everlast.

Charting New Horizons Response Paper

Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Everlast Networks 2025

This page intentionally left blank.

Contents

Document changes and updates

24/08/2025 – Document drafted, and pending final review.

26/08/2056 – Document finalised.

Foreword

The Department of Home Affairs (the **Department**) is right to recognise that Australia's cyber security strategy must continually evolve to meet the challenges of the coming decade.

Horizon 2 of the 2023–2030 Cyber Security Strategy duly recognises the emerging scale, sophistication, and impact of modern cyber threats, and that government, industry, and the community all have vital roles to play in strengthening our national resilience.

The focus on uplift across six "shields" provides a practical framework for addressing immediate risks whilst laying the groundwork for future systemic change, including post-quantum cryptography, critical infrastructure resilience, and securing our country against adverse and emergent regional challenges.

Everlast Networks welcomes the opportunity to contribute to this consultation.

Our company's work focuses on creating Australian-made future-ready security technologies, such as post-quantum safe communications, trusted Secure Gateways, near-zero SWaP solutions for Defence, and the creation of advanced service availability; as well as conducting advanced research and development in communications, trust, and cryptography.

We believe our experience offers useful insights to the Department into how Australia may defend its own interests, and play a leading role in securing our region. We thank the Department for opening this process to broad input, and for its commitment to practical engagement with businesses, researchers, and the wider community.

Executive Summary

This submission aims to address selected consultation questions across the Horizon 2 shields, focusing upon areas where stronger guidance, standards, and coordinated programs stand to deliver tangible benefits.

Our primary recommendations are as follows:

1. Protect against long-term adversarial risks by prioritising migration to post-quantum cryptography, adopting memory-safe languages, and alignment with secure software development frameworks.
2. Ensure the accessibility of security standards such as the Essential Eight with community outreach, educational initiatives, and practical resources, with a particular focus on supporting SMB's, NFP's, and the broader public.
3. Coordinate automated blocking of malicious traffic, strengthen threat intelligence sharing across agencies and sectors, and embed incubation-style programs to safely test and adopt emerging technologies.
4. Enhance regulatory obligations on high-risk operators, improve guidance on foreign ownership and control risks, and rehearse real-world outage scenarios across Cloud, Critical Infrastructure, Telecoms, and Operational Technology.

Taken together, these recommendations emphasise the importance of reforms being both forward-looking and pragmatic. A national strategy must set ambitious goals; however, it must also provide the Australian public, businesses, and agencies with practical tools and support to facilitate such change.

In our view, Horizon 2 presents an excellent opportunity to balance both objectives, and we encourage the Department to embed clear roadmaps, measurable outcomes, and transparent communication, so that all Australians can have confidence in our collective cyber resilience.

2. Developing our vision for Horizon 2

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?

Cyber security policy for the next few years needs to be shaped by clear identification of where technology and threat environments are heading. Horizon 2 is well placed to capture this, but only if it is grounded in the changes we are already seeing in standards, technologies, and adversary tactics. The following trends represent key factors that government should consider as it develops policy and investment priorities.

1. **Post-quantum cryptography.**
   With NIST having finalised the first set of standards, the immediate task of all integrations should be to begin crypto inventories and identify systems that need upgrading. Particular attention and consideration should be given to platforms that store or protect sensitive information over long lifespans, as these are at the highest risk from "harvest now, decrypt later" attacks.
   Hybrid post-quantum modes for TLS 1.3 are mature enough to deploy, and suppliers should be required to publish migration roadmaps and demonstrate interoperability. Computational overheads will exist in the short-term while algorithms catch up, however, advancements in processing and optimisations can lead to better performance than classical cryptography, with a long-term benefit of stronger protection for government and national-interest data.

2. **Encryption and Secure Gateway visibility.**

   The steady adoption of QUIC, Encrypted Client Hello, ESP, and encrypted DNS means that governments can no longer rely on legacy gateway visibility. This change strengthens privacy, but limits the effectiveness of traditional interception-based controls. In response, gateway policy must evolve.
   The Australian Government Gateway Security Standard and ACSC Gateway Guidance provide the right anchor points, but they need to be applied with an emphasis on identity, device posture, and application-level enforcement. Deep packet inspection should become the exception rather than the rule – reserved only for strictly defined uses. In practice, agencies will need to invest in telemetry that provides metadata about connections or obtain systems access, rather than attempting to break encryptions themselves.
   Planning for QUIC and HTTP/3 support in procurement processes – alongside consistent reporting fields for security operations centres – will preserve situational awareness without undermining encryption.

