evaluating associated risk is beyond the capabilities and resources of small businesses. We recommend that the Government publish a simple supply chain risk ratings for foreign countries, similar to DFAT travel advisories, enabling Australian businesses (particularly SMBs) to easily understand and quantify risks associated with vendors in different foreign jurisdictions.

Protect our most valuable datasets

How could government better work with industry to understand data access and transfer across the economy?

Privacy policies published under the Australian Privacy Act provide key insights into data collection and usage patterns. As publicly available documents, these could be analysed at scale to identify common patterns and trends from an economy-wide perspective.

How can government and industry work better together to achieve secure data sharing while preventing exploitation?

We believe this question poses a fundamental contradiction: facilitating data sharing inherently increases exploitation risk. Data shared is data exposed to exploitation. Rather than pursuing "secure" data sharing, we suggest that focus should shift to adapting economic models that function without extensive data sharing requirements.

Promote the safe use of emerging technology

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

The Government should leverage its internal capabilities to assess emerging technology risks and publish clear, easily understood public guidance, incorporating findings into existing resources like Cyber Wardens.

We believe that the most serious national security threat from emerging technologies is the imminent shift in technological dominance which is resulting from the acceleration of innovation and development in China, driven by restrictive trade policies of the USA. This will likely lead to long-term strategic disadvantages for Australia unless geo-political alliances are reframed.

3.3 Shield 3: World-class threat sharing and blocking

Encourage and enable proactive cyber security posture

What could government do to support and empower industry to take a more proactive cyber security posture?

The ability to be proactive with cybersecurity requires time and resources that many Australian businesses simply lack. Small businesses in particular lack the ability to make use of threat sharing/blocking resources currently provided by the Government. Future support must provide actual capability, not just guidance:

- **CTIS Platform Extension:** Partner with technology vendors to integrate ASD CTIS capabilities seamlessly into security tools and make them affordable to SMBs.
- **Sector-Specific Briefings:** Engage industry peak bodies and professional associations for regular threat briefings with actionable guidance
- **"Set and Forget" Integration:** Focus on capabilities requiring minimal ongoing management and maintenance by businesses which consume them.

Does the government need to provide clarity on permissible and non-permissible Active Cyber Defence?

"Active cyber defence" concepts are poorly understood even among cybersecurity professionals. Any government discussion risks misinterpretation as "permission to hack back" regardless of clarity provided. We recommend that the Government focus on specific, actionable tactics they would like industry to adopt, rather than broad conceptual frameworks.

Amplify existing government and industry models

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

Beyond network infrastructure and financial services, operating systems and app stores represent the most promising centralised threat blocking opportunities. The Government should work with technology vendors to embed Australian government threat intelligence directly into their products for distributed, decentralised threat blocking.

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

We believe that this approach may backfire due to existing alert fatigue, potentially causing users to disable warning functionality entirely. An alternative approach which could be considered would be to introduce functionality which quietly correct typos and deceptive characters in domains, either using a browser plugin or DNS-level filtering integrated into networking equipment.

Threat intelligence sharing ecosystem

What more is needed to support a thriving threat sharing ecosystem in Australia?

SMBs and NFPs lack tools to benefit from real-time cyber threat intelligence. A sector-specific ISAC would be helpful, but would need to be majority government funded due to limited financial resources in these sectors.

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

We believe that one the biggest threat intelligence gaps which enables scams is the lack of any publicly accessible database or index of suspected scam phone numbers. We recommend that the Government establish a centralised register of known scam phone numbers, which could then facilitate real-time blocking by telecommunications providers.

Cyber conflict and crisis preparedness

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?

These roles are not clear, as they across a raft of different legislation and regulations, with no easily referenceable single source of truth. The government should conduct a comprehensive review of existing legislation and compile consolidated RACI-style documentation for publication.

Following the publication of these roles, we recommend that the Government plan and host an economy-wide cyber incident response exercises simulating a malicious cyberattack on the scale of the CrowdStrike incident.

Managing vulnerability disclosure

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

Current laws and legal frameworks are too easily weaponised against legitimate security researchers. They facilitate suppression of vulnerability reports, as vendors use them to make legal threats towards anyone who discloses a vulnerability to them. Until researchers are protected from legal liability for discovering and reporting vulnerabilities, businesses have little incentive for adopting collaborative disclosure policies.

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

Yes. Security researchers currently face legal risks when reporting vulnerabilities to companies without responsible disclosure policies. Australia needs a national program and should consider mandatory requirements for software, services, and devices sold domestically.

3.5 Shield 5: Sovereign capabilities

Promote sustainable and diverse cyber workforce

What role should government play in supporting the development and growth of Australia's cyber workforce?