3. **Artificial intelligence.**

   Artificial intelligence presents a dual challenge – it offers powerful new tools for defence and government, but it also introduces fresh attack surfaces. Therefore, treating AI as a regulated system is the most effective way to manage this balance.

   Agencies should maintain a clear inventory of AI deployments, conduct structured threat modelling, and require accountability for risks – aligning high-risk uses with recognised governance standards would provide a solid baseline.

   Additionally, there is a strong case for encouraging more on-device AI processing, since running models locally reduces the need to transmit intellectual property and personal information to centralised platforms. Such an approach fundamentally reduces security and privacy risks. While this may limit model size and update frequency, the trade-off is improved data protection and control for users and agencies.

4. **Migration to memory-safe software.**

   The shift to memory-safe software should be treated as a matter of policy, not preference. Entire classes of vulnerabilities are tied to memory management issues, and languages such as Rust, Go, Java and C# can mitigate these risks from the outset. A transition will require a staged approach, prioritising network-exposed components, cryptographic functions, and privileged code paths.

   For software that cannot yet be replaced, the use of sanitisation, internalising key networks and assets, and fuzzing remain relevant strategies. Procurement and development contracts should also make memory safety the default expectation for new work, while allowing planned refactoring of legacy systems.

   This path will involve some short-term friction, but it buys significant long-term resilience while encouraging room for innovation during reworks.

5. **Securing critical infrastructure.**

   Obligations in both physical and digital security on critical infrastructure (CI) operators are deepening, and resilience can no longer be seen as a compliance exercise alone. CI Operators need to address and manage their own systems, as well as their dependence upon cloud services, telecommunications carriers, subsea cables, and satellites.

   For operational technology (OT), controlled and monitored vendor access, and segmentation both remain essential. Rather than aiming for absolute uptime (which is unrealistic), the emphasis should be on safe degradation and continuity under stress. It is likely that smaller operators will require support and guidance (such as in the form of templates and shared services) in this regard, so that improved uplift may be achieved across the board.

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?

Defence and national security programs such as the *Defence Innovation Hub* and the *Next Generation Technologies Fund* have repeatedly shown the value of incubating new technologies within the government ecosystem. They provide a way to test early-stage ideas, reduce development risk, and give SMBs and researchers a pathway to adoption. By way of example, in 2023–24 more than 80 per cent of Hub projects involved SMB's, with one-third going to first-time suppliers.

This model should be expanded across all levels of government, with dedicated streams for academia and SMB's. By opening secure testing environments, state and territory governments may work alongside the Commonwealth to accelerate the uptake of trusted home-grown Australian cybersecurity technology, while also strengthening skills and research translation. The result would be faster adoption, greater coordination, greater trust and transparency from the public in the different levels of Government, and a stronger national cyber capability base.

3. Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

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

For Small and Medium Businesses (**SMB's**) and Not-For-Profits (**NFP's**), the priority should remain on standards that are practical, well-supported, and already recognised internationally. The ACSC's Essential Eight Maturity Model remains the most accessible baseline, and its staged approach is now being used by state governments as a default reference point. It should be reinforced by broader adoption of ISO/IEC 27001 for information security management, which gives SMB's and NFP's a scalable framework that can grow with their needs.

At the technical control level, the CIS Critical Security Controls provide a prioritised roadmap that is easy to measure against, while the NIST Cybersecurity Framework (CSF 2.0), updated in 2024, has proven useful for organisations that want a balanced mix of governance and technical focus. For software assurance, the NIST Secure Software Development Framework (SSDF) and Australia's alignment to it are increasingly important, particularly where SMB's and NFP's are key components of governmental or critical infrastructure sectors and supply chains.

The key is to pick standards that are already proven, and provide strong opportunities for integration between each other. If Commonwealth, State, and Territory governments reference the same small set of standards when regulating or providing guidance, SMB's and NFP's can focus resources on genuine reform, rather than attempting to comply with multiple redundant frameworks in parallel.

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?

Cyber insurance may play a role for recovery and risk mitigation; however, for many small entities it is neither affordable nor straightforward to access. Premiums have risen sharply in recent years in line with (or exceeding) the cost of living, and policies often come with legalistic exclusions that in practice limit their practical value. Many businesses may also erroneously view such insurance as a substitute for good security practice rather than as complimentary to it, leading to undue complacency.

More fundamentally, insurance is by its nature a reactive measure which attempts to reduce the harm after a cyber security event, rather than seeking to reduce the likelihood thereof. The focus must always remain on affordable baseline security controls to avoid such occurrences in the first place, rather than tacitly accepting that they will occur and focusing on damage control measures.

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?

The well-publicised data breaches involving Optus, Medibank, and Latitude each had direct and disproportionate impact upon large sectors of the Australian public, including our own team members.

- **Optus**: Up to 9.5 million customers (almost 40% of Australia's population) had sensitive personal details exposed, such as passports and driver's licence numbers.[1]
- **Medibank**: Up to 9.7 million current and former customers had highly sensitive health and identity data exposed.[2]
- **Latitude**: Up to 14 million records exposed, including 7.9 million driver's licence numbers and 53,000 passport numbers.[3]

These events left many of us scrambling with minimal guidance from the companies involved, who at best offered short-term credit monitoring or account credits. In some instances, such assistance was provided conditionally upon affected customers waiving their rights to compensation or litigation. The initial and subsequent conduct from those companies also focused upon their own internal risk-mitigation and public relations, demonstrating clear conflicts of interest that were opposed to the best interests and security outcomes of their affected customers. The disjointed nature of these responses left many Australians unsure of what to do next. The government has since improved its communication and created tools via OAIC and ACSC; however, early-stage support was uneven and often falling behind public need.

In future breaches, Horizon 2 should prioritise prompt, clear, and coordinated guidance, available as soon as incidents are disclosed, and ensure identity protection resources are meaningful and

[1] https://www.reuters.com/business/media-telecom/australias-privacy-regulator-sues-optus-over-2022-data-breach-2025-08-08
[2] https://ia.acs.org.au/article/2024/court-docs-reveal-shocking-cause-of-medibank-breach.html
[3] https://www.cshub.com/attacks/news/iotw-latitude-financial-data-breach-affects-14-million-people

long-term. In major incidences such as those outlined above, more directive and centrally coordinated responses in this vein would also be beneficial.

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

It is our view that – in some instances – current regulatory or compliance requirements for third parties working within government or defence ecosystems are lower than what constitutes good practice. For example, under the *Defence Industry Security Program* (DISP), organisations corresponding with Defence need only meet the Essential Eight at Maturity Level 2, focussing largely on patching, application control, and least privilege, or choose from NIST SP 800-171 or ISO 27001 as acceptable alternatives. These options only provide baseline protections, and do not consider nor anticipate emerging threats such as quantum-capable adversaries or highly sophisticated supply-chain attacks.[4]

Current management of these gaps tends to rely upon legacy frameworks rather than proactive adaptation. As an example, organisations often rely on DISP and Defence's authorisation frameworks, or the *Protective Security Policy Framework* (PSPF) and *Information Security Manual* (ISM) to demonstrate compliance. While these are periodically audited and require security documentation, audits (such as an ANAO review in 2024) revealed that Defence itself had only 5% of ICT systems registered in its authorisation system, and nearly half of those either expired or were unaccredited, highlighting a sizeable systemic lag in controls.[5]

We need to look beyond these insufficient baseline requirements. Holistic and fully considered best practice would instead seek to embed frameworks that anticipate quantum risks – such as a phased or stepped migration to quantum-resistant architectures, as recommended in our Department of Home Affairs Secure Gateway Consultation Paper.[6]

Emerging academic work such as the *QUASAR Strategic Framework* (published in May 2025) offers structured approaches for transitioning safely to post-quantum cryptographic systems, with readiness scoring and continuous optimisation. Another roadmap framework (STL-QCRYPTO) proposes industry-specific risk models and implementation timelines, covering critical sectors including government and defence.[7]

In practice, this could take the form of layering in hybrid-PQC TLS, enforcing crypto inventory, and agility – requiring software provenance and secured supply chains, and ensuring that authorisation frameworks like PSPF/DSPF specifically reference quantum readiness and adversary models. Such enhancements need to be mandated to ensure entities are resilient against tomorrow's threats.

[4] https://www.defence.gov.au/sites/default/files/2021-07/disp-cyber-factsheet.pdf
[5] https://www.anao.gov.au/sites/default/files/2024-09/Auditor-General_Report_2024-25_2.pdf
[6] https://everlastnetworks.com.au/wp-content/uploads/2025/08/Aus-Gov-SG-Policy-Consultation-Updated.pdf
[7] https://arxiv.org/abs/2505.17034

3.2 Shield 2: Safe technology

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

One of the biggest challenges in managing foreign ownership control or influence (FOCI) risks is the lack of practical visibility into how technology is built and governed. Commercial software may – by way of example – be headquartered in Australia or trusted allies such as the United Kingdom or the United States, but its core codebase may be compromised by having been developed, maintained, influenced by, or otherwise relying upon contributors or data from adversaries that present strategic risks to Australia. Open-source codebases and projects may be even more compromised – in the same manner as above, a project hosted on GitHub might list an Australian or US maintainer, but the bulk of active committers may be of entirely uncertain provenance.