The government should abandon its misguided efforts toward mandatory professionalisation of "cybersecurity" professionalisation. It must be recognised that cybersecurity is not a distinct profession in and of itself, but rather is a specialisation built upon other foundational career paths. For example:

- A cybersecurity engineer is a specialised IT/systems engineer.
- A cybersecurity auditor is a specialised auditor.
- A penetration tester is a specialised software QA tester.

Rather than attempting to create "cybersecurity professionals" from scratch using generic qualifications which treat cybersecurity as a single monolithic professional, we encourage the Government to adopt an approach that focuses on upskilling professionals in foundational careers to specialise in cybersecurity.

What have been the most successful initiatives and programs that support mid-career transitions?

We are aware of the following programs which have made a positive impact in supporting mid-career transitions:

- Australian Women in Security Network (AWSN) mentoring program.
- WithYouWithMe's services helping military veterans, first responders, and refugees transition into cybersecurity roles.

What are some of the industries with highly transferrable skill sets?

This question incorrectly assumes cybersecurity is a separate career path. Choosing to specialise in cybersecurity is not a matter of what skills are transferrable. The focus should be on what generic foundational skills which are applicable and adaptable to cybersecurity contexts, and what are the professions which build them. For example, nurses acquire many relevant skills in their line of work (e.g. triage, risk assessment, stakeholder management, working under pressure), the knowledge gap is in how to apply them in a cybersecurity context.

Academic research and collaboration

How can government and academia enhance partnership and collaboration on research and policy development activities?

The government must commit to increasing and sustaining academic funding. Repeated funding cuts combined with international student regulations have financially crippled Australian universities, leaving them unable to contribute meaningfully to cybersecurity research and policy development.

Nurture sovereign capabilities development

How would we best identify and prioritise sovereign capabilities for growth and development?

Given Australia's sovereign capabilities are niche, and the wide scale, systemic nature of our dependency on foreign technology, we recommend a risk-based approach:

- Evaluate potential impacts if foreign-controlled technological capabilities were removed, degraded, or weaponised against us.
- Prioritise development of capabilities with the highest potential impacts.

What are the areas of most concern for ICT concentration and what mitigation strategies should be explored?

We believe that the critical dependency on American cloud providers, cybersecurity vendors, and technology companies represents the greatest sovereign risk to Australia. Companies like Microsoft explicitly state US law supersedes other national laws regardless of data residency or service delivery location. Australia's economy is at serious risk of sudden collapse if access to American technology was withdrawn, degraded, or turned against us.

This is not an unlikely hypothetical scenario in the current geo-political climate – the Trump administration has shown clear willingness to abuse their technological dominance against enemies and allies alike. To mitigate these risks, the Government must prioritise sustained investment in locally developed alternatives, and commit government to use of domestic rather than foreign-owned products and services.

3.6 Shield 6: Strong region and global leadership

Cyber diplomacy and deterrence

Do you view attributions, advisories and sanctions as effective tools for countering growing malicious cyber activity?

Current attribution, advisory, and sanctions-based approaches have proven largely ineffective. Public naming and shaming has had minimal deterrent effect on nation-state actors who simply deny allegations, and criminals that remain in uncooperative jurisdictions. Sanctions targeting individuals impose no meaningful costs on supporting governments.

Effective deterrence requires imposing real costs through meaningful economic impacts or threats to governmental stability. The government must take a more assertive stance if it hopes to have any meaningful impact.

Regional engagement

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

We recommend the establishment of a joint regional cybersecurity strategy harmonising approaches across all participating nations, with the aim of creating a consistent vision and coordinated regional cyber defence capability.

Is there additional value that Cyber RAPID can provide beyond its current design and scope?

Extending the scope beyond merely responding to actively pursuing and disrupting organised cybercrime operations, particularly scam call centers, in remote regional areas would provide immense value to the Australian public in the fight against international scammers.

International regulatory alignment

What regulatory frameworks or requirements should be prioritised for international cyber regulatory alignment?

We believe that priority areas should include privacy, artificial intelligence, and data sovereignty. It is our opinion that the EU generally provides superior regulatory examples in these areas.

We also advocate for a global treaty against undermining encryption and security technologies to prevent a "backdoor arms race" between competing governments seeking to weaken security protections contrary to other nations' interests and established human rights.

Conclusion

Australia's cybersecurity future depends on acknowledging real barriers faced by small businesses and NFPs while building genuine sovereign capabilities. Success requires moving beyond ineffective awareness campaigns and free resources toward structural support, financial incentives, and regulatory frameworks creating accountability.

The government must recognise cybersecurity as a specialisation rather than distinct profession, and that current foreign technology dependencies create existential risks to Australian cyber-sovereignty.

Our recommendations provide practical pathways addressing these challenges while supporting government's broader strategic objectives for Horizon 2 (2026-2028) of the cybersecurity strategy.

This submission represents the views and recommendations of Shogun Cybersecurity based on extensive experience serving the Australian small and medium business cybersecurity market.