One particularly eye-opening recent example involved an open-source maintainer being gradually groomed into a trustworthy role, only to push a backdoor security vulnerability that could have compromised SSH across millions of systems. The compromised code infiltrated XZ Utils (a critical Linux compression component), and was capable of subverting SSH authentication by abusing a core Linux library. Because the maintainer had built trust with the developer over time, the change passed review without scrutiny. It took a vigilant developer at Microsoft to spot the anomaly and prevent what some called a 'software supply-chain earthquake' before it was too late.[8] This again highlights the importance of implementing sufficient process management and security frameworks to overcome the inherent human factor weaknesses such as social engineering.

The assistance that most organisations need in this respect is guidance in tracing the ownership and governance of their software. Clear advice on how to identify beneficial ownership, developer geography, and control of code repositories would make risk assessments more consistent across government, defence, and industry. Defence and security agencies *already* flag the risk of foreign adversarial access, but their guidance is often limited to high-level statements. More practical tools and data feeds (such as registries of critical software projects, or ownership and contributor mapping) would be trivial to develop, and would enable smaller organisations to make informed choices.

Because of this gap, our organisation has increasingly invested in building and maintaining our own internal software and intellectual property. While this gives us greater assurance, it is not an efficient or pragmatic solution for the wider economy. A stronger national approach to FOCI assessment – covering both commercial and open-source technologies – would permit entities to rely on common standards, reduce duplication, and ensure that decisions reflect Australia's broader security interests rather than ad-hoc judgments at the organisational level.

[8] https://www.theguardian.com/commentisfree/2024/apr/06/xz-utils-linux-malware-open-source-software-cyber-attack-andres-freund

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

As above outlined, the most effective manner in which government may support safe and responsible uptake of emerging technologies is by creating structured programs, where new tools can be tested and evaluated before wider deployment.

Defence has shown through initiatives – such as the *Innovation Hub* and *Next Generation Technologies Fund* – that incubation models reduce risk and provide SMB's and researchers with a pathway into government use. Similar programs overseas (such as the UK's *Secure Connected Places* playbook and *Catapult* networks, and DARPA's AI assurance trials) further demonstrate how controlled testbeds accelerate innovation while keeping security and ethics front of mind. A comparable, cross-government approach in Australia (at both the federal and state levels) would provide practical guidance and lower barriers for safe adoption.

To summarise, we recommend as follows:

- Build on Defence's incubation models (Innovation Hub, Next Gen Tech Fund) to create secure trial environments across government.
- Establish separate channels for academia/schools, SMB's, and larger vendors to encourage participation from all levels of innovation.
- Provide practical guidance that goes beyond "*what not to do*" by including data governance, security assurance, and ethical use requirements.
- Reference international examples such as the UK's Secure Connected Places initiative, the Catapult innovation hubs, and US DARPA's AI assurance programs as proven models.
- Use these programs to give innovators a pathway from lab to government deployment, while giving agencies confidence that adoption is safe and tested.

3.3 Shield 3: World-class threat sharing and blocking

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

All industry struggles to block malicious traffic at the same speed and scale as threat actors operate; often leaving them on the back foot and in a fundamentally reactive security posture. The Australian Government can help them by coordinating shared defences at the network edge, particularly against known botnets and automated reconnaissance traffic ("knocks") probing for weaknesses before launching larger attacks.

A practical step would be to establish a centrally managed service that distributes high confidence blocklists of hostile IPs and domains to carriers, ISPs, and cloud providers in near real time, and distributed/decentralised into local exchanges or NBN nodes.

Our internal developers have architected and developed these kinds of systems before at scale, and the design and development is something that would be straight forward to rapidly implement. Such an approach would iterate upon the existing *Cyber Threat Intelligence Sharing* (CTIS) program, but move beyond sharing indicators into automated blocking at scale. For example, Singapore's Cyber Security Agency already runs a *Cyber Threat Intelligence Centre* that

pushes blocklists directly to ISPs, cutting down exposure for the public and small businesses that lack advanced filtering tools.

Blocking well-known bot infrastructure at the national border would prevent large volumes of malicious probes from ever reaching Australian end-users, systems, and critical infrastructure. It would also reduce the noise in security monitoring (freeing resources to focus on more advanced or targeted threats), and free up NBN network traffic. Industry should still maintain their own filtering and detection, but a coordinated national layer of defence would raise the baseline across all sectors.

Metrics for success could include reductions in unsolicited inbound traffic measured by major carriers, time-to-block from first detection to implementation, and adoption rates of the service across ISPs and hosting providers – a win-win for all of Australia.

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

Intelligence sharing often fails to land with the groups who need it most because the language is too technical or requires specialist knowledge. To improve outcomes, intelligence should be made more accessible so that industry operators and the broader public can understand and act on it.

For the public, scam and cyber warnings should be written in plain English, free of jargon, and delivered through the same channels where scams are occurring (such as SMS, email, and social media). Clear step-by-step advice ("*check the sender, don't click the link, here's who to call*") is far more effective than technical indicators. Such approaches are already implemented with positive outcomes in the banking, legal, property, and other sectors where customers are encouraged to verify prior to sending large sums of funds.

For industry and government partners, intelligence can still be shared in technical formats, but operational alignment would benefit from agreed standards. Programs like ASD's Cyber Threat Intelligence Service (CTIS) already push indicators, but greater uptake and two-way sharing are needed. Aligning feeds with STIX/TAXII formats, and requiring agencies to publish measurable "time-to-block" data, would make threat sharing more actionable. By producing layered material, Government can close the gap between awareness and action. The outcome should be both improved scam prevention and stronger trust in the Australian Government's guidance.

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

Businesses often hesitate to adopt vulnerability disclosure policies because they fear the technical burden of handling reports or the reputational risk and fallout if a flaw goes public. Government support in both operational and PR areas could help alleviate this.

Many organisations will avoid vulnerability disclosure because they worry about having to handle specialist triage or how to talk about it publicly if things go wrong. Government can provide *exactly* the kind of support that pushes for good:

- Centralised technical resources such as policy templates;
- Response playbooks; and/or
- Access to a trusted responder network.

Combined with guidance or testing in managing external communications around a disclosure, businesses can be seen to have strong disclosure programs that could be celebrated in procurement frameworks or "trusted supplier" lists.

That kind of backing works in practice. For example, Atlassian maintains a transparent vulnerability disclosure programme backed by clear timelines and public advisories; critical vulnerabilities must be fixed within 10 days for cloud products, and within 90 days for data centre releases.

In the Australian Public Service, the APS Commission has a published vulnerability policy that includes safeharbour provisions, timelines for responses, and acknowledgement of researchers.[9] In Europe, the ENISA similarly assists coordinated disclosure via national CERTs, and publishes best practice guides and templates for both public and private entities under NIS2 directives.[10]

Providing similar tools and support across sectors as industry and other governments do (bundling technical, communications, and recognition) would encourage businesses to see disclosure a less of a reputational risk, and more of proof of responsibility and readiness.

[9] https://www.apsc.gov.au/about-us/accountability-and-reporting/vulnerability-disclosure-policy
[10] https://www.enisa.europa.eu/topics/vulnerability-disclosure

Conclusion

Australia's cyber security outlook to 2030 is going to be shaped by rapid technological change, increasingly capable adversaries, and the growing dependence of the broader public and businesses upon digital services and artificial intelligence.

This Department of Home Affairs Consultation highlights the right shields and policy objectives – seeking to uplift businesses, harden gateways, share threats at scale, and ensure resilience in critical infrastructure.

The common thread across all of these policies is the need for practical and coordinated action that is both technically sound and accessible to the broader community. Where policies are too slow or fragmented, it risks leaving gaps that adversaries may exploit. Likewise, where policies are too abstract or technical, and not accompanied by outreach and education to demonstrate their practical and tangible benefits, they risk overwhelming the very organisations they are designed to support, or being written off as unimportant or useless.

These submissions aim to emphasise the importance of forward-looking standards such as post-quantum cryptography, modern gateway controls, and memory-safe development. We also wish to highlight the importance of measures such as clear communication with the public, stronger support for SMB's and NFP's, and national coordination on threat blocking.

By expanding incubation programs across all levels of government, aligning regulation with best practice, and providing practical guidance on ownership and supply chain risks, Australia can strengthen its own resilience, and set a standard for the region.

It now remains for the Australian Government to translate these ideas and the consultation it receives into clear roadmaps, measurable outcomes, and an effective national framework for the future.

We appreciate the opportunity to contribute our insights, and remain ready to support the development of a robust, future-ready cyber security framework. We invite further discussion on the matter if we can be of further assistance in guiding this framework toward a more secure and sovereign nation.

-

Everlast Networks